Kybernetická bezpečnost kamerových systémů se zaměřením na webové kamery

Kristýna Knotková

Bakalářská práce
2019/2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Kristýna Knotková**
Osobní číslo:	**A17092**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Kybernetická bezpečnost kamerových systémů se zaměřením na webové kamery**
Téma práce anglicky:	**CCTV Cyber Security Oriented on Web Cameras**

Zásady pro vypracování

1. Nastudujte problematiku spojenou s kybernetickou bezpečností webových kamer.
2. Vyhodnoťte a popište zranitelnosti webových kamer z hlediska kybernetické bezpečnosti.
3. Vyberte vhodné prostředy a nástroje pro testování webových kamer z hlediska kybernetické bezpečnosti.
4. Otestujte vybrané webové kamery na zranitelnosti.
5. Vhodně vyhodnoťte a reprezentujte výsledky.

Rozsah bakalářské práce:
Rozsah příloh:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KRUEGLE, Herman. CCTV surveillance: analog and digital video practices and technology. Second edition. Amsterdam: Elsevier, BH, [2007], xv, 656 s. ISBN 9780750677684. Dostupné také z: http://www.loc.gov/catdir/toc/ecip0517/2005022280.html
2. OWASP Top 10 – 2017 [online]. 2017 [cit. 2019-11-27]. Dostupné z: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
3. ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, 147 s. ISBN 9788073807375.
4. AWAD, Ali Ismail a Michael C. FAIRHURST. Information security: foundations, technologies and applications. London: The Institution of Engineering and Technology, 2018, xii, 404 s. IET security series. ISBN 9781849199742.
5. PAČKA, Roman. CSIRT: v přední linii boje proti kybernetickým hrozbám. Brno: Centrum pro studium demokracie a kultury, 2019, 131 s. Politologická řada. ISBN 9788073254735.
6. JAŠEK, Roman. Informační a datová bezpečnost. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky, 2006, 140 s. ISBN 8073184567.

Vedoucí bakalářské práce: **Ing. Petr Žáček**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **17. prosince 2019**
Termín odevzdání bakalářské práce: **25. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Ve Zlíně dne 7. prosince 2019

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

Kristýna Knotková v.r.
podpis diplomanta

ABSTRAKT

Tato práce pojednává o kybernetické bezpečnosti kamerových systémů, zejména IP kamer a jejich zranitelnostech. V práci je popsaná terminologie spojená s kamerovými systémy a s kybernetickou bezpečností. Dále se zaměřuje na rozbor možných scénářů útoku na zranitelnosti z pohledu kybernetické bezpečnosti webových kamer. Předposlední částí této práce je výběr vhodných prostředků pro testování webových kamer a poslední částí je samotné testování webových kamer, kdy výsledky jsou sumarizovány v závěru práce.

Klíčová slova: vss, kamerové systémy, kybernetická bezpečnost, zranitelnost webových kamer, kybernetická bezpečnost webových kamer

ABSTRACT

This work deals with cyber security of VSS systems, particularly with IP cameras and their vulnerabilities. The terminology associated with camera systems and cyber security appears in this thesis. It focuses on describing possible attack scenarios which use vulnerabilities from the viewpoint of cyber security of webcams. The penultimate part of this thesis is the selection of suitable means for testing webcams and the last part is the actual testing of webcams, where the results are summarized at the end of the work.

Keywords: vss, camera systems, cyber security, vulnerability of camera, web camera cyber security

Poděkování, motto a čestné prohlášení, že odevzdaná verze bakalářské práce a verze elektronická, nahraná do IS/STAG jsou totožné ve znění:

Prohlašuji, že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Mé poděkování patří Ing. Petrovi Žáčkovi za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování bakalářské práce věnoval.

OBSAH

ÚVOD

Cílem této bakalářské práce je seznámit se s webovými kamerami a kybernetickou bezpečností s nimi spojenou, zachytit nynější zabezpečení webových kamer, jak hardwarově, tak softwarově a následně sepsat scénáře možných útoků na zranitelnosti webových kamer a jejich bezpečnostní opatření.

V dnešní době jsou kamery téměř všude kolem nás. Mají primárně sloužit k zajištění ochrany, ale existuje zde i druhá stránka mince, proto je nutné podívat se na webové kamery zblízka a zjistit, jak bezpečné ve skutečnosti jsou a jak snadné je jejich narušení a přístup do těchto systémů. Kamery jsou hojně používané a tím je i vysoké procento nedostatečně zabezpečených kamer a vstupů do nich. Jelikož se jedná o IP kamery, tedy kamery připojené k internetu (nebo do sítě, které jsou připojené do internetu), je tu spoustu hrozeb s tím spojených. Práce tyto hrozby popisuje a uvádí možná protiopatření.

V teoretické části byl mým cílem popis základních zranitelností z oblasti kybernetické bezpečnosti a jejich vztah k webovým kamerám. Pojmenovat a popsat druhy útoků a hrozeb, které mohou mít spojitost s webovými kamerami, či zařízeními, které s nimi souvisí, a nakonec vybrat nástroje pro testování webových kamer, které použiji v praktické části.

V praktické části se věnuji samotnému testování základních zranitelností vybraných webových kamer. Je zmíněno, jaké existují možnosti průniku do webové kamery a jejich příčiny. Dále jsou vytvořeny scénáře možných útoků ke zjištěným hrozbám, bezpečnostní opatření a prevence proti vzniku těchto hrozeb.

I. TEORETICKÁ ČÁST

1 TERMINOLOGIE

V této části je rozepsána terminologie spojená s danou problematikou. Jsou zde rozepsány termíny: Kamery a jejich princip, rozdíl mezi OCTV a VSS, dříve známé jako CCTV, web-kamery a webové kamery. Dále je toto téma zaměřeno na úvod do hrozeb spojené se softwarem, konfigurací a rozhraním. Pod nadpisem rizika jsou popsána rizika a hrozby webových kamer z pohledu kybernetické bezpečnosti a základní pojmy.

1.1 Kamery

V obecném pohledu lze kameru definovat jako formát fotoaparátu, jenž vytváří velké množství snímků ve velké rychlosti za sebou. Pomocí tohoto faktu lidské oko vidí výsledek jako videozáznam čili film. [1]

Princip kamer

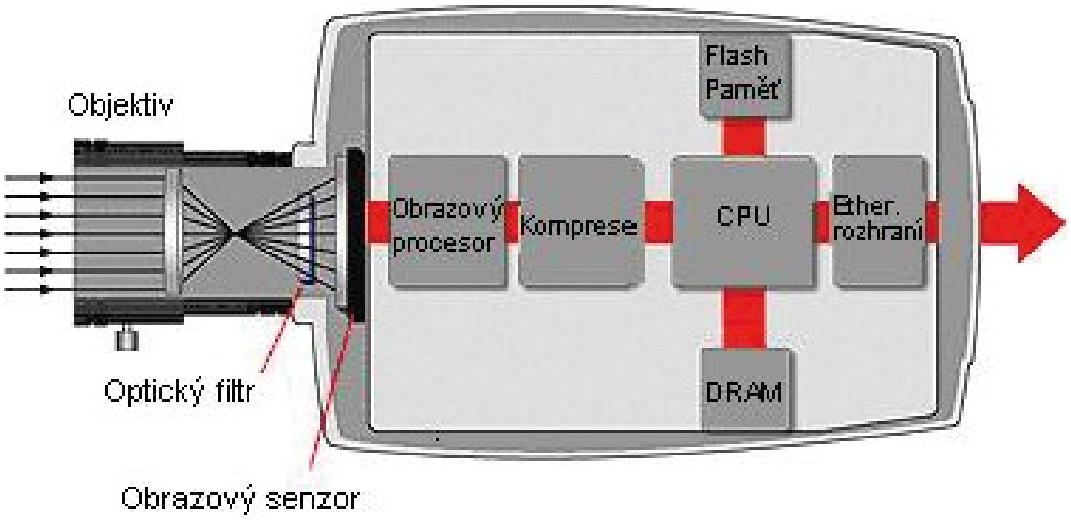
Obrazový čip kamery snímá světlo o různých vlnových délkách, které CCD / CMOS přetváří na elektrický náboj, a ten je dále akumulován. Daným výstupem je tedy analogový CCD, nebo digitální CMOS signál. [2]

Světlo před dopadem na čip projde objektivem kamery a vykreslí tak snímanou scénu. Tato funkce, která vykresluje snímanou scénu, se nazývá MTF (Modulation Transfer Function), a popisuje zkreslení obrazu vůči použitým ohniskovým vzdálenostem objektivu. Mezi objektivem a světlo-citlivým čipem je optický infračervený filtr, který zajišťuje průchod jedné určité vlnové délky, kterou si IP kamera vyžádá. [2]

Pomocí A/D převodníku si obrazový čip přetransformuje analogový signál na digitální a ten je poslán do obrazového procesoru. DSP (Digital Signal Processor), z anglického překladu obrazový procesor použitím funkcí na zlepšení výsledné kvality videa zpracuje signál v digitální podobě. [2]

Části, které obsahují pouze IP kamery:

- CPU (Central Processing Unit) – Centrální procesorová jednotka
- DRAM (Dynamic Random Access Memory) – Dynamická paměť s náhodným přístupem
- Operační paměť – Hlavní paměť
- Flash paměť – Elektricky programovatelná paměť



Obrázek č. 1. - Princip činnosti IP kamery[2]

1.1.1 Open Circuit Television – OCTV

Z anglického překladu otevřený televizní okruh. To ve skutečnosti znamená, že webová kamera vysílá obraz přes veřejnou komunikaci. Tyto kamerové systémy nazýváme také IP kamery, a to díky tomu, že používají ke své činnosti TCP/IP. Jelikož se obraz z těchto kamer vysílá přes počítačovou síť, buď internet, nebo lan, lze ho tak sledovat z kteréhokoliv místa na světě, kde je přístup k internetu. [3]

1.1.2 Video Surveillance System – VSS

Video surveillance system ve zkratce VSS, znamená z anglického překladu dohledový video-systém, dříve známý jako CCTV (uzavřený televizní okruh). Už název svědčí o tom, že se jedná o kamerové systémy, ke kterým lze přistupovat pouze pokud máme k tomuto zařízení přístup (přihlašovací údaje). Právě díky tomu, že k těmto systémům má přístup pouze oprávněná osoba, se tyto systémy používají k zabezpečení objektů. VSS stejně jako OCTV ke své činnosti používají IP – internet protocol, takže jejich záznamy jsou přístupné na internetu, i-když se jedná pouze o přenos, nebo omezený přístup. [3, 4]

Záznamy CCTV lze zpracovávat pomocí PC nebo digitálních rekordérů DVR. Kamery bývají většinou připojeny k monitorům a zařízením, které mohou ukládat video záznam. [3]

VSS je novou zkratkou díky novým přenosovým cestám po IP sítích, jež jsou téměř neomezené. A právě proto se zavedla nová zkratka, jejíž označení je vhodnější než uzavřený televizní okruh. VSS ke své komunikaci používá následující komponenty. [4]

- Kamera
- Přenosová cesta
- Záznamové zařízení
- Zobrazovací zařízení [4]

Obrázek č. 2. – VSS [5]

1.1.3 Web-kamery

Je-li řeč o „web-cams“, neboli web-kamerách, jedná se o kompaktní zařízení, které slouží pro videohovory. Mají jednoduchou konstrukci a způsob zapojení pro užívaní je jednoduchý a nenáročný. [6]

Tyto kamery se často nazývají „webky“, tedy web-kamery, a to z toho důvodu, že web znamená internet a kamera je zařízení snímající obraz. Jde tedy o kameru, která sdílí svůj obraz přes internet.

Obrázek č. 3. – OCTV [7]

1.1.4 Webové kamery

Je zapotřebí rozlišovat webové kamery (IP kamery) od tzn. web-kamer, které jsou k dispozici téměř všude za pár stovek korun. Tyto web-kamery nemají v sobě integrovaný videoserver, jejich funkčnost se zakládá na USB rozhraní a softwaru, ke spuštění je nutností mít počítač, který obsahuje videokartu. [8]

Celkově se webové kamery označují jako VSS (video surveillance system). V dnešní době byla analogová záznamová zařízení nahrazena digitálními. Tento pokrok je znát hlavně v oblasti přenosu signálu a digitalizace videosignálu, proto se začínají prosazovat webové kamery. Webové kamery se připojují drátově či bezdrátově a jejich veškeré nastavení a ovládání lze dělat přes internetové rozhraní. [8]

Kamery mají vlastní IP adresu, běžně v sobě mají už od výroby integrovaný také video-server, který zajišťuje digitalizaci a komprimaci videosignálu. Záznamy webových kamer mají zcela digitální formu, nevyužívají převodníků. Tyto kamery mají v sobě také integrované webové stránky, které umožnují uživateli sledovat střežený prostor z jakéhokoliv místa v síti. (LAN / internet) Proto se používají hlavně při zabezpečení vzdálených objektů. [8, 9]

OCTV, VSS a web-kamery patří mezi kamery dostupné na internetu. Hrozba se tak nachází u všech těchto kamer. Tato bakalářská práce se bude zaměřovat na kamery typu VSS, tedy webové kamery, které slouží k zabezpečení objektů.

1.1.4.1 Software

Existují metody, které umožnují pomocí různých aplikací povolit přístup pro jakékoliv webové kamery. To znamená i do mobilních zařízení, notebooků, tabletů apod. Při lepší znalosti si útočník dokáže prohlédnout záznamy, datumy, kdy byly naposledy uložené a ta více děsivá věc, že může v reálném čase sledovat oběť, může mít před sebou jak živý obraz, tak i najít GPS pozici. [10]

Existují průzkumy, které dokazují to, že v googleplay obchodě a applestore se nachází více než milion malware aplikací, které si denně stahují tisíce lidí. [10]

1.1.4.2 Konfigurace

Je důležité, aby každý, kdo si pořizuje kamerové systémy či jakékoliv zařízení připojené k internetu, dbal na bezpečnost a jeho prvotní nastavení. Spousta uživatelů se domnívá, že se jich to netýká, a ponechávají ve svých kamerových zařízení původní nastavení, do kterého je ovšem velice snadné se dostat při znalosti základních údajů.

Testy, které byly prováděny na velkém množství online kamer, ukazují desítky tisíců webových kamer, které mají stále původní uživatelské přihlašovací údaje. Je potřeba změnit jak uživatelské jméno, tak heslo, aby tyto údaje nebyly snadno dostupné. [10]

1.1.4.3 Rozhraní

Každá webová kamera má možnost grafického nebo jen konzolového rozhraní. Mezi grafické a konzolové rozhraní se zařazuje velké množství rizik spojené s kybernetickou bezpečností. Obecně na grafické rozhraní lze útočit různými způsoby. Úspěšnost takového útoku záleží na zabezpečení zařízení, které používá uživatel k přístupu grafického nebo konzolového rozhraní. Co se týče konzolového rozhraní, existují možnosti přístupu do počítače, ze kterého lze kameru ovládat, například pomocí získání citlivých údajů. Dále útočník může vstoupit do konzolového rozhraní pomocí metody vzdáleného přístupu.

1.2 Rizika

Pojem „riziko“ znamená určitou míru pravděpodobnosti, že hrozba, která negativně ohrožuje aktivum, může nastat a poškodí chráněné aktivum. V tomto případě je aktivum webová kamera, která má určitou zranitelnost, a možnost zneužití této zranitelnosti je hrozba. [11]

U webových kamer existují různá rizika spojená s napadením kamery a jejich záznamů. Jelikož v kybernetickém prostoru se nachází spousta zneužitelných zranitelností a tím pádem i hrozeb jejich zneužití, je už jen to, že přístup k webovým kamerám probíhá přes internet, samo o sobě rizikem.

1.2.1 Základní pojmy

Jeden z nejdůležitějších pojmů spojeným s rizikem, jsou aktiva. Aktiva lze definovat jako majetek, nebo chráněný zájem. Jedná se o jakoukoliv věc, kterou chceme zabezpečit. Zranitelnost je slabina neboli možnost útoku na chráněné aktivum. Hrozba je pak schopnost negativně poškodit chráněné aktivum. [11, 12, 13]

1.2.2 Rizika spojená s kybernetickou bezpečnostní

Rizika v kybernetické bezpečnosti lze chápat jako souhrn nedbalých činností uživatele, instalatéra a hojně i vývojáře rozhraní u kamer, což vede k útokům či zvětšení pozornosti útočníka. Tato rizika a útoky mohou probíhat následovně:

- Útoky na webové stránky, získávání citlivých údajů.
- Vnucení nežádoucích emailů, které následně mohou způsobit škodu v daném zařízení.
- Nelegální stahování souborů, které mohou být nakaženy, vedoucí ke spuštění malware na daném zařízení.

1.2.3 Hrozby spojené s kybernetickou bezpečností

Hrozba, jak už bylo popsáno (viz 1.2.1), je možnost zneužití slabiny aktiv, která vede k negativnímu dopadu chráněného aktiva. [12]

Co se týče kybernetické bezpečnosti, lze zranitelnost a možnosti jejich zneužití popsat jako:

- Defaultní přihlašovací údaje vedoucí k snadné dostupnosti do daného zařízení.
- Slabé přihlašovací údaje vedoucí k rychlému rozluštění a dostupnosti do daného zařízení.
- Nedbalost bezpečnosti či nevědomost z pohledu uživatele, vedoucí k napadení zařízení např. přes phishingové zprávy nebo spamu.
- Stahování a instalace souborů s neověřením jejich bezpečnosti, vedoucí k nákaze zařízení malwarem.

- Nelegální stahování souborů, které jsou většinou nakaženy malwarem.
- Nedbalost uživatele při zabezpečení zařízení připojená k internetu vedoucí k různým typům útoků (záleží o jakou slabinu a zařízení se jedná).
- Nedostatečně zabezpečená zařízení připojená k internetu, vedoucí k různým útokům (záleží o jakou slabinu a zařízení se jedná).
- Nedostatečné zabezpečení sítě vedoucí k snadné dostupnosti do sítě a do zařízením k ní připojené.

1.3 Kybernetická bezpečnost – Terminologie

Kybernetická bezpečnost z anglického slova Cyber Security, je bezpečnost týkající se počítačových sítí. Jedná se o spojitost kyberprostoru s bezpečností. Kyberprostor (Cyber-space) je popisován jako všechen internet a zařízení s ním spojené. Kybernetická bezpečnost se potom týká zabezpečení daného kyberprostoru. [14]

1.3.1 Základní pojmy kybernetické bezpečnosti

V tomto podtématu jsou zahrnuty pojmy spojené s kybernetickou bezpečností a způsoby šíření nežádoucích zpráv, které vedou k napadení zařízení uživatele. Jsou zde popsány hrozby, které by mohly vést k přístupu do webové kamery.

1.3.1.1 Phishing

Phishing od slova password harvesting fishing, znamená sběr hesel rybařením. Phishing je oklamání příjemce falešnou zprávou, bývají to soubory ukryté v obrázcích. Většinou se vyskytují v emailových verzích, příjemce dostane zprávu velice podobnou určité stránce (například zpráva od banky a zároveň žádost o změnu hesla). Email může obsahovat odkaz, na který lze kliknout. Tento odkaz bude odkazovat na stránku podobnou té bankovní a zároveň vyzve k zadání původních přihlašovacích údajů. V tu chvíli webová stránka oskenuje zadané přihlašovací údaje a uloží je do svojí databáze. Phishingům se většinou jedná o získání citlivých informací, tj. v tomto případě přihlašovací údaje. [15]

1.3.1.2 Spam/ham

Jedná se o masově šířené zprávy, a to především o reklamní emaily. V těchto emailech jde většinou o získání citlivých údajů. Na rozdíl od spamu, je zde termín ham, ve kterém se jedná o nežádoucí zprávu určenou pro jednotlivce, kde je obsah jednorázový. [16]

1.3.1.3 Hoax

Hoax nápodobně, jako phishing pracuje na principu falešnosti. Jedná se o šíření zbytečných řetězových reakcí, které nazýváme hoaxy. Tyto zprávy bývají většinou neškodné, ale znepříjemňují adresátovi život. [16, 17]

Princip: Zpráva se tváří, jakože je pravá, ale ve skutečnosti se jedná o podvod. Může se vyskytovat na internetu v podobě stránky, na níž jsme online → vyskočí okno s informacemi o nebezpečí a varování. (Může se tvářit jako antivirový program s vysoce podobným designem.) Poté co vyskočí dané okno → hoax žádá o sdílení a následně se uživatelské zařízení nakazí a sdílí tu samou zprávu prostřednictvím jeho sociální sítě a tímto stylem se rozšiřuje k dalším lidem. [17]

1.3.1.4 Malware

Malware lze definovat jako škodlivý program nebo program, který v sobě skrývá škodlivé brouky. Tito brouci pak posílají údaje na třetí strany. V dnešní době se nejčastěji jedná o hrozbu typu Trojský kůň. [18]

Malware se může nacházet v legálním obchodě, jako je googleplay. Po stáhnutí aplikace nakažené malwarem si aplikace vyžádá práva pro přístup např. k fotografiím, GPS poloze, kontaktům apod. Jakmile aplikaci povolíme přístup k těmto údajům, aplikace je rozešle na třetí strany. Jedná se tedy o únik citlivých údajů. Typy malware mohou vypadat následovně:

Počítačový virus

Počítačový virus lze chápat jako část kódu nebo program, který spustí nežádoucí činnost na PC či jiném zařízení bez vědomí nebo svolení uživatele. Velké množství virů je navrhnuto tak, aby získalo kontrolu nad systémem, který mu podlehl, a spustilo na něm ničivé akce. Počítačový virus se rozšiřuje na stejném principu jako ten biologický, až na to, že k tomu používá síť. [19]

Obrázek č. 4. – Počítačový virus [18]

Tyto viry se mohou vyskytovat v podobě stažených souborů s příponou .exe, prohlížeč .pdf, běžně používané programy apod. Lze ho také získat stažením souboru z internetu, jakmile se spustí daný soubor, spustí se společně s ním i virus, který se následně začne kopírovat do jiných souborů v daném zařízení a začne na něm provádět změny. [19]

Spyware

Už od názvu je zřejmé, že se jedná o verzi malware, která slouží ke špehování uživatelů a získání jejich citlivých údajů, které následně odesílá třetím stranám. Spyware je velice těžké odhalit. Podobně jako počítačový virus se instaluje společně s jiným programem. Lze jej také získat pomocí otevření infikované přílohy z emailů.[20]

Obrázek č. 5. - Spyware [20]

Keylogger

Keylogger je verze spyware, který snímá veškeré otisky prstů na klávesnici. Mohou tak získat veškeré citlivé informace, které v danou dobu uživatel „prozradí“ přihlašováním se do sítí, jako je například internetové bankovnictví. [21]

Jeho získání na zařízení je podobné jako počítačový virus, malware a spyware. Aplikace pro keylogger se najde i ve spoustě firem, ve kterých zaměstnavatelé sledují svoje zaměstnance, jestli dělají svoji práci. Tam však bývá zaměstnanci oznámeno, že se na jeho pracovní notebook instaluje sledovací zařízení.

Trojský kůň

Je to typ počítačového viru, který se jeví jako užitečná funkce, program, který lze stáhnout zadarmo. Místo toho však způsobuje vážné škody a krádeže dat. [22]

Trojský kůň se dostane do zařízení stejně jako počítačový virus. Šíří se často pomocí phishingových zpráv – infikovanými emailovými přílohami, také bývá ukrytý v bezplatných hrách, filmech či hudbě. [22]

1.3.1.5 DDoS

DDoS z anglického překladu Distributed Denial of Service, znamená distribuované odmítnutí služby. Jedná se o masové útoky na jednu konkrétní webovou stránku či IP adresy. Útočníkům jde zejména o zahlcení sítě natolik, aby nebyla zpřístupněna dalším uživatelům. [23]

1.3.1.6 Pojmy související s webovými kamerami

Z výše uvedených pojmů (viz 1.3.1) budou vytknuty ty, které úzce souvisí s napadením webové kamery a jak toho lze dosáhnout.

- Phishing – zjištění citlivých údajů
- Spam/ham – zjištění citlivých údajů
- Malware – zjištění citlivých údajů
    - Počítačový virus – vzdálené ovládání zařízení
    - Spyware – zjištění citlivých údajů
    - Keylogger – zjištění citlivých údajů
    - Trojský kůň – krádež citlivých údajů, zničení software zařízení
- DDoS – nedostupnost kamery, rozhraní

Citlivé údaje zde chápeme z velké části jako přihlašovací údaje k rozhraní webové kamery, a také jako zjištění lokace uživatele.

1.3.2 Rizika spojená s problematikou kybernetické bezpečnosti

Je velice důležité dbát na zabezpečení a protiopatření veškerých zařízení, která mohou být spojená s webovými kamerami. Rizika spojená s problematikou kybernetické bezpečnosti mohou být: krádež citlivých údajů, zavirování a špehování.

1.3.2.1 Krádež citlivých údajů

Krádež citlivých údajů je chápána jako získání přihlašovacích údajů do rozhraní webové kamery. Toto je možné různými způsoby. Tyto způsoby byly již popsány výše (viz 1.3.1) a jedná se zejména o:

- Phishing
- Spam/Ham
- Malware
    - Spyware
    - Keylogger

1.3.2.2 Zavirování

Zavirování může způsobit fatální následky zařízení, jenž je prostředkem ke spojení s webovou kamerou či jeho kamerovým záznamem. Zavirování může poškodit počítač a následně i webovou kameru, která je k němu připojená. Druhá možnost je, že útočník, který vytvořil daný virus, může ovládat danou kameru a sledovat jeho záznamy bez vědomí uživatele. Způsoby poškození zařízení (viz 1.3.1) jsou:

- Počítačový virus
- Trojský kůň
- DDoS

1.3.2.3 Špehování

Špehování může mít za následek zjištění citlivých údajů, tedy přihlašovacích údajů k danému rozhraní, ke kterému lze přistupovat pomocí počítače uživatele. Po zjištění těchto údajů má útočník webovou kameru v plné moci. Způsoby špehování z pohledu kybernetické bezpečnosti mohou být následující (viz 1.3.1):

- Keylogger
- Spyware

Existují také fyzické způsoby k zjištění citlivých údajů, které si uživatel způsobí sám tím, že zadává přihlašovací údaje před další osobou, nebo si údaje ukládá na PC, či píše na papír, který uživateli unikne k třetím stranám. Nezmění-li uživatel přihlašovací údaje dostatečně brzy, další osoba bude mít plný přístup k webové kameře.

1.3.3 Standardy kybernetické bezpečnosti

V kybernetické bezpečnosti se začaly vytvářet standardy v posledních několika letech kvůli rostoucím útokům na citlivé informace, které uživatelé vkládají do svých zařízení, a ta zpravidla bývají připojena k internetu. Uživatelé také vkládají čím dál více a více informací do těchto zařízení, která potřebují být nutně zabezpečena. A tím vznikají větší nároky na informační věrohodnost a bezpečnost. [14]

Jeden z nejdůležitějších směrů kybernetické bezpečnosti je ochrana proti krádeži identity. Podniky a organizace očekávají větší jistotu v počítačové bezpečnosti, protože potřebují chránit know-how firmy, osobní údaje vlastních zaměstnanců či jejich partnerů. Taktéž jako vláda, která potřebuje uchránit důležité informace.[14]

Nejvíce používaný bezpečnostní standard je ISO / IEC 27002. Skládá se ze dvou částí a to: z části 1. BS 7799 a části 2. BS 7799. Tento standard byl vytvořen Britským standardizačním institutem (BSI). V nynější době se nazývá ISO 27001. [14]

1.3.4 Technologie spojená s kybernetickou bezpečností

S každou technologií jsou spojená určitá rizika. Následně se téma věnuje možnostem připojení, komunikaci webových kamer a možnými scénáři útoku na webovou kameru přes tyto komunikační kanály.

1.3.4.1 Sítě

Co je potřeba brát ve velkou úvahu při bezpečnosti webových kamer, je to, jakým způsobem tyto kamery komunikují. Tyto kamery mají v sobě zakomponovanou vlastní IP adresu a vestavěné parametry, které zajišťují komunikační část. Cokoliv spojené s obstaráním komunikace mezi sledováním obrazu přes síť je obsaženo v jednotce kamery, která obsahuje vlastní software, jenž slouží pro webové rozhraní, FTP server, FTP klienta a emailového klienta. Jednotka také vlastní jeden nebo více logických vstupů a výstupů.

Vlastnosti kamer, jako jsou inteligentní analýza obrazu či ovládání programovatelných I/O a komunikace se serverem obstarává řídící procesor (CPU), pamět Flash a DRAM. Každý výrobce vytváří vlastní hardwarové řešení, tudíž u každé kamery od jiného výrobce může být hardwarové řešení vytvořeno jiným způsobem. [2]

Vlastnost těchto kamer, která zajištuje fungování v ethernetové síti, je tak originální, že kamera nepotřebuje další periferní zařízení. Jediné, co ke své funkčnosti potřebuje, je připojení k PC či DVR, které je vybaveno příslušným VMS (Video Management Systém) softwarem. [2]

Každá webová kamera je připojená k internetové síti, typ připojení může být následný:

- Drátové připojení (LAN)
- Bezdrátové připojení (Wi-Fi)

1.3.4.2 Hardware

U webových kamer máme tzn. ethernet rozhraní. Toto rozhraní slouží k tomu, aby kamera měla přístup k internetu. Pokud by byl kabel odpojen, je možné, že kamera ztratí propojení s internetem a přestane správně fungovat. Je potřeba, aby kamera byla umístěna ve vysoké poloze, aby k ní nebyl snadný přístup. Nebo kameru připojit bezdrátově (přes Wi-Fi, pokud to kamera umožňuje), kde je riskantní slabé internetové připojení nebo jeho dostupnost. Ostatně v obou případech je potřeba mít stálé a rychlé internetové připojení.

1.3.4.3 Aplikace

U jakékoliv aplikace určené pro operace s kamerovými systémy je nutné dbát na bezpečnost s ním spojenou. Některé aplikace mohou být uživatelsky přívětivé a mají možnost automatického přihlášení, což je ovšem chyba. Tohle je jeden z riskantních kroků, které lze udělat při manipulaci s kamerovými systémy. Pro větší bezpečnost je potřeba se podívat, zdali aplikace neumožnuje dvoufázové ověření při přihlašování a pokud ano, je lepší ho aplikovat.

1.3.4.4 Operační systémy

Podobné hrozby, jaké jsou u aplikací, existují i u operačních systémů. Pokud se přistupuje ke kamerovým systémům přes počítač, je nutné dbát i na jeho zabezpečení a dodržování omezenosti přístupu k tomuto zařízení.

Existují zde hrozby jako je stažení a spustění malwaru, pokud se malware dostane do zařízení, pomocí kterého je ovládaný kamerový systém, získá tím i přístup do jeho rozhraní. Proto je nutné zabezpečit jak přístup k danému zařízení, tak přístup k aplikaci, která ovládá samotný kamerový systém.

Scénáře útoků mohou být nejen typu staženého malware, a proto je vhodné uvést příklad. Pomocí operačního systému názvem Linux si lze vytvořit script, pomocí nějž je možné vytvořit link, kterým se lze dostat do webových kamer. Funguje to tak, že hacker zašle email v podobě phishingu a oběť, která na link klikne, akceptuje útočníkovi přístup do své webové kamery. [10]

1.3.4.5 Internet of things

Internet of things, zkráceně IoT, je z anglického překladu internet věcí. Jedná se o skupinu fyzických zařízení, která jsou připojena na internet a navzájem mezi sebou dokážou komunikovat.

IoT se dají nazvat inteligentní budovy, ty mají v sobě spoustu prvků, které lze řídit například pomocí ovladače. Všechny možnosti, které poskytuje inteligentní budova domovu jsou propojené, a to počítačovou sítí. Pokud webová kamera nacházející se v této skupině zařízení není dostatečně zabezpečena, pro útočníky je velice snadné dostat se do zbytku IoT v inteligentní budově. Útočník pak může ovládat celou domácnost, a to pouze kvůli chybně nainstalované či nakonfigurované webové kameře.

Stejně tak, jako když se může „hacker“ (útočník) dostat do kamery, může i do IoT a následně tak do kamery. Proto je důležité mít dobře zabezpečená všechna zařízení, která jsou připojená na internet a lze je ovládat.

1.3.4.6 Firewall

Firewall je v překladu bezpečnostní zeď, která slouží k bezpečnosti v síti na principu oddělení přicházejících a odcházejících paket podle určitých pravidel.

Firewall se rozděluje do několika částí:

1. Paketový firewall

Pravidla fungují tak, že firewall je má předem definovaná a to zejména, jaké adresy a porty přicházejí a na jaké adresy a porty mohou jít dál. [24]

2. Aplikační brány

Aplikační brána funguje na bázi dvou spojení:

- Klient (uživatel) se připojí na aplikační bránu, kde aplikační brána vytvoří nové spojení, kde je pak klientem aplikační brána.
- Data, která aplikační brána získá ze serveru, a pak předá klientovi.

3. Stavové paketové firewally

   Pracují stejně jako paketový firewall, jen přidá funkci, která zrychlí filtrování.[24]

4. Stavové paketové firewally s kontrolou protokolů a IDS (Intrusion Detection System – systém pro odhalení průniku)

   Vysoce kontroluje spojení procházejících dat známých protokolů i aplikací. Mohou zakázat vstup http spojení, v němž objeví tunelování jiného protokolu.[24]

1.3.4.7 Hardware firewall

Hardware firewall je samostatné zařízení, na rozdíl od softwarového, který je pouze program. Principově jsou na tom stejně.

1.3.4.8 IDS/IPS

IDS z anglické zkratky Instrusion Detection System, znamená systém pro odhalení průniku. Kontroluje spojení mezi procházejícími daty známých protokolů i aplikací. [24]

IPS z anglické zkratky Instrusion Prevention Systems, znamená systém prevence průniku. Dokáže sledovat škodlivou činnost operačního systému a rozpoznat ji, zaznamenat informace a zablokovat. Ke svojí činnosti používá odhalení protokolových anomálií. IPS může být využit v rámci celé sítě, nebo jen operačního systému (OS). [25]

1.3.4.9 Zálohovací zařízení

Jedná se o zařízení určené k ukládání aktuálních dat a informací za účelem jejich archivaci pro následující použití. Může se jednat o harddisky, USB Flash Disky, CD, DVD a jiné přenosové zařízení s určitou kapacitou vůči zachovávaným datům. Zálohovací zařízení mohou sloužit pro zachování kamerových záznamů po určitou dobu. Existují možnosti uchovávání dat pouze po určitou dobu např. 24 hodin, data se po překročení limitu kapacity přemazávají a znovu nahrávají nový záznam.

1.3.4.10 Zařízení pro přenos

Zařízení pro přenos nazývaná jako tokeny, též jako „Flash disky“. Mohou sloužit pro záznam identifikačních klíčů, kde je lze využít jako ověření identity jedince. Identita též bývá chráněna pomocí hesla. Pokud dojde k odcizení tokenu bez použití hesla, lze se snadno dostat do systému. [24]

1.3.4.11 Webové kamery

Tím, že je kamerový záznam uchováván v internetové podobě, nebo jeho přístup je přes internetové rozhraní, k sobě přitahuje velké množství rizik spojené s kybernetickou bezpečností. S tím úzce souvisí hardwarové řešení a možnosti připojení k internetu. Aby kamera dobře fungovala a byla zde možnost připojení přes internet, je nutné kameru kvalitně nainstalovat a zabezpečit její přístup k internetu.

Pro bezpečný chod kamerových systémů je nutné dbát na kvalitní konfiguraci aplikací, pomocí níž se uživatel připojuje do kamerového systému, totéž platí i pro zabezpečení tohoto zařízení. Počítač je cílem útoků ze všech stran, a tak je potřeba dbát na jeho správné zabezpečení. Útočník se může dostat ke kamerovým záznamům přes zavirovaný počítač, a to pouze z nedbalosti z pohledu uživatele. To samé platí i u IoT, jakékoliv zařízení připojené k internetu v domácnosti je potřeba mít pod ochranou, existuje spousta možností přístupu přes IoT do sítě a pak do kamerových systémů.

Je důležité mít správně nastavený firewall, aby byl přístup do webové kamery stěžejní. Co se týče hardware firewall, může se jednat o prevenci proti útokům, či zlepšení zabezpečení sítě, ve které je webová kamera připojena.

Existují stavové paketové firewally s kontrolou protokolů a IDS, které slouží pro odhalení průniku. IDS umožnuje lepší zabezpečení systému webové kamery společně s IPS, které slouží pro prevenci napadení operačního systému.

Zálohovací zařízení jsou důležitá pro běžný chod kamerových systémů, pro ukládání kamerových záznamů a spolehlivost uložení jejich dat.

Další důležitá věc je to, aby lidé dbali na opakovanou změnu defaultních přihlašovacích údajů ke své kameře. Když tyto údaje nezmění, do kamery se může dostat kdokoliv a změnit tak přihlašovací údaje, nastavení kamery, v horším případě sledovat a odposlouchávat okolí.

2 ZRANITELNOSTI

Pojem zranitelnost se používá pro označení slabiny chráněného aktiva (zranitelnost je vlastností aktiva), tedy webové kamery nebo jejího rozhraní. Na zranitelnost působí hrozby, což znamená riziko, které je potřeba eliminovat, nebo utlumit tak, aby zranitelnost nemohla být lehce zneužita. V kybernetické bezpečnosti se může jednat o: [26]

- HW chyba serveru, kde jsou zálohované kamerové záznamy
- Nezabezpečený server, kde jsou zálohované kamerové záznamy
- Nezabezpečené rozhraní webové kamery
- Slabé heslo
- Implementovaná chyba
- Defaultní nastavení konfigurace
- Defaultní přihlašovací údaje
- Možnosti špionáže

V této části jsou rozepsány možné scénáře útoků z pohledu útočníka na zranitelnosti webových kamer a jejich samotné zranitelnosti z pohledu jak software, tak hardware.

2.1 Zranitelnosti webových kamer

Z programátorského hlediska se jedná o chybu, která se nachází v hardware nebo v software zařízení a způsobí tak bezpečnostní problém. Většinou jsou tyto chyby zneužity pro ovládnutí domácí počítačové sítě nebo pouhé sledování a zjištění soukromých informací, které bývají následně zneužity. [27]

Příklady využití webových kamer:

- Sledování dopravy
- Průběh stavby
- Zpravodajství týkající se zimních středisek
- Sledování počasí v různých krajinách
- Turistické akce
- Dětské chůvičky
- Sledování mobilních zařízení
- Sledování obchodů a pracovních míst
- Zabezpečení objektů

2.1.1 Nastavení konfigurace

Nastavení konfigurace, tedy změna uživatelského jména a hesla je nejdůležitější část při přidání nové kamery do domácnosti. Spousta lidí na tuto skutečnost příliš nedbá a tím riskují, že se do jejich sítě někdo může dostat. Při nedbalosti u nastavení konfigurace se může pachatel dostat nejen do kamery, která sleduje domácnost, ale také do celé sítě.

2.1.1.1 Defaultní nastavení konfigurace

Už jen to, že někdo nechá defaultně nastavenou kameru na přihlašovacích údajích od výrobce, publikuje snímanou scénu veřejně na internet. Dřív nebo později se do zařízení někdo dostane, buď pachatel nebo tzv. roboti, kteří jsou například u serveru shodan, který funguje na určitém algoritmu, který zkouší každé zařízení připojené k internetu a když má dané zařízení otevřený port, shodan zjistí, o jaké zařízení se jedná. Získá jeho informace a přidá ho do své databáze internetových zařízení. Uživatelé shodanu pak mohou sledovat snímanou scénu z dané kamery. [28, 29]

Pro další dohledání a dodatečné zobrazení kamer nám slouží google. Při znalosti základních parametrů inurl, intitle a webového rozhraní různých výrobců, lze tak dohledat další kamery. Link vypadá následovně: inurl:view/viewer_index.shtml [28, 30]

Kde view/viewer_index.shtml je webové rozhraní výrobce webových kamer. Při vložení tohoto linku do vyhledávače google, vyskočí různá kamerová zařízení, které si lze prohlédnout. Už jen daná situace, že lze zobrazit tyto snímané scény z kamery je zranitelnost, jíž je nutné zamezit. [28, 30]

Dalším serverem pracujícím podobně, jako je shodan se nazývá Insecam. Důvodem vytváření těchto serverů je upozornit majitele na to, že jejich zařízení nejsou bezpečná a měli by s tím něco dělat. Insecam funguje na principu, že eviduje do své databáze málo zabezpečené soukromé webkamery, které mají povolený anonymní přístup z internetu. [28, 31]

2.1.1.2 Nedostatečné heslo

Existuje spousta programů, které slouží pouze k tomu, aby se dostaly do nedostatečně zabezpečeného zařízení, jako je webová kamera. Tyto programy mohou fungovat pomocí metody brutte force attack, což je analytický test pro vyzkoušení všech možných nastavení klíče a vyhodnocení, zda byl nalezen ten správný. Některé programy mohou fungovat na principu, že zkoušejí všechna hesla, která byla již prolomena, ty se nachází ve zveřejněné databázi.

2.1.1.3 Implementovaná chyba

Implementovaná chyba je negativní vlastnost zařízení, která může být zneužita hrozbou. Tyto chyby jsou vestavěné v zařízení od výrobce. Implementovaná chyba někdy umožňuje snadnější přístup k webové kameře, toho pak útočník dokáže zneužít v jeho prospěch.

2.1.2 Zálohování kamerových záznamů ve virtualizovaném prostředí

Zálohování ve virtualizovaném prostředí se může nacházet na firemních či domácích serverech. Jde zde o situaci, kdy někteří majitelé firem či bezpečnostní manageři podceňují bezpečnost týkající se kvalitního a aktuálního zabezpečení. Chyba, která se ve firmách stává často, je, že dostupnost k serverům není obtížná. Dostane-li se neoprávněná osoba do této místnosti, může napáchat fyzické škody na daném serveru. Nemusí se ovšem jednat pouze o fyzickou poruchu, znalejší člověk může napáchat v serverovně i jiné negativní škody. Např. Vložení malware do serveru, přenastavení serveru, vyjmutí kamerového záznamu, dostupnost ke kamerovému záznamu.[32]

Dalším problémem zde může být špatná konfigurace firewallů a neaktualizovaný software. Pro příklad: Antivirové programy, ty je vždycky potřeba mít v aktuální verzi, server je může aktualizovat automaticky a tím snižuje výkonnost serveru po určitou dobu. Pokud jsou ochrany serveru zastaralé, mohou je pak útočníci využívat po delší dobu.[32]

2.1.3 Wi-Fi

Jedná se o typ počítačové sítě, ve které jsou informace přenášeny pomocí elektromagnetických vln, nikoliv kabelem. Jádrem každé Wi-Fi sítě je přístupový bod (Access Point = AP) např. router. Jedná se o zařízení, které komunikuje s dalšími zařízeními v síti. MAC adresa je tzn. Media Access Control, u níž první 3 byte identifikují výrobce, který přiděloval adresu a další 3 byte jsou přidělovány výrobcem jakýmkoliv způsobem.

Wi-Fi je jedna z možností, jak se dostat do IoT v jakémkoliv objektu. Je nutné dbát na zabezpečení konfigurace spojené s internetem, stejně jako k webové kameře. V případě, že útočník prolomí heslo v routeru, uvidí pak další zařízení v dané síti.

- V případě, kdy webová kamera neobsahuje žádné heslo, útočník nad ní převezme svoji kontrolu hned po prolomení přístupu k Wi-Fi síti.
- V případě, kdy webová kamera obsahuje defaultní heslo, stačí si jej vyhledat v již existujících databázích hesel na internetu.

- V případě, kdy se v kameře nachází implementovaná chyba, způsobí možnosti zneužití k snadnější dostupnosti do webové kamery.

V případě, kdy se útočník dostane ke kameře přes Wi-Fi, může sledovat provoz kamery, ale k jejímu ovládání bude mít omezený přístup. Toto je scénář, kdy útočník neprolomil heslo od webové kamery, pouze Wi-Fi sítě.

2.1.3.1 Bezpečnostní opatření pro Wi-Fi síť

- Umístnění AP do středu budovy
- Dávat pozor, aby AP nebyl poblíž oken
- Pokrytí Wi-Fi sítě by nemělo dosahovat dál, než je zeď a okna budovy
- Důležité jsou také pravidelné prohlídky
    - Kontrola signálu vně budovy
    - Kontrola, zdali se nenachází v síti neschválené AP
- Omezit připojení MAC adres
    - Provádět aktualizaci
- Omezit nebo vypnout DHCP (Dynamic Host Configuration Protocol) = automatické přiřazování statických IP adres
    - Při omezení DHCP omezit přidělování IP adres jen na počet zařízení, které využívají Wi-Fi.[33]

2.1.3.2 Ochrana proti přístupu k lokální síti

- Nedát možnost útočníkovi vejít do daných prostor s přístupem k internetu.
- Nedávat heslo od Wi-Fi neoprávněné osobě.
- Zabezpečit místo, kde je možné se připojit kabelem, vůči neoprávněným osobám.
- Zabezpečit router
- Mít kvalitní heslo k přístupu do zařízení v této síti
- Mít kvalitní heslo k přístupu do routeru

2.1.4 Rozhraní

Každá kamera má svoje vlastní rozhraní. Webovou kameru lze po autorizovaném přihlášení ovládat z internetového prohlížeče. Při nesprávném nastavení pak může rozhraní kamery obsahovat následující zranitelnosti.

2.1.4.1 Cross site scripting (XSS)

Z pohledu webové stránky, na které je umístěno veškeré ovládání kamery, jsou zde rizika, která majitel kamery neovlivní. Jedná se o chyby ze strany programátora, který vytvářel dané webové rozhraní. Útočník zabývající se tzn. cross site scripting může tyto chyby zneužít a připsat si zde vlastní script.

Cross site scripting je metoda, pomocí níž útočník narušuje webovou stránku využitím nedostatečného zabezpečení webové stránky – chyby ve skriptech, kódech. Využívá se zejména v neošetřených vstupech. [33]

Prvním krokem je, že útočník hledá chyby na jednotlivých internetových stránkách. Po nalezení chyby v některém z kódů webové aplikace si útočník vytvoří vlastní kód a zavede ho do této aplikace. Pomocí tohoto kódu pak může způsobit škody, například získání citlivých údajů, phishing, znefunkčnění stránky apod. [33]

K útokům pomocí cross site scripting se používá programovací jazyk JavaScript. Bezpečnostní protiopatření ze strany uživatele může být vypnutí JavaScriptu ve webovém prohlížeči. Ze strany výrobce kamery:[33]

- Dělání penetračních testů
- Kontrola kódu použitého na webovém rozhraní
- Po zjištění zranitelnosti opatřit, aby útok nadále nebyl umožněn

2.1.4.2 Injekce

Injekce je typ zranitelnosti, která funguje na principu, že útočník vloží nežádoucí data do nezabezpečeného kódu, a tím způsobí, že interpret začne vykonávat příkazy a posílat nežádoucí data bez řádné autorizace. Interpret je program, který umožnuje vykonávat zápis jiného programu v jeho zdrojovém kódu ve zvoleném programovacím jazyce. [34]

V případě rozhraní webové kamery by tento útok mohl způsobit, že útočník se do webového rozhraní dostane bez kvalifikované autorizace.

2.1.4.3 Nefunkční autentizace

Nefunkční autentizace se často nachází ve webových aplikacích, a to zejména jako implementovaná chyba, nebo nedostatečně vytvořený(zabezpečený) kód. Zneužití této zranitelnosti může způsobit převzetí kontroly nad databází uživatelských účtů nebo celého systému.[34]

2.1.4.4 Nezabezpečení citlivých dat

Jedná se o nedostatečně zabezpečený přenos a uchovávání citlivých dat, tedy použití slabých šifrovacích algoritmů. Toto může vést k jejich krádeži a následnému zneužití či jejich změnění.[34]

2.1.4.5 XML External Entities (XXE)

Jedná se o možnost upravování či jakékoliv ovlivnění XML obsahu na webové aplikaci a s tím spojené hrozby typu DDoS/DoS útoků. Tato zranitelnost také umožnuje útok typu cross site scripting (viz 2.1.4.1) a také injekci (viz 2.1.4.2), zranitelnost typu SQL Injekce může vést k zneužití útočníkem, který má možnost vymazat/upravit veškerou databázi či dotazovat se na citlivé údaje spojené s rozhraním webové kamery. [34]

2.1.4.6 Nefunkční kontrola přístupu

Při nesprávně zabezpečené kontrole přístupu může dojít k tomu, že bude zneužita útočníkem k zjištění citlivých údajů. [34]

2.1.4.7 Použití známých zranitelných komponent

Komponenty, chápány jako knihovny, frameworky apod. ve většině případů běží s nejvyššími oprávněními. Pokud tento komponent obsahuje zranitelnost, která je zneužita, může to vést k velkému úniku dat či převzetí kontroly nad celým serverem. Rozhraní, které používají již velmi známé zranitelnosti, se nachází v rizikové oblasti a mohou umožnit spousty útoků a negativních dopadů. Veškeré ovládání a snímky kamery by tak padly do rukou útočníka. [34]

2.1.4.8 Nedostatečné testování

Nedostatečné testování, tak jako všude, může způsobit nevědomost o útočníkovi, snažícího se aplikovat plánovaný útok ve webové aplikaci. A taktéž při nedostatečném testování je vyšší pravděpodobnost výskytu zranitelností, které mohou útočníci zneužít k jejich prospěchu. Je potřeba, aby vývojáři průběžně prováděli penetrační testy, aby omezili možnost útoků na webové rozhraní kamer. [34]

2.1.4.9 Nedostatečně zabezpečené přesměrování

Pokud webové rozhraní kamery používá při přihlašování k ovládání kamery přesměrování na jinou stránku, mohou tak útočníci tohoto zneužít a přesměrovat uživatele na

stránky typu phishing. Uživatelé tak předají své přihlašovací údaje útočníkům, aniž by si toho všimli. [34]

2.1.5 Připojení kabelem

Připojení k internetu je nutné pro vzdálený přístup ke kamerovému systému. Tuhle funkci používá téměř každý, kdo si pořídí IP kameru. V kybernetické bezpečnosti se tak odvíjí rizika s tímto spojená.

Fyzické ohrožení kamery spočívá v přeříznutí kabelů vedoucích do kamery, což způsobí znemožnění téměř veškerého přístupu do webové kamery. Tyto zranitelnosti nezasahují do kybernetické bezpečnosti, a proto dále nebudou zmiňovány.

2.1.6 Operační systémy

Nachází-li se veškeré zpracování kamerových systémů na PC, existují zde možné scénáře pro útočníka, které by mohly ohrozit kamerové záznamy či přístup k samotné kameře.

2.1.6.1 Neaktualizované antivirové programy a firewall

Stejně jako u všech zařízení, které potřebují ochranu, je nutné pravidelně aktualizovat antivirové programy a firewall. V případě, kdy se pokouší útočník dostat do počítače majitele webové kamery, se může stát, že antivirový program v rozpoznávání útočníka selže a nevykáže žádnou činnost. V případě, kdy antivirové programy a firewall jsou dlouhodobě neaktualizované, útočník může mít nad zařízením moc po celou tuto dobu.

Existují i případy, kdy uživatelé nezajistí žádnou antivirovou ochranu na svém zařízení, a tudíž je pro útočníka po ovládnutí tohoto zařízení snadné i získat přístup pro ovládání webové kamery. To ovšem závisí na tom, zda majitel použije kvalitní heslo do rozhraní k webové kameře, nebo slabé až žádné heslo.

2.1.6.2 Malware

Při omylném stažení počítačového virusu či trojského koně do počítače při nedostatečně zabezpečené lokální síti a počítače se může stát, že útočník ho bude moct vzdáleně ovládat. V případě, kdy majitel kamery používá aplikaci pro kamerové systémy z daného počítače s automatickým přihlašováním, útočník získá okamžitě přístup do kamery a její nastavení. V případě, kdy by majitel měl zaheslované přihlašování s nedostačujícím heslem,

by útočník použil programy pro prolomení hesel a po delším čase by přístup do kamery stejně opět získal. Další časté zranitelnosti při tomto ději bývají ukládání hesel do PC. Jakmile nad ním útočník převezme kontrolu, může si na něm najít uložené přihlašovací údaje a opět má snadný přístup ke kamerovým záznamům a jejich konfigurací.

Typ spyware, který pomůže útočníkovi získat citlivé informace,se nazývá keylogger (viz 1.3.1). Již zmíněný program, který zachytává stisknuté klávesy. Při přihlašování do rozhraní webové kamery tento program naskenuje stisknuté klávesy a útočník získá přístup do webové kamery, aniž by musel ovládat majitelův počítač.

Stejně jako nepozornost při stažení malware do počítače může mít neopatrné zacházení při prohlížení pošty katastrofální následky. Od toho tu jsou metody k získávání citlivých údajů s názvem phishing, spam a ham (viz 1.3.1). Při nedostatečné opatrnosti může útočník získat informace, které mu pomohou získat i dostupnost k přihlášení do webové kamery.

2.1.6.3 Fyzický přístup k PC

Podobně, jako kvalitní zabezpečení pro síť, je potřeba dávat si pozor na neoprávněný přístup fyzické osoby k používanému notebooku, nebo PC. Může se stát, že majitel kamery odejde od svého počítače, na kterém běží v pozadí rozhraní webových kamer a zapomene jej uvést do režimu spánku, kdy uživatel musí zadat heslo k přístupu do PC. Neoprávněná osoba toho zneužije a získá přístup do kamery a její veškeré konfigurace.

V dalším případě se může stát, že přístup je sice zaheslován, avšak majitel si nechává heslo napsané na papíře, které má přímo u svého PC, nebo uložené ve svém počítači. Pak je opět jasné, že neoprávněná osoba získá bezproblémový přístup ke kamerovým záznamům.

Při větší znalosti a zákeřnosti neoprávněné osoby, která se dostala k fyzickému počítači, ze kterého se ovládají kamerové systémy, je možnost, že útočník nahraje vlastní malware do počítače, pomocí nějž může majitele špehovat a následně zjistit přihlašovací údaje, které majitel používá k přístupu do rozhraní webové kamery, což povede k tomu, že útočník získá neomezený přístup ke kamerovým systémům, dokud majitel nezmění přihlašovací údaje.

2.1.7 Kybernetickou bezpečnost dělíme na několik fází

*„**Fáze č. 1 - Ochrana proti vniknutní "zvenčí"***

Jedná se o zapojení firewallů a antivirových programů do sítě. Tyto služby dokáží odfiltrovat většinu případných útoků, jež přichází z venkovního prostředí firmy. [35]

Fáze č. 2 - Ochrana proti únikům dat "zevnitř"

Výše uvedené služby neochrání společnost ze strany jejich zaměstnanců a návštěvníků. K tomuto slouží různé monitorovací a další systémy, jež zamezují například vynesení dat z budovy. [35]

Fáze č. 3 - Zálohování dat

Další částí kybernetické bezpečnosti je zálohování dat pro případ výpadku systémů či externího vlivu – například požáru. [35]“

3 VÝBĚR VHODNÝCH PROSTŘEDKŮ PRO TESTOVÁNÍ WEBOVÝCH KAMER

Tato kapitola je zaměřená na vysvětlení pojmů spojených s testováním zranitelností webových kamer a popis nástrojů sloužících k testování zranitelností. Popsané termíny a nástroje se boudou vyskytovat nadále v praktické části.

3.1 Slovník spojený s testováním zranitelností webových kamer

Tato část se zaměřuje na vysvětlení pojmů spojených s testováním zranitelností webových kamer a jejich využití. S těmito termíny se bude dále pracovat v praktické části této bakalářské práce.

3.1.1 Defaultní přihlašovací údaje

V kapitole defaultní nastavení konfigurace (viz 2.1.1.1) je blíže popsána situace spojená s defaultně nastavenou konfigurací, úzce související s defaultními přihlašovacími údaji. Znamená to, že majitel kamery ponechal nastavení přihlašovacích údajů podle výrobce, kdy je snadné si dohledat uživatelské jméno i heslo.

3.1.2 Slabá hesla

Situace je podobná, jako při užívání defaultního nastavení přihlašovacích údajů. Slabá hesla jsou snadněji prolomitelná, než dlouhá a silná s využitím speciálních znaků a velkých/malých písmen. Slabé heslo může také znamenat heslo, které bylo již prolomeno a jejich databáze prolomených hesel byla zveřejněna. Slabé heslo znamená zranitelnost k dostupnosti webové kamery. Tuto zranitelnost popisuji blíže v kapitole nedostatečné heslo (viz 2.1.1.2).

3.1.3 Python

Python je v IT sektoru programovací jazyk, který bude využit při vytvoření scriptu v robot frameworku, pro testování vybraných zranitelností webových kamer. [36]

3.1.4 Structured Query Language – SQL

Už od názvu je známo, že SQL je strukturovaný dotazovací jazyk. Tento jazyk je používán k manipulaci s databázemi. [37]

3.1.5 Rozhraní kamery

Webová kamera může mít různá uživatelská rozhraní, které si určí výrobce webové kamery. Rozhraní celkově může mít více významů, a to např. webová aplikace, uživatelské rozhraní, API, ABI, GUI. Tyto pojmy jsou vysvětleny v následujících podkapitolách.

3.1.5.1 User interface – Uživatelské rozhraní

Je chápáno jako software, který je přizpůsoben ke komunikaci mezi uživatelem a zařízením s kterým uživatel potřebuje komunikovat. [38]

3.1.5.2 Webová aplikace

Webovou aplikaci lze chápat jako stránku v prohlížeči, pomocí níž přistupujeme k webovým kamerám. Většina webových aplikací je tvořena tak, aby byl uživatel omezen o některé funkce, které např. u API může ovládat. K vytvoření webové aplikace se většinou používají jazyky HTML, JavaScript a XMLHttpRequest, který využije webová aplikace ke komunikaci mezi serverem a klientem pomocí protokolu HTTP. [39]

3.1.5.3 Application Programming Interface – API

API je rozhraní, pomocí nějž lze programovat další aplikace. API obsahuje další funkce, jako např. různé knihovny. Tato knihovna programátorovi slouží k využití a pomoci při programování jeho aplikace. Funkce jako jsou knihovny programátor používá, aby jej sám nemusel programovat. [40, 41]

3.1.5.4 Application binary interface – ABI

ABI je nízko-úrovňové rozhraní, které obsahuje soubory pravidel, podle kterých zkompilovaný program může dále fungovat beze změn na veškerých systémech, jež obsahují kompatibilní ABI. ABI zařizuje spolupráci mezi procesy a jádrem operačních systémů. [41]

3.1.5.5 Graphical User Interface – GUI

GUI už od názvu představuje grafické uživatelské rozhraní, pomocí něhož je zařizována komunikace mezi uživatelem a zařízením pomocí grafických prvků, jako jsou např. menu, pole pro přihlášení, obrázky, tlačítka apod. [42]

3.1.6 Network Maper – Nmap

Nmap je bezpečnostní skener portů, který se používá k hledání hostitelských počítačů a služeb na počítačové síti. Z Nmap už od anglického názvu vyplývá, že se jedná o vytvoření mapy sítě. Ke své činnosti využívá speciálně upravené pakety a analyzuje odpovědi. [43]

Vlastnosti

- Zjištění otevřených portů ve více zařízeních
- Identifikace služeb, které běží na těchto portech
- Identifikace operačního systému, který běží na daných portech
- S funkcí NSE lze interaktivně komunikovat s daným systémem.

Použití

- Audity služeb a OS v PC sítích
- Správa sítě
- Penetrační testování a bezpečnostní audity
- Zmapování sítí

3.1.7 Security Headers

Security Headers jsou bezpečnostní HTTP hlavičky, jež upravují pravidla pro bezpečnou komunikaci mezi prohlížečem a serverem. V následujících podkapitolách budou popsány typy bezpečnostních HTTP hlaviček. [44, 45]

3.1.7.1 HTTP Strict Transport Security – HTTPS

HTTP Strict Transport Security, též nazývaný jako HSTS, nebo HTTPS je hlavička sloužící pro bezpečnou komunikaci mezi prohlížečem a serverem pouze a jen pomocí protokolu HTTPS. Tato hlavička se používá zejména k ochraně před útoku typu „man in the middle“. Hlavička určuje, aby prohlížeč následných několik sekund přistupoval na webové stránky pouze přes HTTPS protokol. Pro odsouhlasení hlavičky je nutné si požádat o důvěryhodný SSL certifikát. [45]

3.1.7.2 Content Security Policy – CSP

Content Security Policy, dále jen CSP je hlavička, která se věnuje tomu, co vše za soubory může být nahráno do webových stránek a jakým způsobem. CSP slouží pro zabez-

pečení stránek proti vkládání škodlivých funkcí a způsobením útoků typu „cross site scripting“ nebo například „SQL Injection“, tedy celkově útokům typu „XXE“ (viz 2.1.4.5). Jedná se o zablokování vkládání např. obrázků, skriptů, fonty, media apod. CSP má velký obsah pravidel, podle kterých se řídí. Pokud načítaný obsah nevyhovuje těmto pravidlům, je zablokován a vypíše chybovou hlášku. [45]

3.1.7.3 X Frame Options – XFO

X Frame Options, dále jen XFO je hlavička zakazující vkládání webu a jeho částí do jiných webů. XFO ochraňuje uživatele před útoky typu „Injection“ či „Pishing“ a preventivně zabraňuje zneužití vlastního obsahu na jiné weby. [45]

3.1.7.4 X-Content-Type-Options – XCTO

Tato hlavička kontroluje nastavení formátu zdrojových souborů, zdali jsou správné. Dává příkazy prohlížeči, aby si nejdříve ověřil, jestli je správně nastavený MIME ve zdroji. Tento typ hlaviček zabraňuje útokům typu „XXE“ (viz 2.1.4.5). MIME je zde chápáno jako typ internetového media. [45]

3.1.7.5 X-XSS-Protection – XXP

XXSS Protection, ve zkratce XXP se používá pro nastavení konfigurací XSS filtrů, které se nacházejí v prohlížeči. Používá se proti útokům typu „XSS“ (viz 2.1.4.1). Při dobře zabezpečených vstupech v aplikaci slouží hlavička jako další vrstva bezpečnosti proti těmto útokům. [45]

3.1.7.6 Referrer-Policy – RP

Hlavička Referrer Policy, ve zkratce RP umožňuje omezit hodnoty v záhlaví Referrer. Tato hlavička byla vytvořena za účelem nabídnout větší bezpečnost. Lze použít proti útokům typu „XSS“ (viz 2.1.4.1). Při správném nastavení může tato hlavička chránit před identifikací uživatele na sociálních sítích, když sdílí jednotlivé odkazy. [45]

3.2 Nástroje pro testování zranitelností webových kamer

Tato část popisuje funkčnost nástrojů pro testování zranitelností webových kamer, jejich možnosti a využití. Nachází se zde Kali linux, SPARTA, Shodan, SSL Labs, Robot framework, OWASP ZAP a VMware.

3.2.1 Kali linux

Kali linux je linuxová distribuce, která byla vytvořena na základě operačního systému linux. Kali linux se zaměřuje na provedení penetračních testů. Pro testování zranitelností webových kamer bude nainstalován v programu VMware, kde budou následně použity jeho funkce. [46, 47]

3.2.1.1 SPARTA – Legion

Legion, dříve známý, jako SPARTA je GUI pro jazyk python. Jedná se o nástroj, který pomáhá při penetračním testování síťové infrastruktury. Šetří uživateli čas tím, že zobrazuje výsledky pohodlným stylem a uživatel se tak může více soustředit na výsledky než samotné nastavování parametrů, které jsou k tomu potřebné. [48]

3.2.2 Shodan

Shodan (viz 2.1.1.1) jak již známo je webová aplikace, která se věnuje nedostatečně zabezpečeným zařízením, která se nacházejí na internetu. Pomocí této aplikace budou vyhledávány jednotlivé webové kamery a bude zjišťováno, jaké kvality jsou jejich zabezpečení. [29]

3.2.3 SSL Labs

SSL Labs se věnuje kvalitě zabezpečení zařízeních, které jsou dostupné na internetu. Je to webová aplikace, která se používá při zjišťování kvality připojení, šifrování a kvality nastavení konfigurace jednotlivých zařízení. [49]

3.2.4 Robot framework

Jedná se o testovací nástroj napsaný v jazyce Python, lze ho využít i v jiném jazyce. Tento nástroj bude použit při vytváření a spouštění softwarového testu. [50]

3.2.5 OWASP ZAP

Open Web Application Security Project (OWASP) Zed Attack Proxy (ZAP) je testovací nástroj, který slouží pro automatické zjištění určitých hrozeb v softwarové aplikaci. Tento nástroj také obsahuje vysoce výkonný API, který umožní uživatelům větší možnosti, co se desktopového rozhraní týče. [51]

3.2.6 VMware

VMware je produkt společnosti VMware Workstation. Jedná se o program, který umožnuje virtualizaci jednoho nebo více počítačů v jediném hostitelském počítači. Lze do něj nainstalovat různé operační systémy a jiné verze, než které se nacházejí na hostitelském PC. Díky tomuto programu je možné testovat různé virové hrozby a dělat penetrační testy bez možnosti ohrožení vlastního počítače. Do VMware bude nainstalován Kali linux, v němž bude probíhat testování zranitelností spojených s webovými kamerami. [52, 53]

II. PRAKTICKÁ ČÁST

4 APLIKACE ZJIŠTENÝCH INFORMACÍ NA TESTOVÁNÍ WEBOVÉ KAMERY

V této praktické části bylo cílem zaměřit se na testování vybraných webových kamer na webových stránkách pro zjištění chybějících bezpečnostních hlaviček. Další testování probíhalo v nástrojích operačního systému kali linux, ve kterém byla testována jedna webová kamera.

4.1 Testování IP kamery

Kamera pro testovací prostředky se jmenuje Day/Night Surveillance Camera. Její popis je následující:

- Model: TL-SC3171.
- Power: 12 V DC 1 A.
- Default settings: User: admin Password: admin
- SN: 112CD101484
- MAC: 940C6DB0796E

Postup při zavedení kamery do provozu

Pro zapojení kamery byl použit switch, který byl zapojen do routeru. Další síťový kabel byl zapojen ze switche do kamery a další do PC. Napájecí kabel jak ze switche, tak z kamery, byl zapojen do zdroje elektrického proudu.

Obrázek č. 6. – Switch - zapojení

Obrázek č. 7. – Zadní strana kamery – zapojení

Pro rozhraní typu GUI bylo potřeba stáhnout instalační soubor z internetu – link : https://www.tp-link.com/cz/support/download/tl-sc3171/?fbclid=IwAR3AZuOC-KarR3mTR7y8NTiVi92IVPPzfL1buSWuoBDQPsdWR-OzpV5w4n-0#Utility.

Jelikož kamera byla dříve používaná v laboratorních pracích, přístupové údaje byly pozměněny. Tudíž bylo potřeba provést reset kamery, který lze vidět na obrázku č. 7. v levé zadní části kamery. Následně po resetu fungovaly defaultní přihlašovací údaje, tedy user: admin, password: admin. Kamera se připojila na lokální IP adresu a připojit se k webovému rozhraní šlo tedy pouze z dané místní sítě. IP adresa: 192.168.100.238

4.1.1 Soupis vlastností z pohledu bezpečnosti

Klady

- Kamera nemá možnost připojení pomocí VPN.

Zápory

- Webové rozhraní stránky není zabezpečeno protokolem Https.
- Webová stránka nemá platný certifikát.
- Kamera používá zastaralý software/firmware
- Většina nastavení kamery nefunguje přes jiné prohlížeče, než je Internet Explorer
- Rozhraní kamery nepodporuje žádné dvoufázové ověření

4.1.2 Možné scénáře útočníka a jejich protiopatření

IP kamera byla v testovacím prostoru zapojena do lokální sítě, což znamená, že z jiné sítě se nelze připojit přímo do kamery. Šlo by to tehdy, kdyby měl útočník vzdálený přístup k zařízení, pohybující se v této lokální síti. Příklady zneužití můžou být např. vzdálená plocha nebo VPN. Jelikož kamera nepodporuje připojení VPN, není zde hrozba připojení do kamery přes její server. VPN by v tomto případě hrozilo pouze tehdy, pokud by se útočník dostal přes VPN (jiného zařízení) do lokální sítě, ve které je kamera připojena. Má-li útočník přístup k lokální síti pomocí vzdáleného přístupu, má tím i přístup ke kameře, která je na této síti umístěna.

V tomto případě lze chránit počítač tak, že je nutné, abychom vždy byli opatrní při stahování souborů a složek. Je zde nutná snaha o pasivní i aktivní zabezpečení zařízení připojených na internet. Pokud zařízení umožnují dvoufázová ověření, tak jej aplikovat. Hraje zde velkou roli tzn. lidská hloupost a také nevědomost. Hrozby mohou přijít z jakékoliv sociální sítě, či si je lze způsobit samotným jednáním uživatele. Stáhnutí jakéhokoliv malware může obsahovat možnosti vzdáleného přístupu k počítači.

Prevence proti vzniku hrozby

- Číst příbalové manuály a aktivovat jakákoliv bezpečnostní opatření, která lze aktivovat na daném zařízení (dvoufázové ověření).
- Po připojení zařízení do chodu ihned změnit původní přihlašovací údaje.
- Nestahovat přílohy a neklikat na linky z emailů od neznámých adresátů (prevence zavirování PC).
- Ochrana sítě a zařízení v nich, skrze které by se dalo ke kameře dostat.
- Nestahovat ilegální soubory z internetu (nenavštěvovat podezřelé webové stránky).
- Mít aktivovaný antivirový software.
- Heslo nastavit dostatečně bezpečné a silné (nevyskytující se ve slovnících, které se nachází například v příloze obsah cd). Toto aplikovat na jakékoliv zařízení připojené k internetu, které umožnuje zadání přihlašovacích údajů.
- Při používání webových stránek se dívat na platnosti certifikátů, kontrolu připojení.

4.1.3 Hrozby spojené s ostatními zařízeními

Jedná-li se stále o kameru připojenou do lokální sítě, jsou tu hrozby, které je vhodné uvést. Spoustu hrozeb je spojeno se zařízeními, které jsou připojené k internetu. To může být stolní počítač, notebook, mobilní telefon, tablet apod. Pokud se útočník dostane do jednoho z těchto zařízení, může se tím dostat i do lokální sítě, ve které je kamera připojena. Tudíž se potom tady nachází stejná hrozba, jako u kamery připojené do veřejné sítě. V tomto případě by bylo vhodné nastavit síť tak, aby bylo možné se do kamery dostat pouze z jednoho bodu (např. notebook). Ne každá kamera obsahuje toto nastavení, ale pokud ano, je vhodné nastavit whitelisty paket, které mohou projít k danému zařízení buď ve firewallu kamery (pokud to umožňuje) a zároveň v nastavení síti, nebo pouze nastavit toto omezení v routeru. Dalším vhodným opatřením vůči této hrozbě je zabezpečit dané zařízení a vyvarovat se vůči hrozbám typu phishing, spam/ham, malware – počítačový virus, spyware, keylogger, Trojský kůň (viz 1.3).

Stejně jako u zařízení připojených k internetu, je potřeba chránit i samotnou síť, správné nastavení routeru a nepřístupnost Wi-Fi sítě mimo objekt. V případě nezabezpečení lokální sítě jsou hrozby stejné, jako když se jedná o veřejnou síť. Snadný přístup do sítě – snadný přístup do zařízení k ní připojené – webová kamera (viz 2.1.3).

4.1.4 Hrozby spojené s kamerou samotnou

Kamera sama o sobě používá zastaralý software, což znamená, že neprobíhají ze strany výrobce aktualizace, které by pomáhaly k aktivnímu zabezpečení této webové kamery. Zastaralý software v sobě může obsahovat spousty nevyřešených bezpečnostních chyb, které pak napomáhají útočníkovi. Po případném napadení tohoto systému útočník může mít kontrolu nad zařízením napořád díky neaktualizovaného softwaru.

Další hrozbou a poměrně důležitou zranitelností v dnešní době je, že webová kamera není připojena přes protokol HTTPS, tedy nemá zabezpečené připojení. Útočníci pak mají možnosti, jak zaútočit na danou webovou adresu. Tyto typy útoků mohou vypadat následovně: Útočník může odposlouchávat komunikaci mezi prohlížečem (uživatelem) a serverem. Co se týče webové aplikace pro kameru, útočník zjistí přihlašovací údaje k dané webové kameře a připadne mu do ní přístup. Útočník tak může sledovat obrazový přenos webové kamery bez vědomí majitele, dokud se sám neprozradí, nebo dokud majitel nerozpojí internetové připojení z webové kamery. Další nebezpečí, hrozící z neprovozování https protokolu, je možnost zfalšování zpráv. To znamená, že u nezabezpečeného http protokolu jsou možné útoky typu DDoS, což by způsobilo nefunkčnost webové kamery na delší dobu.

Existuje zde další scénář možného připojení útočníka ke kameře, a ten je následující: uživatel (majitel kamery) si zřídí SSH vzdálené připojení k počítači, který teď bude brán jako server, ze kterého se lze připojit k webové kameře. A připojení k tomuto serveru probíhá pomocí defaultního portu 22, což je zmíněné SSH připojení. Majitel používá metodu připojení pomocí hesla, což je varianta, která se nedoporučuje, protože není zas tak bezpečná, jako kdyby si majitel zvolil variantu s SSH klíči, které jsou bezpečné. Při zřízení SSH připojení je nutné zvolit jiný port než defaultní 22, protože to by pak vedlo k možnému napadení systému a jeho odposlouchávání. Hrozí zde útoky hrubou silou a v případě slabého hesla útočník získá přístup do samotného operačního systému počítače (serveru), který pak může ovládat, což by vedlo i k přístupu ke kameře. Opatření je nejen změnit defaultní port 22, ale také vytvořit silné heslo jak k přístupu SSH, tak k uživateli administratora, nebo v linuxu root. Omezit uživatele, kteří se mohou připojovat k danému serveru. V nejlepším případě zrušit přístup přes administratora/root v SSH připojení a povolit jej pouze, pokud byl uživatel ověřen. Další možná opatření jsou: začít se přihlašovat při použití SSH klíčů, SSH server mít připojený v lokální síti.

4.1.5 Hrozby spojené s kamerou připojenou do veřejné sítě

Testovaná webová kamera se sice nenachází ve veřejné síti, avšak je vhodné uvést i hrozby týkají se kamery, která by byla zapojena do veřejné sítě, či používala ke svému přenosu VPN.

První hrozba, která se nachází u webových kamer připojených do veřejné sítě, je, že do kamery může mít přístup kdokoliv z jakéhokoliv zařízení nacházející se v síti. Při takové situaci je nutné provést nastavení firewallu buď v rozhraní samotné kamery, nebo nastavení v síti. Nejlepší způsob by byl omezit přístup do kamery tak, že bude mít přístup pouze jeden počítač nacházející se v dané síti. Dále pak tento počítač zabezpečit silným heslem a přístup k tomuto počítači omezit.

V případě, že je kamera zapojena do veřejně přístupné datové zásuvky, je možné kameru z této zásuvky vypojit a přenos tak bude nadále nefunkční. Proto je nutné i z fyzického hlediska připojit kameru takovým způsobem, kterým nebudou napájecí kabely snadno odpojitelné. Například kabely vedoucí do zásuvky vložit do zdi v pancéřových trubkách, konec pak zapojit do zásuvky, ke které nelze přistoupit zvnějšku. V nejlepším případě zapojit kabely do uzavřené místnosti, do které má přístup omezený počet lidí.

4.2 Seznam testovaných adres a jejich výsledky

K tomuto kroku byly použity dvě online webové aplikace, pomocí kterých byly zjištěny jejich zranitelnosti a možná historie jejich napadení. Tyto webové aplikace jsou následující: https://securityheaders.com/ a https://www.abuseipdb.com/.[45]

Stránka AbuseIPDB funguje na principu databáze, ve které jsou umístěny IP adresy, které v historii již byly napadeny, nebo jsou brány jako nebezpečné či podezřelé. Webová aplikace Securityheaders slouží pro zobrazení zranitelností a následný popis možných nedostatků hlaviček u zadané IP adresy. Tato stránka hodnotí adresy od A do F, kde A je ta nejlepší známka a F ta nejhorší. Testování pomocí těchto stránek proběhlo v květnu roku 2020, následné informace se mohou lišit od aktuálních.

Seznam testovaných adres a jejich sběr informací byl proveden v květnu roku 2020 na serveru shodan.io pod kategorií „web cams“ a z tohoto seznamu byly náhodně vybrány IP adresy IP kamer, které byly následně testovány. Aktuálně se tyto informace mohou změnit podle aktualizací bezpečnosti, změny IP adres kamer apod. Nástroj shodan.io byl zvolen,

protože se jedná o typ OSINT nástroje, což znamená, že se jedná o veřejně dostupné informace. V testování budou popsány nejvíce důležité zranitelnosti, které byly popsány a vysvětleny v již dříve zmiňovaném tématu (viz 3.1.7). [29]

4.2.1 Adresa 1 - 101.132.145.56

Při použití AbuseIPDB vychází, že tato adresa se nenachází v dané databázi. Webová aplikace Securityheaders ohodnotila tuto adresu známkou D, kde XCTO a XFO zabraňují útokům typu XXE, Injection, nebo Pishingu. Tato stránka nemá bezpečnostní hlavičky CSP, RP a FP. Kde CSP může být příčinou útoků typu XXE na tuto IP adresu, tzn. není zde zablokováno vkládání obrázků, skriptů, fonty, media apod. RP hlavička by nabídla větší bezpečnost, která by mohla být použita proti útokům typu XSS. Co se týče FP, jedná se o Feature-Policy, což je nová hlavička, která se stará o kontrolu, které funkce a API se mohou používat v prohlížeči. Další věc je to, že adresa 1 nepoužívá HTTPS protokol, což znamená, že mezi prohlížečem (uživatelem) a serverem nedochází k bezpečné komunikaci.

4.2.2 Adresa 2 - 82.228.230.28

Při použití AbuseIPDB vychází, že tato adresa se nenachází v dané databázi. Webová aplikace Securityheaders ohodnotila tuto adresu známkou F. To je nejhorší možné ohodnocení v této webové aplikaci. Je odůvodněno tím, že daná adresa neobsahuje žádné bezpečnostní hlavičky a nemá spojení pomocí https protokolu. Jsou zde možné útoky typu XSS, XXP, clickjacking, XXE apod.

4.2.3 Adresa 3 - 47.252.23.1

AbuseIPDB nemá informace o této stránce ve své databázi. Securityheaders vyhodnotila tuto stránku za D, stejně jako u adresy 1. Adresa má 2 hlavičky a to: XCTO a XFO, tyto hlavičky zabraňují útokům typu XXE, Injection, nebo Pishingu. Tato stránka nemá bezpečnostní hlavičky CSP, RP a FP, kde nezavedení hlavičky CSP může být příčinou útoků typu XXE, tzn. není zde zablokováno vkládání obrázků, skriptů, fonty, media apod. RP hlavička by nabídla větší bezpečnost, která by mohla být použita proti útokům typu XSS. Co se týče FP, jedná se o Feature-Policy hlavičku, která se stará o kontrolu, které funkce a API se mohou používat v daném prohlížeči.

A jako poslední důležitá věc je to, že jak adresy 1 a 2, tak adresa 3 nepoužívá https protokol, což znamená, že mezi prohlížečem (uživatelem) a serverem nedochází k bezpečné komunikaci.

4.2.4 Adresa 4 - 47.74.17.64

AbuseIPDB nemá informace o této stránce ve své databázi. Securityheaders vyhodnotila tuto stránku za D, stejně jako u adresy 1 a 3. Adresa má 2 hlavičky a to: XCTO a XFO, tyto hlavičky zabraňují útokům typu XXE, Injection, nebo Pishingu. Tato stránka nemá bezpečnostní hlavičky CSP, RP a FP, kde nezavedení hlavičky CSP může být příčinou útoků typu XXE, tzn. není zde zablokováno vkládání obrázků, skriptů, fonty, media apod. RP hlavička by nabídla větší bezpečnost, která by mohla být použita proti útokům typu XSS. Co se týče FP, jedná se o Feature-Policy hlavičku, která se stará o kontrolu, které funkce a API se mohou používat v daném prohlížeči.

A jako poslední důležitá věc je to, že jak adresy 1 a 2, tak adresa 3 nepoužívá https protokol, což znamená že mezi prohlížečem (uživatelem) a serverem nedochází k bezpečné komunikaci.

4.2.5 Adresa 5 - 37.10.172.38

AbuseIPDB nemá informace o této stránce ve své databázi. Securityheaders vyhodnotila tuto stránku za D, stejně jako u adresy 1, 3 a 4. Stránka na této adrese má 3 bezpečnostní hlavičky a to: XCTO, XFO a CSP. Tyto hlavičky zabraňují útokům typu XXE. Tato stránka neobsahuje hlavičky RP a FP, které slouží pro další zabezpečení, zabraňujícím útokům typu XSS. Další zranitelností je, že stránka nepoužívá HTTPS protokol.

4.2.6 Adresa 6 - 109.206.96.58

Při použití AbuseIPDB vychází, že tato adresa se nachází v dané databázi. Byly zaznamenány 2 reporty, z toho první byl zaznamenán ke dni 29. září 2019. Pomocí stránky Securityheaders nelze tuto IP adresu najít.

4.2.7 Adresa 7 - 47.252.28.53

AbuseIPDB nemá informace o této stránce ve své databázi. Securityheaders vyhodnotila tuto stránku za D, stejně jako u adresy 1, 3, 4 a 5. Stránka na této adrese má 2 bezpečnostní hlavičky a to: XCTO a XFO. Tyto hlavičky zabraňují útokům typu XXE. Stránka neobsahuje hlavičky CSP, RP a FP. To znamená, že na stránce jsou možné útoky typu XSS. Další zranitelností stránky je, že nepoužívá HTTPS protokol.

4.2.8 Adresa 8 - 149.129.181.102

AbuseIPDB nemá informace o této stránce ve své databázi. Securityheaders vyhodnotila tuto stránku za D, stejně jako u adresy 1, 3, 4, 5 a 7. Tato stránka má 2 bezpečnostní hlavičky a to: XCTO a XFO, které zabraňují útokům typu XXE. Stránka neobsahuje bezpečnostní hlavičky CSP, RP a FP. Na tuto adresu je tedy možné provést útoky typu XSS. Další zranitelností je nepoužívání HTTPS protokolu, a tudíž komunikace mezi prohlížečem (uživatelem) a serverem není bezpečná.

4.2.9 Adresa 9 - 47.112.120.148

AbuseIPDB nemá informace o této stránce ve své databázi. Securityheaders vyhodnotila tuto stránku za D, stejně jako u adres 1, 3, 4, 5, 7 a 8. Tato stránka má 2 bezpečnostní hlavičky a to: XCTO a XFO, které zabraňují útokům typu XXE. Stránka neobsahuje bezpečnostní hlavičky CSP, RP a FP. Na tuto adresu je tedy možné provést útoky typu XSS. Další zranitelností je nepoužívání HTTPS protokolu, a tudíž komunikace mezi prohlížečem (uživatelem) a serverem není bezpečná.

4.2.10 Adresa 10 - 159.138.231.23

AbuseIPDB nemá informace o této stránce ve své databázi. Securityheaders vyhodnotila tuto stránku za D, stejně jako u adres 1, 3, 4, 5, 7, 8 a 9. Tato stránka má 2 bezpečnostní hlavičky a to: XCTO a XFO, které zabraňují útokům typu XXE. Stránka neobsahuje bezpečnostní hlavičky CSP, RP a FP. Na tuto adresu je tedy možné provést útoky typu XSS. Další zranitelností je nepoužívání HTTPS protokolu, a tudíž komunikace mezi prohlížečem (uživatelem) a serverem není bezpečná.

4.2.11 Adresa 11 - 172.104.163.142

AbuseIPDB nemá informace o této stránce ve své databázi. Webová aplikace Securityheaders ohodnotilo tuto adresu známkou F, což je nejhorší možné ohodnocení v této webové aplikaci. Je odůvodněno tím, že daná adresa neobsahuje žádné bezpečnostní hlavičky a nemá spojení pomocí HTTPS protokolu. Jsou zde možné útoky typů, XSS, XXP, XXE apod.

4.2.12 Adresa 12 - 47.110.56.24

AbuseIPDB nemá informace o této stránce ve své databázi. Securityheaders vyhodnotila tuto stránku za D, stejně jako u adres 1, 3, 4, 5, 7, 8, 9 a 10. Tato stránka má 2 bezpečnostní hlavičky a to: XCTO a XFO, které zabraňují útokům typu XXE. Stránka neobsahuje bezpečnostní hlavičky CSP, RP a FP. Na tuto adresu je tedy možné provést útoky typu XSS. Další zranitelností je nepoužívání HTTPS protokolu, a tudíž komunikace mezi prohlížečem (uživatelem) a serverem není bezpečná.

4.2.13 Adresa 13 - 8.208.11.85

AbuseIPDB nemá informace o této stránce ve své databázi. Securityheaders vyhodnotila tuto stránku za D, stejně jako u adres 1, 3, 4, 5, 7, 8, 9, 10 a 12. Tato stránka má 2 bezpečnostní hlavičky a to: XCTO a XFO, které zabraňují útokům typu XXE. Stránka neobsahuje bezpečnostní hlavičky CSP, RP a FP. Na tuto adresu je tedy možné provést útoky typu XSS. Další zranitelností je nepoužívání HTTPS protokolu, a tudíž komunikace mezi prohlížečem (uživatelem) a serverem není bezpečná.

4.2.14 Adresa 14 – 47.96.122.85

AbuseIPDB nemá informace o této stránce ve své databázi. Securityheaders vyhodnotila tuto stránku za D, stejně jako u adres 1, 3, 4, 5, 7, 8, 9, 10, 12 a 13. Tato stránka má 2 bezpečnostní hlavičky a to: XCTO a XFO, které zabraňují útokům typu XXE. Stránka neobsahuje bezpečnostní hlavičky CSP, RP a FP. Na tuto adresu je tedy možné provést útoky typu XSS. Další zranitelností je nepoužívání HTTPS protokolu, a tudíž komunikace mezi prohlížečem (uživatelem) a serverem není bezpečná.

4.2.15 Adresa 15 - 212.171.21.229

AbuseIPDB nemá informace o této stránce ve své databázi. Webová aplikace Securityheaders ohodnotilo tuto adresu známkou F. To je nejhorší možné ohodnocení v této webové aplikaci. Je odůvodněno tím, že daná adresa neobsahuje žádné bezpečnostní hlavičky a nemá spojení pomocí HTTPS protokolu. Jsou zde možné útoky typů, XSS, XXP, XXE apod.

4.2.16 Vyhodnocení zabezpečení všech adres

Tabulka č. 1. – Vyhodnocení zabezpečení seznamu adres

Adresa č.	**Abuse IPDB**	**Hod-nocení**	**XCTO**	**XFO**	**CSP**	**RP**	**FP**	**HTTPS**
Adresa 1	Ne	D	Ano	Ano	Ne	Ne	Ne	Ne
Adresa 2	Ne	F	Ne	Ne	Ne	Ne	Ne	Ne
Adresa 3	Ne	D	Ano	Ano	Ne	Ne	Ne	Ne
Adresa 4	Ne	D	Ano	Ano	Ne	Ne	Ne	Ne
Adresa 5	Ne	D	Ano	Ano	Ano	Ne	Ne	Ne
Adresa 6	Ano	-	-	-	-	-	-	-
Adresa 7	Ne	D	Ano	Ano	Ne	Ne	Ne	Ne
Adresa 8	Ne	D	Ano	Ano	Ne	Ne	Ne	Ne
Adresa 9	Ne	D	Ano	Ano	Ne	Ne	Ne	Ne
Adresa 10	Ne	D	Ano	Ano	Ne	Ne	Ne	Ne
Adresa 11	Ne	F	Ne	Ne	Ne	Ne	Ne	Ne
Adresa 12	Ne	D	Ano	Ano	Ne	Ne	Ne	Ne
Adresa 13	Ne	D	Ano	Ano	Ne	Ne	Ne	Ne
Adresa 14	Ne	D	Ano	Ano	Ne	Ne	Ne	Ne
Adresa 15	Ne	F	Ne	Ne	Ne	Ne	Ne	Ne

Z tabulky č. 1. – Vyhodnocení zabezpečení seznamu adres vychází, že stránka AbuseIPDB neobsahuje žádnou z vybraných adres ve své databázi krom adresy č. 6. Hodnocení adres bylo ve většině případů za D, 3 případy byly za F. Kromě zmíněných 3 případů byla u všech adres zaznamenána hlavička XCTO – X-Content-Type-Options a XFO – X Frame Options. Bezpečnostní hlavička CSP – Content Security Policy byla zaznamenána pouze u adresy 5, zbylé ji již neobsahovaly. Dále pak u žádné ze seznamu adres nebyly

nalezeny hlavičky RP-Refferer-Policy a FP – Feature Policy. Jako poslední výsledek vyplývající z testování nebyl zjištěn HTTPS protokol u žádné z testovaných adres, pomocí níž dochází k bezpečné komunikaci mezi prohlížečem a serverem.

4.2.17 Jak opatřit jednotlivé bezpečnostní hlavičky ve webové aplikaci

Každou hlavičku lze zabezpečit nastavením, které jsou vysvětleny níže. Celé opatření u testovaných kamer, pokud to lze - nebude na úrovni serveru, ale musel by se změnit a nastavit firmware kamery, což ukazuje na to, že většina kamer je v základu vůči tomuto nezabezpečená. (Lze to zabezpečit nastavením sítě a routeru). Tyto syntaxe a kódy jsou vysvětleny k použití pro softwarové webové servery Apache a Nginx. [55, 56]

4.2.17.1 X-Content-Type-Options

Syntax pro hlavičku XCTO:

```
X-Content-Type-Options: nosniff
```

Nastavení v Nginx

```
add_header X-Content-Type-Options "nosniff" always;
```

Nastavení v Apache

```
header always set X-Content-Type-Options "nosniff“
```

4.2.17.2 X Frame Options

Syntax pro hlavičku XFO:

```
X-Frame-Options: SAMEORIGIN
```

Nastavení v Nginx

```
add_header X-Frame-Options "SAMEORIGIN" always;
```

Nastavení v Apache

```
header always set X-Frame-Options "SAMEORIGIN“
```

4.2.17.3 Content Security Policy

Syntax pro hlavičku CSP:

```
„Content-Security-Policy: <policy-directive>; <policy-directive>“
```

4.2.17.4 Refferer-Policy

Syntax pro hlavičku RP:

```
„enum ReferrerPolicy {
        "",
    "no-referrer",
"no-referrer-when-downgrade",
    "same-origin",
      "origin",
  "strict-origin",
"origin-when-cross-origin",
"strict-origin-when-cross-origin",
    "unsafe-url"
        };
```

„Kde no-referrer určuje, že žádné informace o referreru se nebudou posílat spolu s požadavky od konkrétního klienta do žádosti jakéhokoli původu. Zajistí to, že záhlaví bude zcela vynecháno.“ [58]

„„no-referrer-when-downgrade“ odešle úplnou adresu URL spolu s požadavky z nastavení prostředí chráněného TLS na potenciálně důvěryhodnou adresu URL a požadavky klientů, kteří nejsou žádným původem chráněni pomocí TLS. Žádosti od klientů chráněných TLS na adresy URL, které nejsou potenciálně důvěryhodné, nebudou obsahovat žádné refererové informace. Hlavička referer HTTP nebude odeslána.“ [58]

„same-origin“ specifikuje, že úplná adresa URL, zpracovaná pro použití jako referer, se při zadávání požadavků na stejný původ od konkrétního klienta odešle jako referer informace. Na druhou stranu, žádosti od sdílených zdrojů nebudou obsahovat informace o refereru. Referer hlavička HTTP nebude odeslána. [58]

„origin“ specifikuje, že pouze serializace ASCII původu klienta požadavku je odesílána jako informace referer, když od konkrétního klienta žádá o stejný původ i požadavek sdíleného zdroje. [58]

„strict-origin“ odešle serializaci ASCII z požadavku od klienta při zadávání požadavků: [58]

- z objektu nastavení prostředí chráněného TLS na potenciálně důvěryhodnou adresu URL a od objektů nastavení prostředí, které nejsou chráněny TLS, do jakéhokoli původu. [58]

Na druhé straně žádosti od klientů chráněných TLS na adresy URL, které nejsou potenciálně důvěryhodné, nebudou obsahovat žádné referové informace. Hlavička HTTP odesílatele nebude odeslána. [58]

"origin-when-cross-origin" specifikuje, že úplná adresa URL, zpracovaná pro použití jako referer, je odesílána jako referer informace při provádění žádostí stejného původu od konkrétního klienta požadavku, a provede pouze serializaci ASCII původu klientova požadavku, který je odeslán jako informace o předávajícím při provádění žádostí o sdíleném zdroji od konkrétního klienta. [58]

"strict-origin-when-cross-origin" specifikuje, že úplná adresa URL, která je zpracována pro použití jako referer, je odesílána jako referer informace při provádění požadavků na stejný původ od žádosti konkrétního klienta a provede ASCII serializaci pouze pokud je stejný původ klienta při požadavku u provádění žádostí sdíleného zdroje: [58]

- z objektu nastavení prostředí chráněného TLS na potenciálně důvěryhodnou adresu URL a od objektů nastavení prostředí, které nejsou chráněny TLS, do jakéhokoli původu. [58]

Na druhé straně žádosti klientů chráněných TLS na adrese URL, které nejsou potenciálně důvěryhodné, nebudou obsahovat žádné informace o refererovi. Hlavička HTTP odesílatele nebude odeslána. [58]

„unsafe-url“ určuje, že úplná adresa URL, která je zpracována pro použití jako referer, je odesílána společně se sdíleným zdrojem a původními žádostmi, které jsou vytvořeny od původního konkrétního klienta. [58]

4.2.17.5 Feature Policy

Syntax pro hlavičku FP:

```
„Feature-Policy: autoplay 'none'; camera 'none'
```

Nastavení v Nginx

```
add_header Feature-Policy "autoplay 'none'; camera 'none'" always;
```

Nastavení v Apache

```
header always set Feature-Policy "autoplay 'none'; camera 'none'"
```

4.2.17.6 Expect-CT

Tato hlavička umožňuje kontrolu certifikátu u webových stránek.

Syntax pro hlavičku Expect-CT vypadá následovně:

```
Expect-CT: max-age=604800, enforce, report-uri=https://www.example.com/report
```

Nastavení v Nginx

```
add_header Expect-CT "max-age=604800, enforce, report-
    uri='https://www.example.com/report' always;
```

Nastavení v Apache

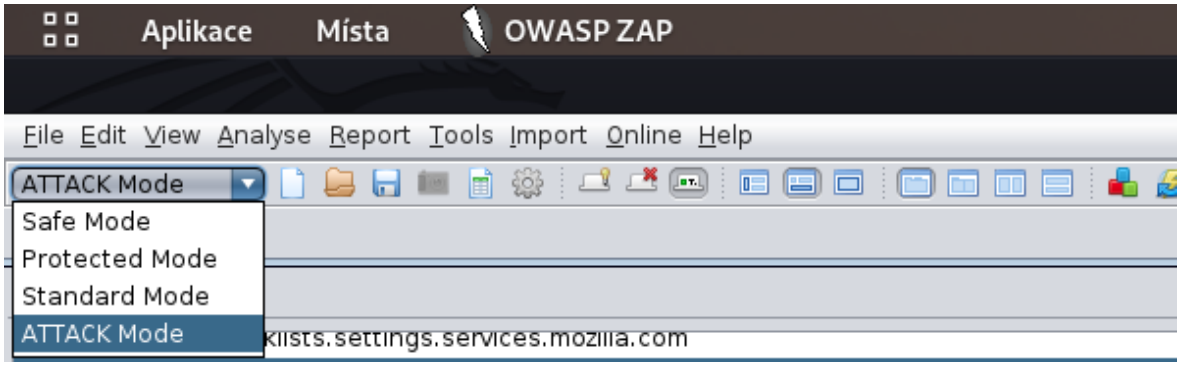
```
header always set Expect-CT "max-age=604800, enforce, report-
    uri=https://www.example.com/report“
```

4.3 Testování v nástrojích z kali linuxu

V kali linuxu byly vybrány 2 testovací nástroje, a to OWASP Zap tool a Legion, dříve známý, jako SPARTA. Tyto nástroje testují TOP 10 základních zranitelností webových aplikací. Na těchto dvou nástrojích byla otestována jedna webová kamera, která byla zapojena do lokální sítě. Test probíhal z té samé sítě, ve které byla kamera připojena.

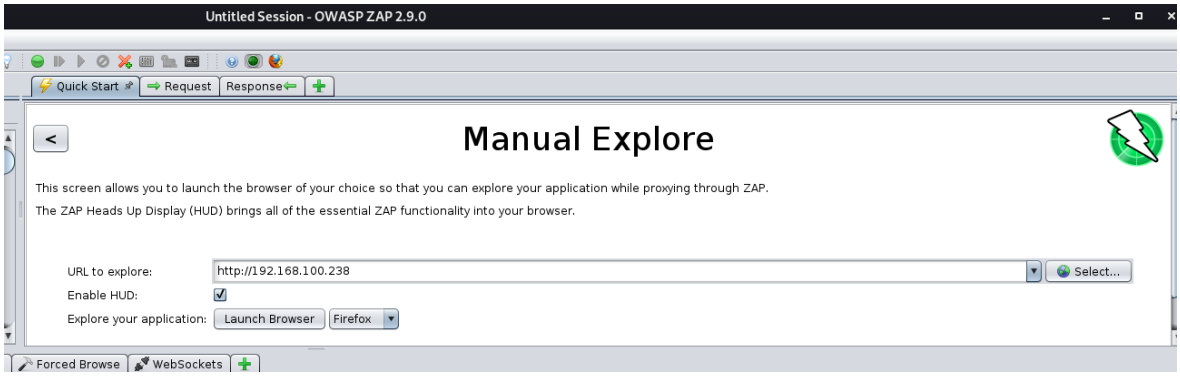
4.3.1 OWASP Zap tool

Předtím, než byl proveden test v nástroji OWAPS Zap tool, bylo prvně potřeba zapnout „ATTACK Mode“ (viz obrázek č. 8.).



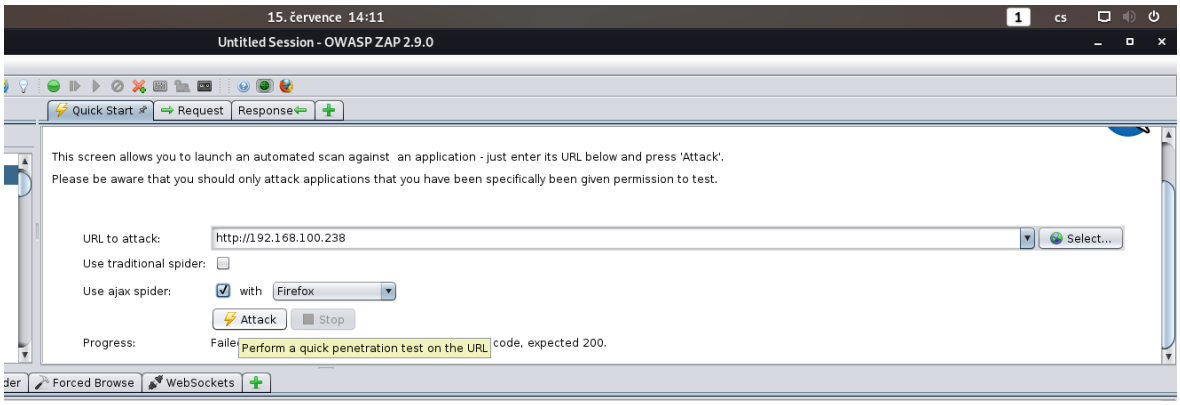
Obrázek č. 8. – OWASP ZAP – ATTACK Mode

Druhým krokem bylo nastavit v nástroji adresu webové stránky, kterou chceme testovat. Tento krok se nachází v pravé části nástroje s názvem „Manual Explore“ (viz obrázek č. 9.), kde se zadá IP adresa nebo URL adresy webové stránky, kterou chceme testovat. U vybrané kamery, která sloužila pro testování, byla adresa http://192.168.100.238/index.htm.



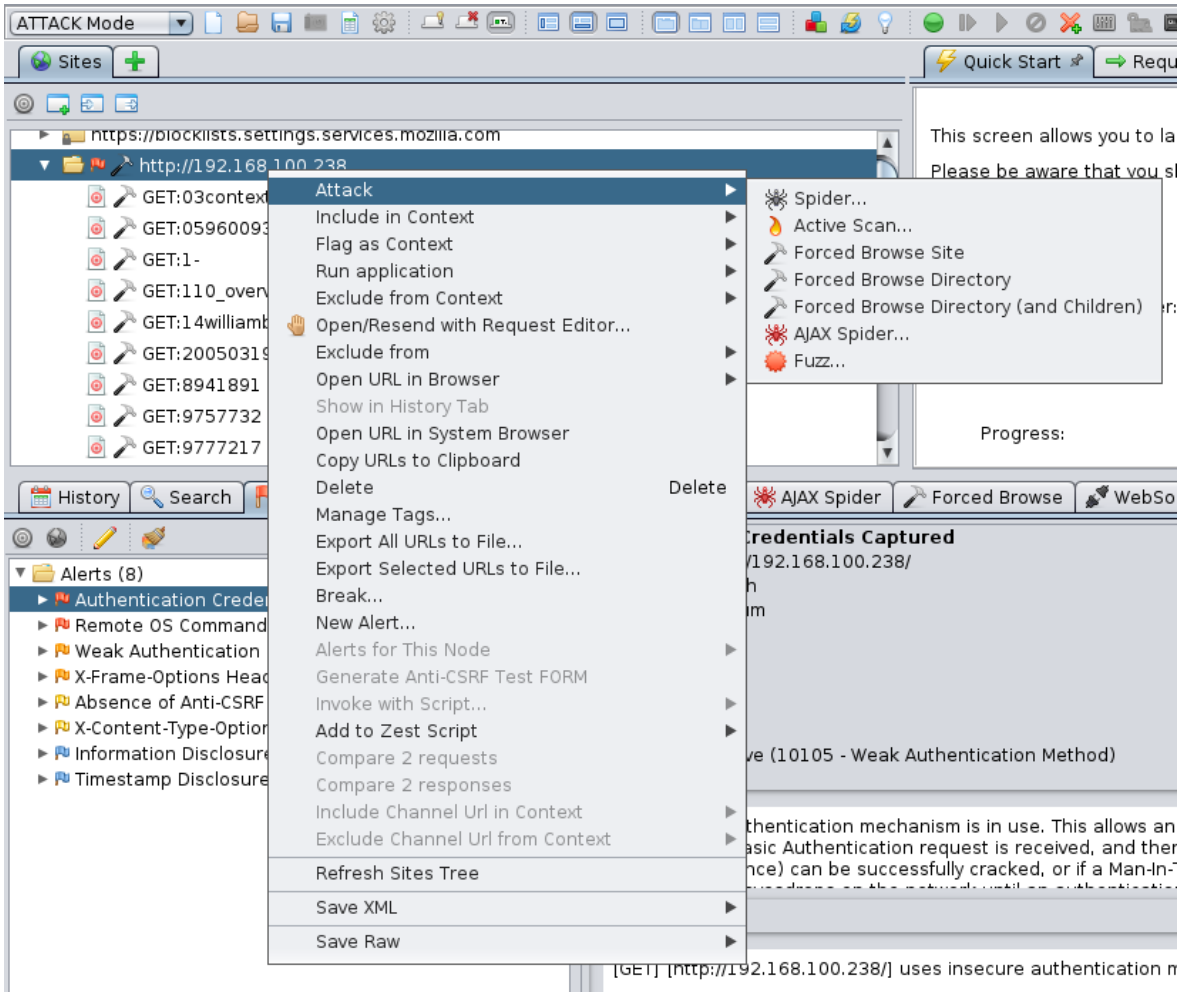
Obrázek č. 9. – OWASP ZAP – Manual Explore

Třetím krokem byl krok s názvem „Automated Scan“, který lze najít ve stejné části, jako „Manual Explore“. Do tohoto pole byla zadaná stejná adresa, jako u Manual Explore. Scan byl následně spuštěn pomocí tlačítka Attack (viz obrázek č. 10.).



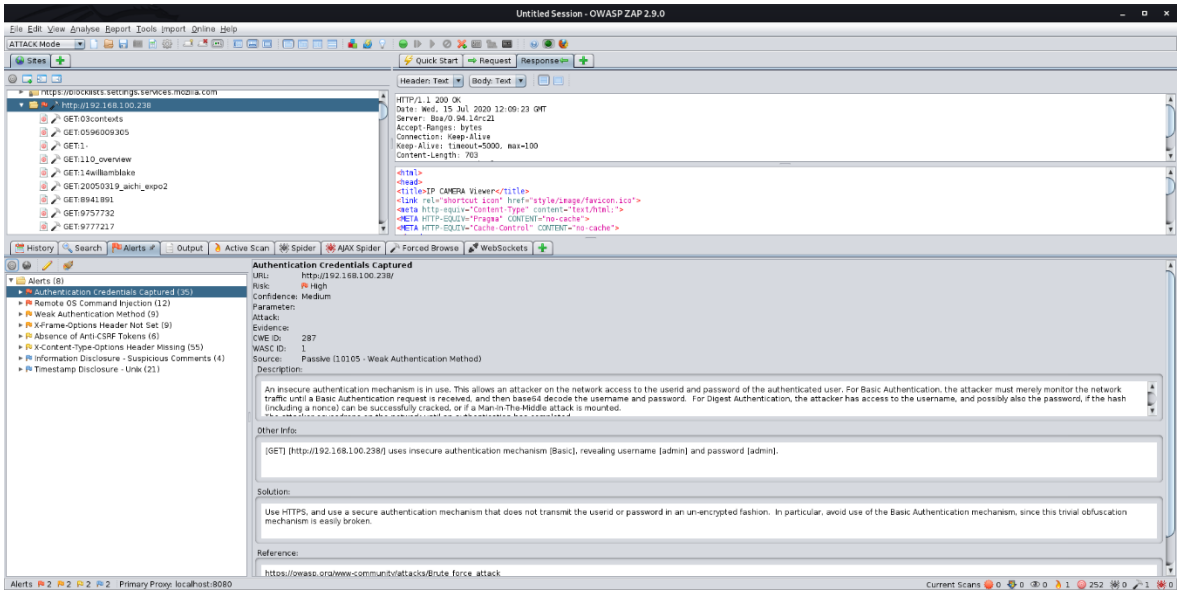
Obrázek č. 10. - OWASP ZAP – Automated Scan

Dalším krokem bylo vybrat, který konkrétní útok chceme zvolit pro danou webovou stránku (viz obrázek č. 11.).



Obrázek č. 11. - OWASP ZAP – Attack

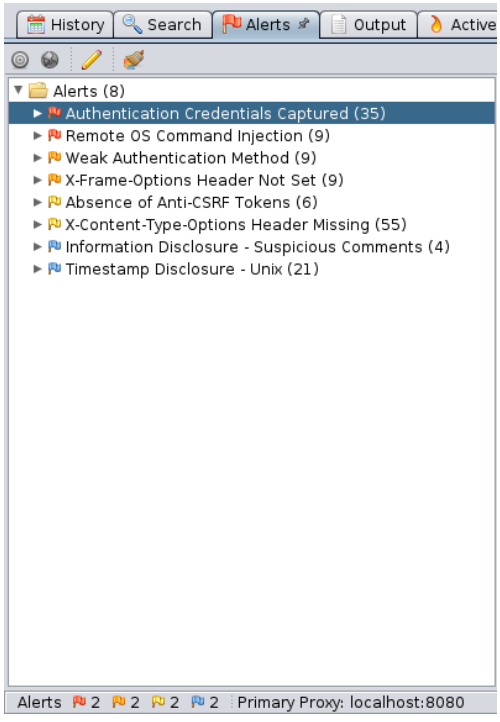
Výsledky testování jsou ukázány v prostřední části lišty nástroje s názvem „Alerts“. Kde po rozkliknutí jednotlivých „Alertů“ lze vidět zranitelnosti testované webové aplikace a případné doporučení, jak zabránit hrozbám, které z nich vyplývají.



Obrázek č. 12. - OWASP ZAP – Alerts

4.3.1.1 Soupis výsledků testování v OWASP ZAP tool

V nástroji OWASP ZAP tool jsou ve výsledku sepsány zranitelnosti a hrozby pomocí vlajek, které jsou barevně odlišeny podle toho, jakou váhu rizika jednotlivá zranitelnost má. Tyto vlajky jsou ukázané v části nástroje s názvem „Alerts“ (viz obrázek č. 13.). Červená vlajka: Vysoké riziko, oranžová vlajka: střední riziko, žlutá vlajka: nízké riziko, modrá vlajka: rady/typy k lepšímu zabezpečení webové aplikace.



Obrázek č. 13. – OWASP ZAP – Alert flags

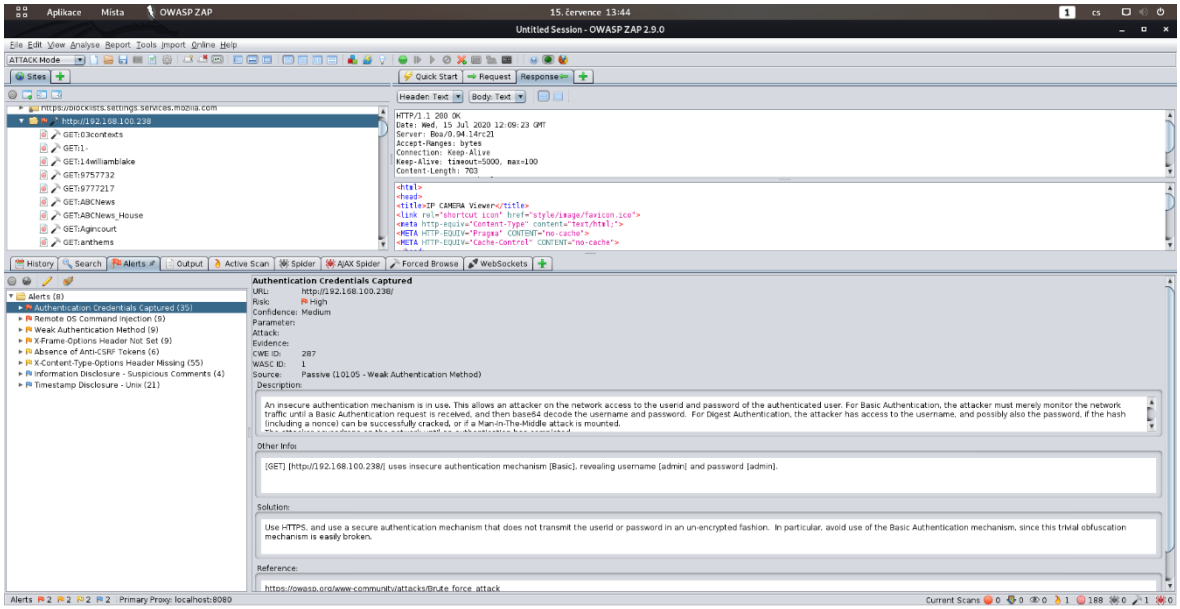
Na obrázku č. 13. lze vidět, že každá z vlajek má určitý název. Jedná se o název zranitelností dané webové aplikace.

Jako první nejdůležitější alert se zranitelností, která má nejvyšší stupeň rizikovosti je „Authentication Credentials Captured“ (viz obrázek č. 14.). V popisu této zranitelnosti se nachází menší scénář hrozby spojené s touto zranitelností. „Authentication Credentials Captured“ poukazuje na to, že webová stránka používá nezabezpečený mechanismus ověřování. To umožňuje útočníkovi v síti přístup k uživatelskému jménu a heslu ověřeného uživatele. Pro získání těchto údajů musí útočník monitorovat provoz v síti, dokud nepřijme hodnotu s požadavkem na základní ověřování, pak tuto hodnotu daného požadavku přeloží podle base64 a získá uživatelské přihlašovací údaje. Pro „Digest access authentication“ (což je způsob, jakým webová aplikace posílá citlivé informace, jako jsou přihlašovací údaje) platí, že útočník může mít přístup k přihlašovacím údajům společně s heslem, pokud jejich hash obsahuje kryptografickou nonce, což pak způsobí, že heslo může být prolomeno, nebo pokud je síť odposlouchávána útokem „Man-In-The-Middle“. Útočník odposlouchává síť do té doby, dokud není ověření dokončeno.

Pomocí tohoto nástroje byly také zjištěny přihlašovací údaje a to jsou: username: admin a password: admin

Doporučené opatření je následné:

- Pořídit si certifikát na danou webovou aplikaci a začít používat zabezpečené připojení mezi prohlížečem a serverem
- Vyhnout se používání zastaralé metody ověřování



Obrázek č. 14. – OWASP ZAP – Authentication Credentials Captured

Jako druhé riziko s nejvyšší hodnotou vyšla zranitelnost s názvem „Remote OS Command Injection“ (viz obrázek č. 15.). Jedná se o techniku útoku, při které se používá neoprávněné provádění akcí v příkazovém řádku operačního systému. Tento útok je možný, pokud aplikace přijímá nedůvěryhodný vstup pro vytváření příkazů operačního systému nezabezpečeným způsobem, který zahrnuje nesprávnou dezinfekci dat nebo nesprávné volání externích programů.

Opatření vůči této zranitelnosti:

- Pokud to lze, používat raději co nejvíce volání funkcí z knihovny než externí programy k obnovení požadované funkce
- Spustit kód v "jail" nebo v podobném prostředí typu sandboxů, které vynucuje přísné hranice mezi procesem a operačním systémem. To může účinně omezit, ke kterým souborům lze přistupovat v určitém adresáři, nebo které příkazy mohou být prováděny daným softwarem.
- Příklady na úrovni OS zahrnují Unix chroot jail, AppArmor a SELinux. Spravovaný kód může obecně poskytovat určitou ochranu. Například java.io.FilePermission v Java SecurityManager umožňuje určit omezení pro operace se soubory.

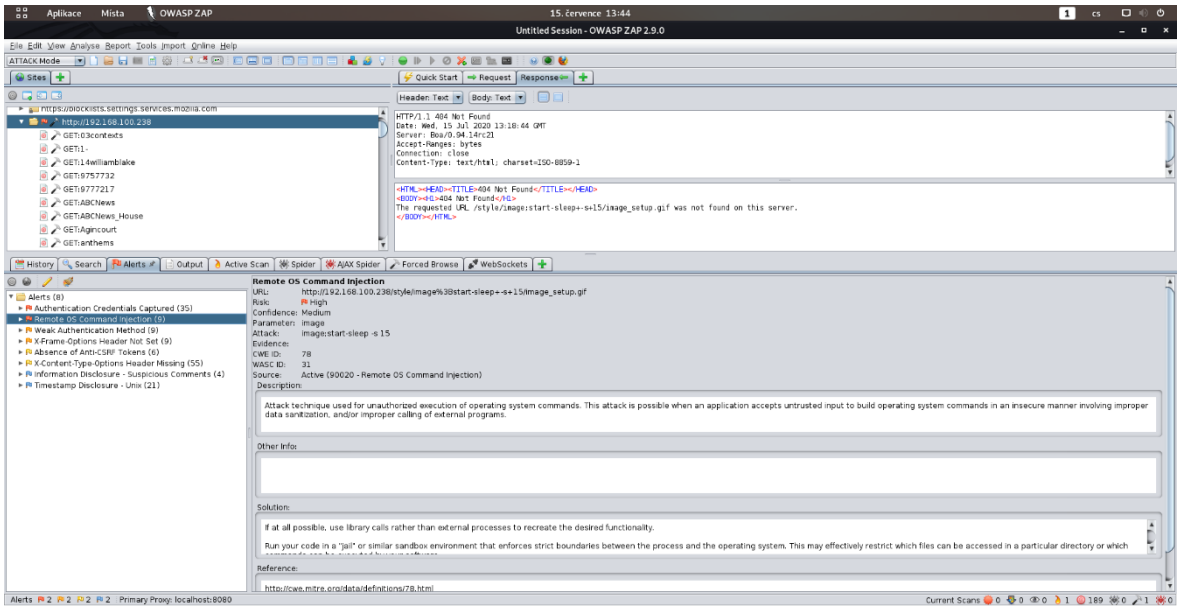
  To nemusí být proveditelné řešení a omezuje to pouze dopad na operační systém, zbytek dané aplikace může být stále předmětem zneužití.
- U všech dat, která budou použita ke generování příkazu, které mají být provedeny, uchovávat mimo externí kontrolu co nejvíce jak je to možné. Například ve webových

aplikacích to může vyžadovat uložení příkazu lokálně ve stavu relace namísto jeho odeslání klientovi do skrytého pole formuláře.

- Používat prověřenou knihovnu nebo rámec, který nedovolí, aby k této slabosti došlo, nebo poskytuje konstrukce, které usnadňují vyhýbání se této slabosti.
- Zvážit například použití ovládacího prvku kódování ESAPI nebo podobného nástroje, knihovny nebo rámce. To pomůže programátorovi kódovat výstupy způsobem méně náchylným k chybám.
- Pokud je potřeba používat navzdory riziku dynamicky generované řetězce dotazů nebo příkazy, je potřeba řádně ošetřit argumenty a v těchto argumentech se vyhnout všem zvláštním znakům. Nejlepším způsobem je zamezit nebo vyfiltrovat všechny znaky, které neprocházejí extrémně přísným whitelistem (vše, co není alfanumerický znak nebo mezerník). Pokud jsou stále potřeba některé speciální znaky, například mezera, je potřeba zabalit každý argument do uvozovek po kroku zamezení / filtrování/. Dávat pozor na injekci argumentů.
- Pokud program, který má být spuštěn, umožňuje specifikovat argumenty ve vstupním souboru nebo ze standardního vstupu, je nutné zvážit použití tohoto režimu k předávání argumentů namísto příkazového řádku.
- Pokud jsou k dispozici strukturované mechanismy, lze použít ty, které automaticky vynucují oddělení mezi daty a kódem. Tyto mechanismy mohou být schopny poskytovat příslušné ošetření, kódování a ověření automaticky, místo toho, aby se spoléhaly na vývojáře, aby poskytl tuto schopnost v každém bodě, kde je generován výstup.
- Některé jazyky nabízejí více funkcí, které lze použít k vyvolání příkazů. Pokud je to možné, je vhodné indentifikovat jakoukoli funkci, která vyvolá příkazový shell pomocí jediného řetězce, a nahradit ji funkcí, která vyžaduje individuální argumenty. Tyto funkce obvykle provádějí vhodné citování a filtrování argumentů. Například v jazyce C funkce system () přijímá řetězec, který obsahuje celý příkaz, který má být proveden, zatímco execl (), execve () a další vyžadují řadu řetězců, jeden pro každý argument. V systému Windows přijímá CreateProcess () najednou pouze jeden příkaz. Pokud se v Perl system () vyskytuje s řadou argumentů, bude ošetřovat každý z nich.
- Pokud lze předpokládat, že veškerý vstup je škodlivý, je potřeba použít strategii ověřování vstupu „accept known good“, tzn. použije se whitelist přijatelných vstupů,

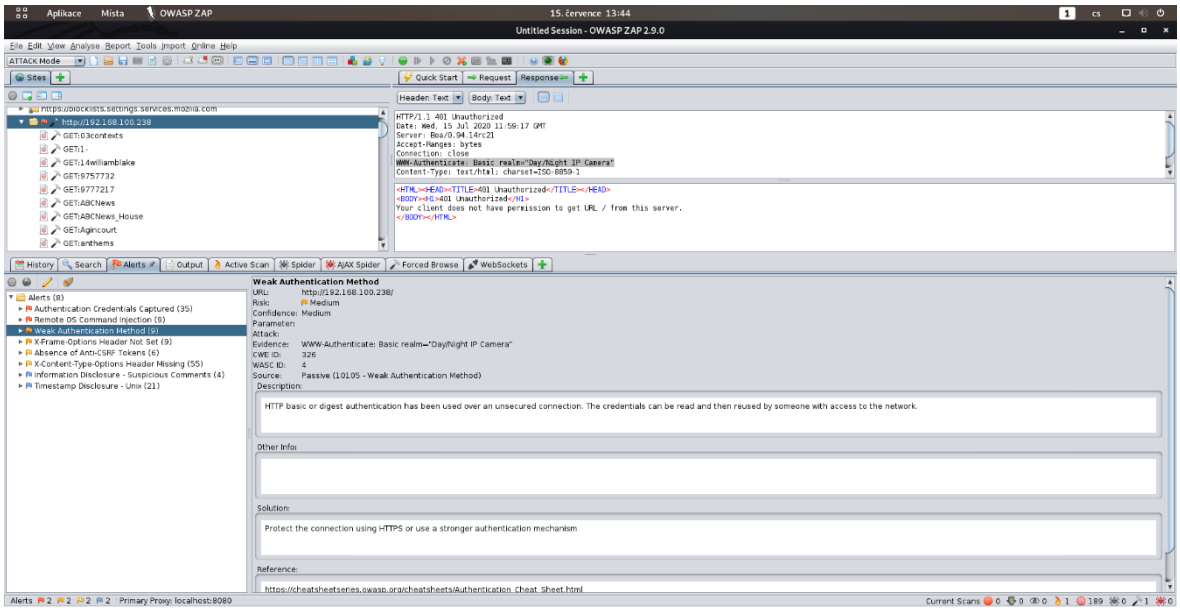
které přesně odpovídají specifikacím. Ten pak odmítne jakýkoliv vstup, který přesně nevyhovuje zadaným specifikacím, nebo jej transformuje na něco, co mu vyhovuje. Není vhodné spoléhat se na Blacklisty ve všech případech, avšak Blacklisty mohou být užitečné pro detekci potenciálních útoků nebo pro určení, které vstupy jsou natolik nesprávné, že by měly být přímo odmítnuty.

- Při ověřování vstupu vzít v úvahu všechny potenciálně relevantní vlastnosti, včetně délky, typu vstupu, celého rozsahu přijatelných hodnot, chybějících nebo zvláštních vstupů, syntaxe, konzistence v souvisejících oblastech a souladu s určitými standardy.
- Při vytváření řetězců příkazů OS používat přísné whitelisty povolených adres, které omezují znakovou sadu na základě očekávané hodnoty parametru v požadavku. To nepřímo omezí rozsah útoku.
- Je potřeba si všimnout, že správné ošetření vstupů je nejúčinnějším řešením pro zabránění implementování příkazů do OS, i když ošetření vstupu může poskytnout určitou hloubku obrany. Je to proto, že účinně omezuje to, co se objeví na výstupu. Ošetření vstupu vždy nezabrání implementace příkazů OS, zejména pokud je zde povinnost podporovat volná textová pole, která by mohla obsahovat libovolné znaky. Například při vyvolávání mail programu bude pravděpodobně nutné povolit, aby pole předmětu obsahovalo jinak nebezpečné vstupy, jako je „;“ a ">" znaky, které by bylo třeba zamezit nebo nějak omezit.



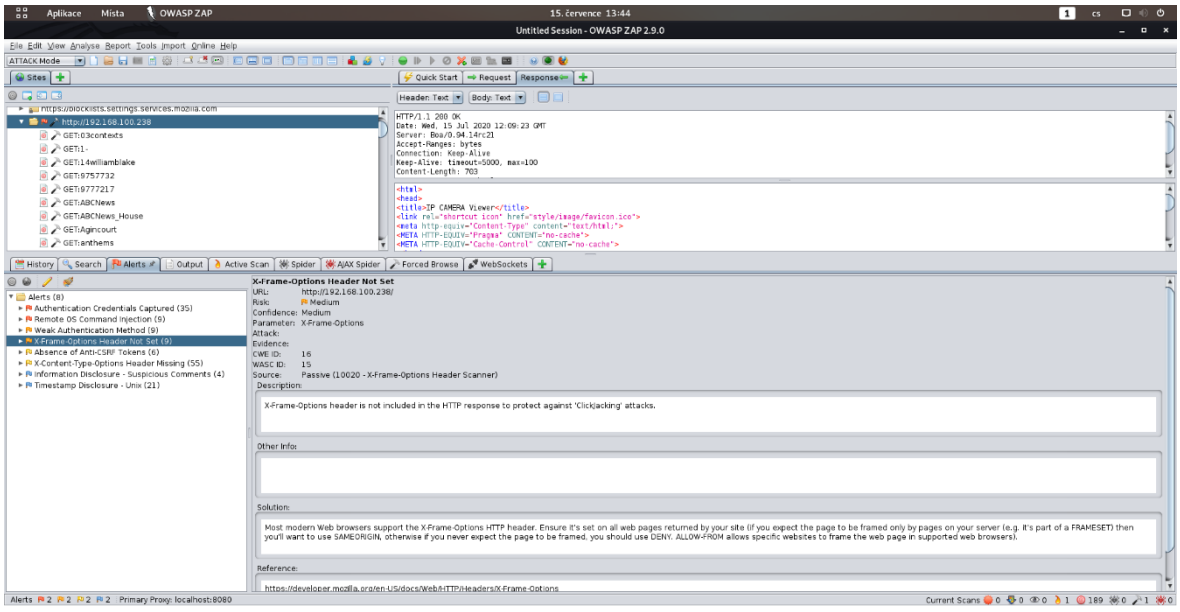
Obrázek č. 15. – OWASP ZAP - Remote OS Command Injection

Jako střední riziko nástroj ukázal „Weak Authentication Method“ (viz obrázek č. 16.), což znamená z překladu slabá metoda ověřování. Ta celkově poukazuje na to, aby webová aplikace začala používat zabezpečené připojení pomoci https protokolu nebo ať je použita silnější metoda ověřování.



Obrázek č. 16. – OWASP ZAP – Weak Authentication Method

Další zranitelnost středního rizika byla „X-Frame-Option Header Not Set“ (viz obrázek č. 17.). Už z názvu je jasné, že se jedná o špatné nastavení XFO, jejichž příkladné nastavení je vysvětleno v kapitole s názvem „Jak opatřit jednotlivé bezpečnostní hlavičky ve webové aplikaci“ (viz 4.2.18).

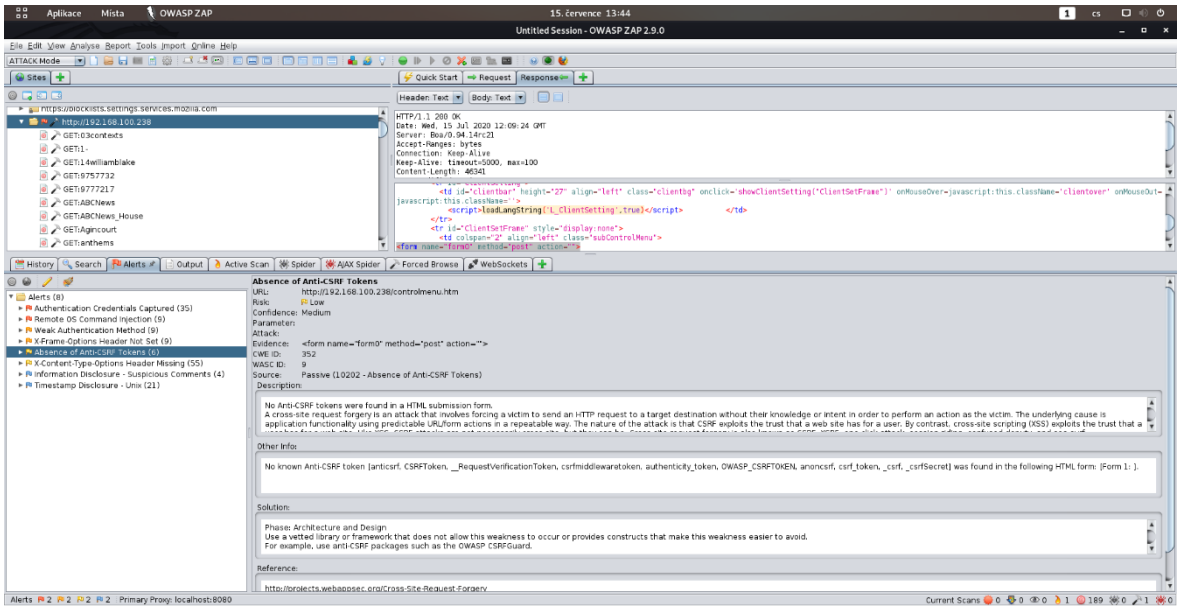


Obrázek č. 17. – OWASP ZAP – X-Frame-Option Header Not Set

Zranitelnost s rizikem, označeným jako slabé, nese název „Absence of Anti-CSRF Tokens“ (viz obrázek č. 17.). Jedná se o to, že webová aplikace nepoužívá tzn. Anti-CSRF tokeny, které slouží pro zabezpečení webové stránky před útoky typu CSRF. Což může útočník zneužít k tomu, aby webová stránka automaticky odeslala uživatele na jinou (škodlivou) stránku bez jeho vědomí. Jsou zde tak možné útoky typu sociálního inženýrství nebo XSS s kterými CSRF spolupracuje, aby dosáhl svých cílů.

Opatření vůči zranitelnosti Absence of Anti-CSRF:

- Používat ověřenou knihovnu nebo rámec, který neumožňuje, aby došlo k této zranitelnosti.
- Ujistit se, že webová aplikace neobsahuje zranitelnosti typu XSS.
- Vytvořit kryptografické nonce, tedy náhodné hodnoty pro jednotlivé formuláře a ujistit se, že nelze tyto hodnoty obejít pomocí XSS.
- Identifikovat zvláště nebezpečné operace, při kterých by uživatel nemohl provést operaci bez toho, aby potvrdil tuto akci, která pro něj může být nebezpečná.
- Nepoužívat metodu GET pro žádný požadavek, který může vyvolat změnu stavu.
- Zkontrolovat hlavičku http referer, zda žádost pochází z očekávané stránky.

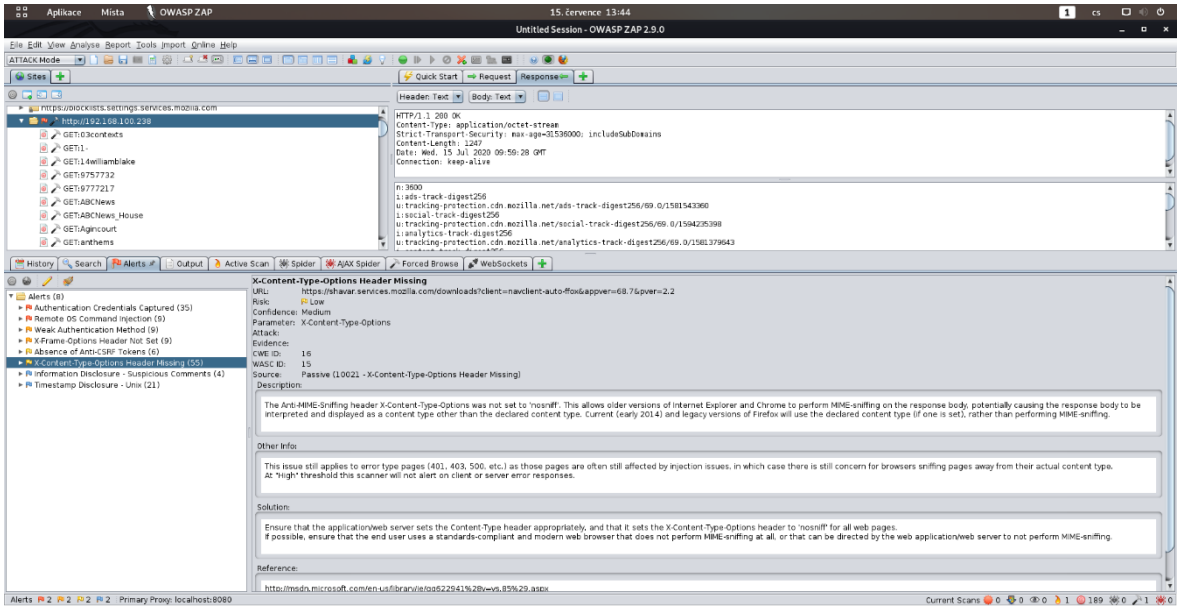


Obrázek č. 18. – OWASP ZAP – Absence of Anti-CSRF Tokens

Další riziko s označením, jako slabé je „X-Content-Type-Options Header missing“ (viz obrázek č. 19.). Už z názvu vyplývá, že se jedná o špatně nastavenou hlavičku (viz 4.2.18). To umožnuje starším verzím Exploreru a Chrome útoky typu XXE.

Opatření vůči této zranitelnosti je tedy následující:

- Nastavit správně hlavičku XCTO
- Donutit uživatele používat moderní browsery, které neumožňují úpravy MIME formátu, nebo odkazovat uživatele na stránku, která neumožňuje úpravy MIME zdroje.

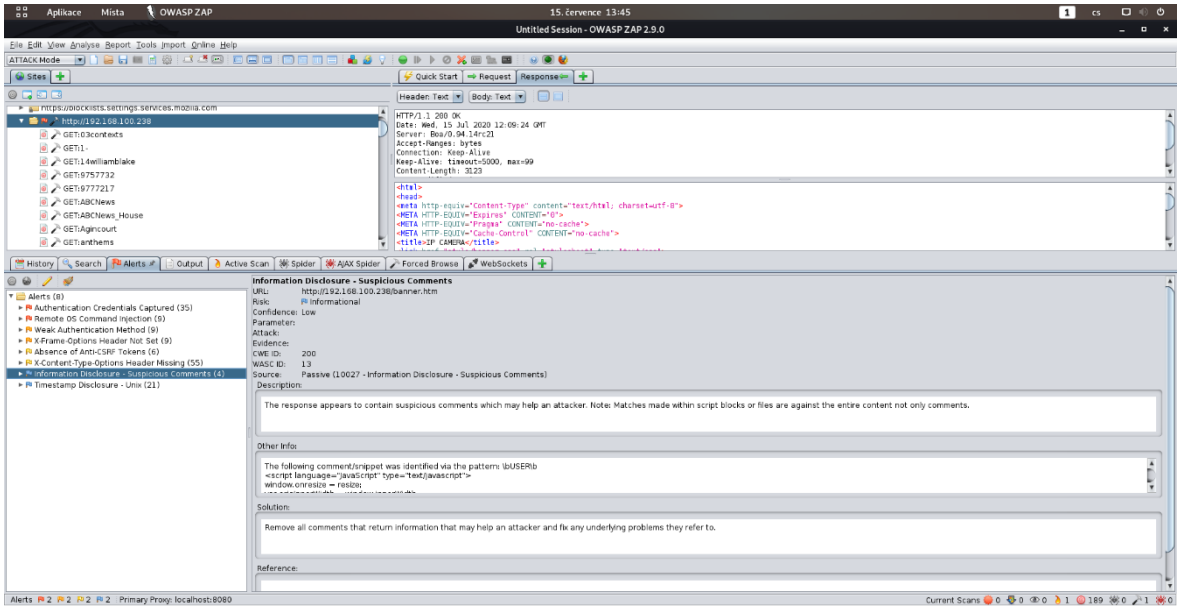


Obrázek č. 19. – OWASP ZAP – X-Content-Type-Options Header missing

Rada, nebo tip toho, jak zlepšit webovou aplikaci, která byla testována, je „Informations Disclosure – suspicious comments“ (viz obrázek č. 20.). Naznačuje a doporučuje, aby byly odstraněny veškeré komentáře, které mohou pomoci útočníkovi.

Opatření vůči této zranitelnosti:

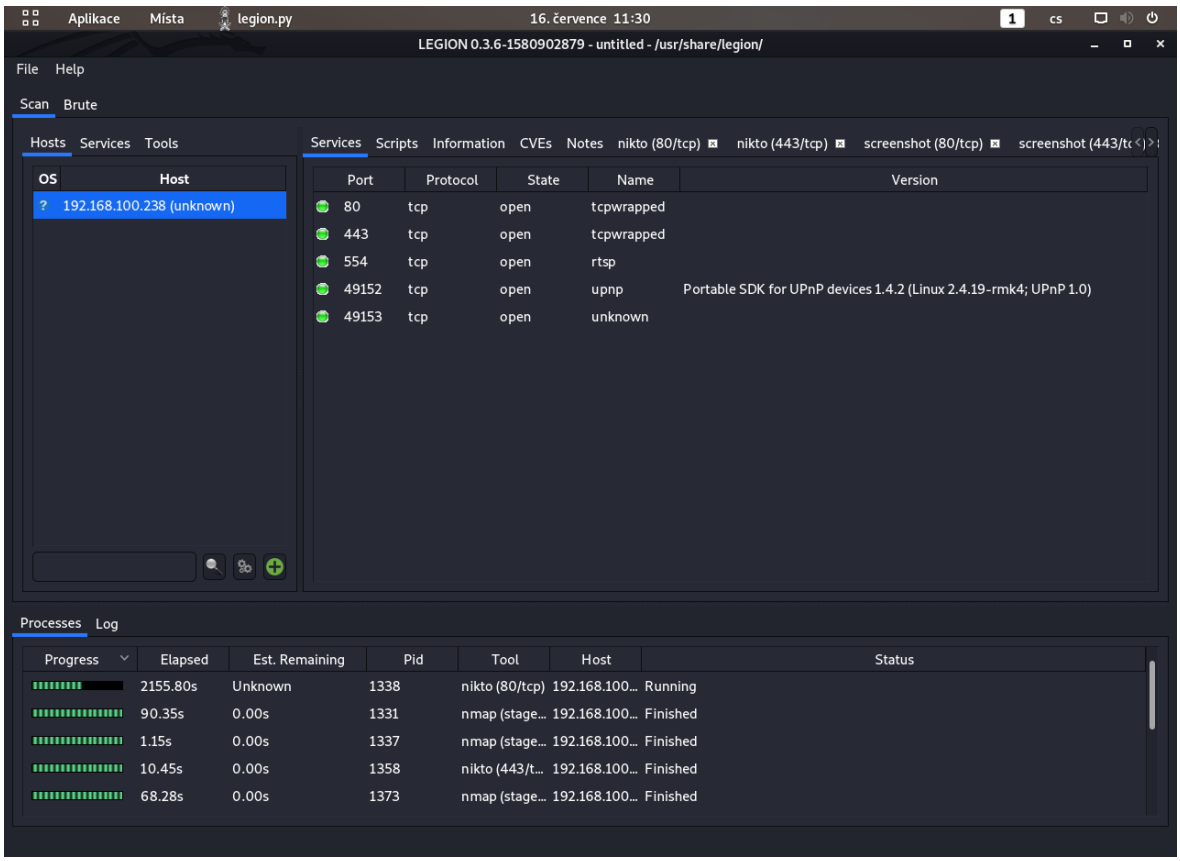
- Odstranit veškeré komentáře



Obrázek č. 20. – OWASP ZAP – Informations Disclosure – Suspicious Coments

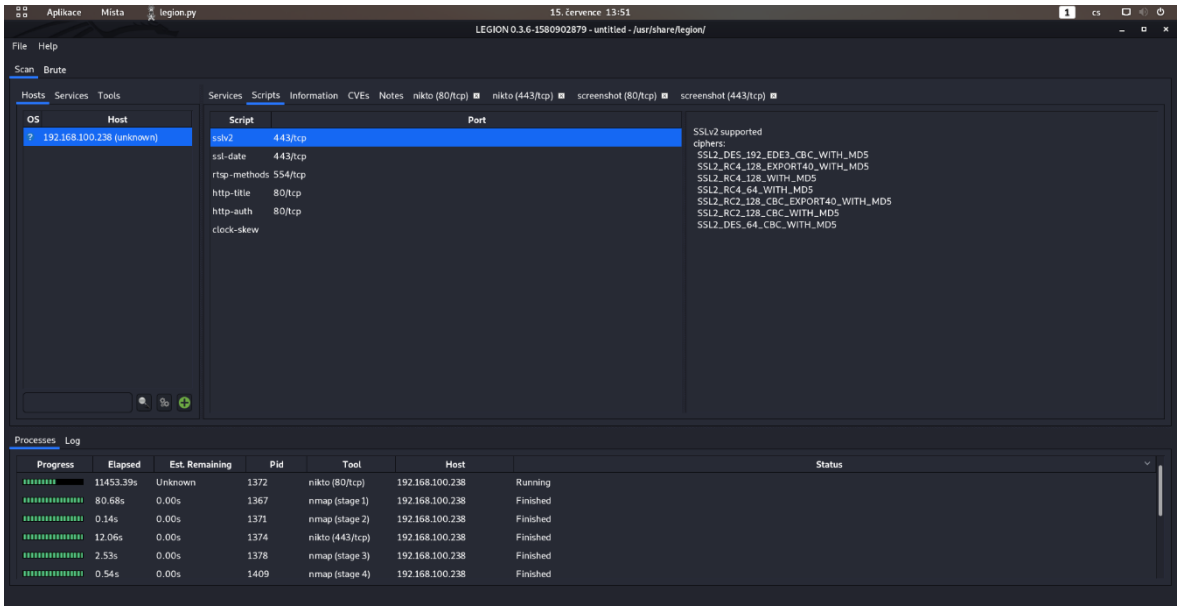
4.3.2 SPARTA – Legion

Při použití nástroje Legion, dříve známého jako SPARTA, byly zjištěny informace o zranitelnostech na testované webové aplikaci.



Obrázek č. 21. – Legion – Services

Obrázek č. 21. ukazuje již výsledky z testování v nástroji Legion. Po zadání IP adresy ji Legion oskenoval a ukázal otevřené porty dané IP adresy a který protokol používá, to lze vidět v záložce „Services“. V dalších záložkách vedle „Services“ lze vidět různé výsledky daného skenu, které jsou znázorněny níže. Ve spodní části nástroje se nachází záložka jménem „Processes“, což jsou procesy, které byly provedeny nebo se stále provádějí.



Obrázek č. 22. - Legion – Scripts

Na obrázku č. 22. lze vidět, jaké šifry podporuje testovaná adresa.

Podporované šifry:

- SSL2_DES_192_EDE3_CBC_WITH_MD5
- SSL2_RC4_128_EXPORT40_WITH_MD5
- SSL2_RC4_128_WITH_MD5
- SSL2_RC4_64_WITH_MD5
- SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
- SSL2_RC2_128_CBC_WITH_MD5
- SSL2_DES_64_CBC_WITH_MD5

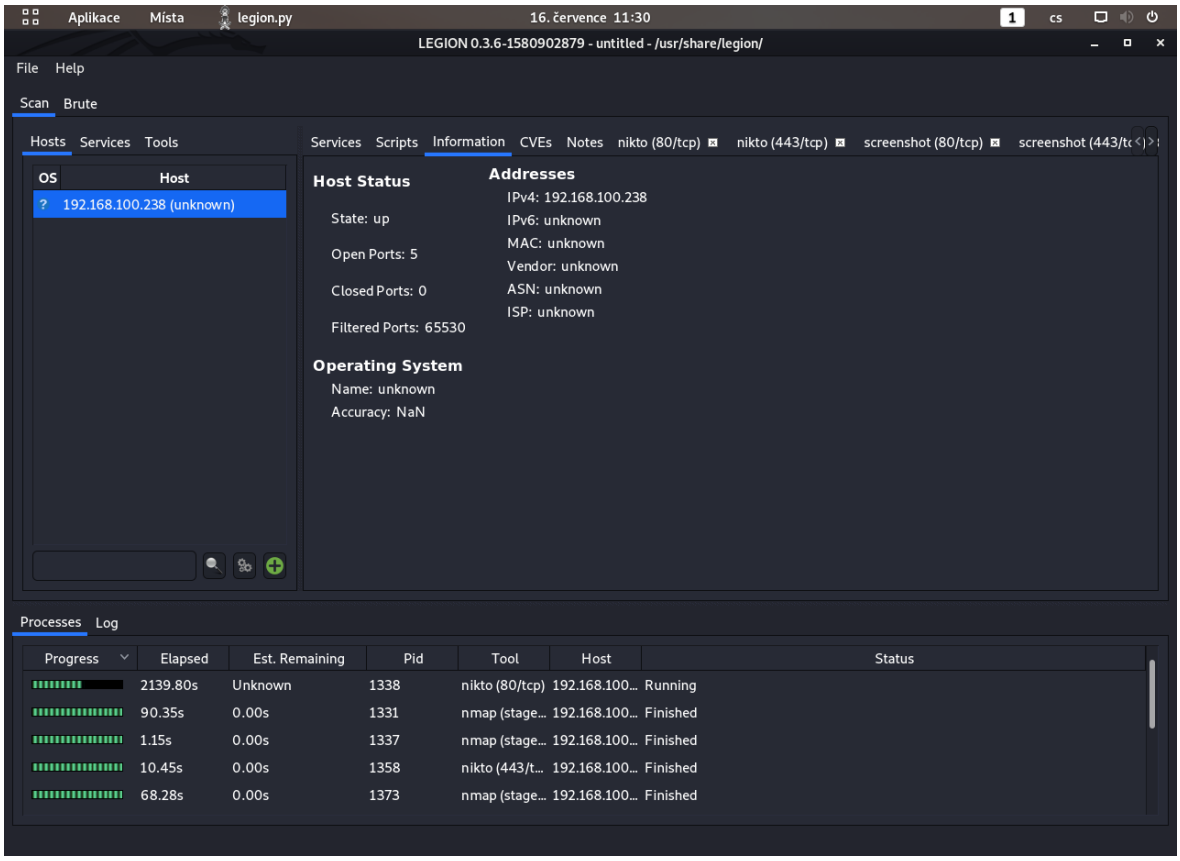
Z čehož vychází, že veškeré šifry, které jsou podporované v tomto případě, jsou zastaralé a lehko prolomitelné. V podporovaných šifrách se nacházejí symetrické šifry, což znamená, že k šifrování používají pouze jeden klíč a to privátní. Tyto šifry jsou: DES, RC2, RC4.

Další důležitá věc je ta, že tyto šifry nepoužívají dostatek bitů k zašifrování, a právě proto jsou snadněji prolomitelné než ty novější. Samozřejmě každým rokem jsou šifry zlepšovány

a je vhodné přizpůsobovat se aktuálním verzím tohoto typu zabezpečení. Z nástroje lze vidět, že podporované velikosti bitů u šifer jsou následující: 64,128,192.

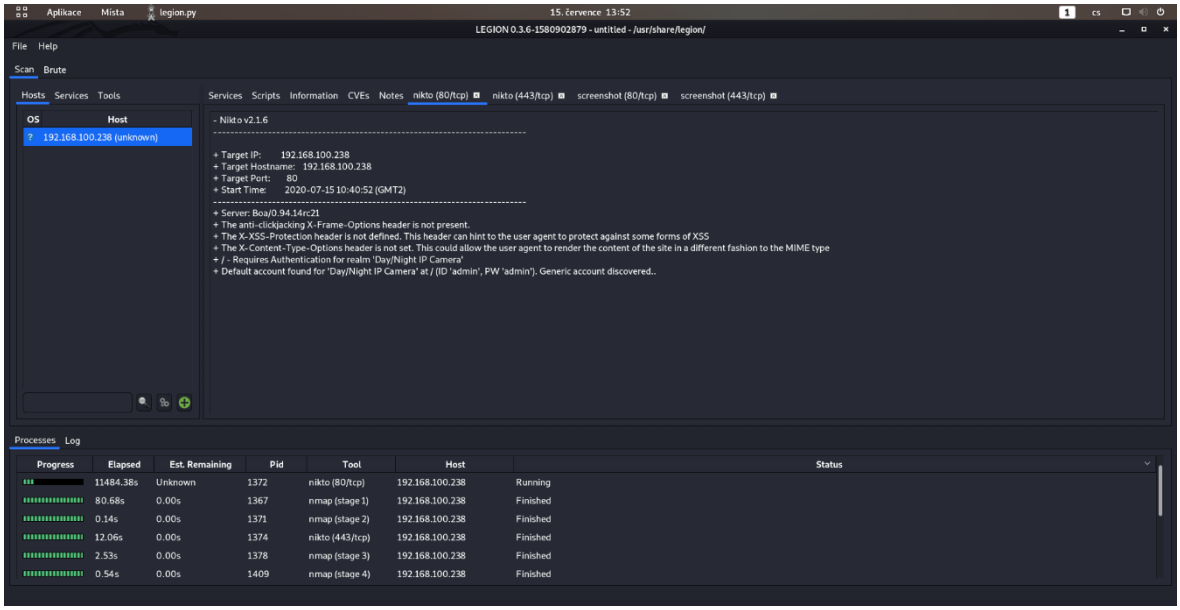
MD5 je zastaralý způsob šifrování a lepší náhradou tohoto šifrování jsou SHA-256, SHA-384, SHA-512 a novější.

Co se týče CBC, tedy „Cipher Block Chaining“ z anglického překladu řetězení šifrových bloků, je sice hojně používán, avšak má nevýhodu právě tu, že každý šifrovaný blok je závislý na tom předchozím. Lepší náhradou tohoto typu šifrování by bylo použít blokovou šifru AES-128, AES-192, AES-256, a novější.



Obrázek č. 23. – Legion – Information

Na obrázku č. 23. lze vidět informace týkající se skenu na testované adrese. Lze vidět, kolik otevřených či zavřených portů se nachází na dané adrese, a dodatečné informace.



Obrázek č. 24. – Legion – nikto

Na obrázku č. 24. je znázorněn výsledek ze skriptů nikto, který objevil zranitelnosti typu:

- Webová stránka neobsahuje implementaci anti-clickjacking ochrany v bezpečnostní hlavičce X-Frame-Options
- Webová stránka neobsahuje bezpečnostní hlavičku X-XSS-Protection
- Webová stránka neobsahuje bezpečnostní hlavičku X-Content-Type-Options
- Defaultní přihlašovací údaje na dané adrese.

4.4 Využití skriptu pro získání přístupu do webových kamer

V této oblasti praktické části byly vytvořeny seznamy defaultních přihlašovacích údajů a nejpoužívanější hesla. Tyto přihlašovací údaje by mohly být využity k zjištění přihlašovacích údajů pomocí skriptu v robot frameworku (či jiném automatizačním nástroji pro webové aplikace). V další části byly popsány scénáře možného útoku pomocí skriptů, které fungují na bázi znalých slovníkových seznamů loginů a hesel.

4.4.1 Testování slabých hesel

V této kapitole jsem se věnovala nalezení zveřejněných databází hesel a loginů, nejčastěji používaných hesel po celém světě a defaultních hesel ke kamerám od různých výrobců (viz příloha obsah cd). Tyto databáze hesel by mohly být použity k nalezení správného hesla pomocí skriptu v robot frameworku.

4.4.2 Testování v robot framework

Pro použití skriptu pro získání přihlašovacích údajů z pohledu útočníka je první nutné zjistit 4 základní údaje, a to:

- Znalost IP adresy / url
- Přístup do lokální sítě / nebo kamera se nachází na veřejné síti
- Znalost jména a hesla
- Znalost login tlačítka

V testovaném prostoru se jedná o:

- IP: 192.168.100.238
- Přístup do lokální sítě
- Znalost jména a hesla: admin;admin – lze použít databáze jmen a hesel
- Znalost login tlačítka

V případě kamery připojené do veřejné sítě by se jednalo o:

- Využití veřejného přístupu k síti
- Získání IP adresy
- Využití databáze jmen a hesel
- Zjištění login tlačítka pomocí zobrazení zdrojového kódu stránky, kde jej lze najít. V případě, kdy nelze najít login tlačítko, lze použít různé doplňky v prohlížeči, které zjišťují cestu k danému tlačítku jednodušeji.

4.4.3 Testování přihlašovacích údajů na základě databází

V této oblasti praktické části byly vytvořeny seznamy defaultních přihlašovacích údajů a nejpoužívanější hesla. Tyto přihlašovací údaje by mohly být využity k zjištění přihlašovacích údajů pomocí skriptu v robot frameworku. V další části byly popsány scénáře možného útoku pomocí skriptů, které fungují na bázi slovníkového útoku. Jde o útok, který využívá databázi známých a frekventovaných sad loginů a hesel. Vše je za předpokladu, že útočník má znalost IP adresy webové stránky. Hlavní zaměření tohoto skriptu je tedy na login, kde zdůrazňuji, že kamery většinou nemají ochranu „fail to ban“, což znamená, že po určitém počtu špatného zadání přihlašovacích údajů stránka nezablokuje daného uživatele na definovaný čas. Tento skript byl a bude funkční, pouze pokud útočník má přístup k login page kamery.

4.4.3.1 Způsob útoku na kameru pomocí skriptu pro získání přihlašovacích údajů

V případě, kdy je možné kameru vidět, tedy buď je napojená do veřejné sítě, nebo má útočník přístup do lokální sítě (např. fyzické napojení do ethernetové zásuvky, kde kamera není oddělena na síti), je možné provést tento útok. Útočník musí prvně zjistit IP adresu, fieldy a buttony, které jsou důležité indikátory pro skript. Pak se spustí skript, pomocí kterého se zjistí správné loginy a hesla, jenž následně tyto parametry zadá a vyzkouší každé jednotlivé jméno a heslo, a jakmile narazí na to správné a uspěje, test ukončí a vypíše správné přihlašovací údaje. Na získání správných loginů a hesel je definován zdroj, ve kterém jsou uloženy textové soubory s databázemi defaultních přihlašovacích údajů nebo těmi údaji, které byly již prolomeny (viz příloha). Příklady toho, jak vypadá takový skript, se nachází v příloze obsah cd.

4.4.3.2 Princip fungování přiložených skriptů

Jedná se o kombinaci skriptů v jazyce Python (soubor .py) a skriptů pro Robot Framework (soubory .robot).

Skript „keywords.robot“ obsahuje základní funkci pro kontrolu, zdali kombinace login/heslo je validní přihlašovací kombinace, či ne. Skript využívá na vstupu dvojici stringů – login + heslo.

Skript „vars.robot“ slouží pro uložení údajů, které jsou potřebné pro fungování skriptu. Slouží pro uložení informací, které jsou využité k navigaci v rámci přihlašovací stránky (rozhraní) kamery. Pro přihlášení je tedy nutné znát parametr určující pole pro login, dále pro heslo a parametry pro identifikaci a kliknutí na tlačítko odeslání informací k zalogování. A nakonec je nutné znát URL či IP rozhraní pro login.

Skript v jazyce Python „GenerujTestKomplet.py“ slouží pro vytvoření testovacího skriptu „Skript-LoginyAHeslo.robot“. Skript má na vstupu zvolené slovníky pro loginy a hesla.

Výsledný skript „Skript-LoginyAHeslo.robot“ tedy na základě „keywords.robot“ a „Vars.robot“ otestuje a zaznamená, který z dvojice login/heslo je validní a který není. Výsledky jsou uloženy do souboru „loginsExisted.txt“

ZÁVĚR

Cílem této bakalářské práce bylo nastudovat a popsat problematiku spojenou s kybernetickou bezpečností webových kamer. Dále popsat a otestovat vybrané webové kamery z pohledu kybernetické bezpečnosti a prezentovat výsledky. V teoretické části se věnuji problematice spojené s bezpečností webových kamer. V této části jsem tedy nastudovala velké množství literatury a následně sepsala ty nejdůležitější pojmy, spojené se zadanou problematikou. Dalším krokem v této části bylo sepsat termíny možných zranitelností a hrozeb, spojené s kybernetickou bezpečností webových kamer. Dále jsou pak vysvětleny zranitelnosti, hrozby a následná bezpečnostní opatření. Poslední splněný bod v teoretické části byl výběr vhodných prostředků pro testování webových kamer, kde byly popsány a vysvětleny testovací nástroje.

K testování webových kamer byly zvoleny nástroje OWASP ZAP tool, Legion a Robot framework. OWASP ZAP tool společně s Legionem testuje TOP 10 základních zranitelností webových aplikací a pomocí robot frameworku byl vytvořen skript pro testování přihlašovacích údajů na základě databází. Pro webové veřejné kamery byly zvoleny shodan, abuseIPDB, security headers.

V praktické části byly otestovány vybrané IP kamery, které jsou na internetu veřejně dostupné, byly zjištěny jejich zranitelnosti, sepsány možné hrozby z pohledu útočníka a následná opatření. Byla vybrána jedna kamera, která byla otestována přímo fyzicky, a dalších 15 veřejně dostupných na internetu online. Fyzicky dostupná kamera byla otestována v nástroji OWASP ZAP tool, legion a webové kamery online byly otestovány nástroji AbuseIPDB a security headers. Dále byly popsány možné hrozby a scénáře útoků přes ostatní zařízení, hrozby spojené s kamerou samotnou a hrozby spojené s kamerou připojenou do veřejné sítě. Výsledky z testování webových kamer jsou takové, že většina kamer je v základu nezabezpečená a je nutné je zabezpečit přes nastavení sítě a routeru. Hlavní věc, kterou je potřeba zmínit je, že většina kamer poskytuje přenos v síti přes 80 port, což je http připojení, kde je jejich velká slabina, protože útočníci mohou odposlouchávat komunikaci a veškeré informace probíhající mezi uživatelem a serverem, například přihlašovací údaje. Dále kamery v základu nemají nastavené security headers a to kvůli svému firmware. Jediná opatření vůči tomuto jsou zabezpečení sítě, které je již zmíněno výše a v přístupu k rozhraní kamery. Další věc je ta, že majitelé ponechávají přednastavené přihlašovací údaje, či nezmění přihlašovací údaje na dostatečně silné proti prolomení. To samé platí u IoT či jiná

zařízení v síti s kamerami, kde je nutné dbát na zabezpečení všech zařízení, která jsou připojená k internetu, protože jakmile se útočník dostane do lokální sítě přes tyto zařízení, získá tím i přístup k webové kameře.

Do budoucnosti by bylo možné navrhnout aplikaci pro testování webových kamer, nebo hlubší testování jedné IP adresy webové kamery a testování této kamery z různých hledisek kybernetické bezpečnosti. Také by bylo vhodné koupit dvacet až třicet nejznámějších kamer, které se prodávají a otestovat je na všechny zranitelnosti zmiňované v této bakalářské práci. Další možná tématika z pohledu této bakalářské práce je tvorba dostatečně bezpečných hesel k zařízením připojeným do internetu, případně ke kamerám. Výše popsané problematiky by mohly být využity při zpracování diplomové práce.

SEZNAM POUŽITÉ LITERATURY

[1] Kamera: Definice. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2012, 13.12.2012 [cit. 2020-02-22]. Dostupné z: wiki.knihovna.cz

[2] ŠEVČÍK, Ing. Jiří. Princip činnosti, typy a komunikační rozhraní IP kamer. Tzbinfo: Nejnavštěvovanější odborný portál pro stavebnictví a technická zařízení budov [online]. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství: © Copyright Topinfo s.r.o. 2001-2020, všechna práva vyhrazena., 2013, 21.10.2013 [cit. 2020-01-16]. ISSN ISSN 1801-4399. Dostupné z: https://elektro.tzb-info.cz/10480-princip-cinnosti-typy-a-komunikacni-rozhrani-ip-kamer

[3] Jm-elektro: Jm-Elektro s.r.o. komplexní elektroinstalace. Jm-elektro: Jm-Elektro s.r.o. komplexní elektroinstalace [online]. Jana Palacha 1297 Zelené Předměstí 530 02 Pardubice: © 2020. JM - Elektro s.r.o, 2009, 2020 [cit. 2020-02-22]. Dostupné z: jmelektro.cz

[4] MIČULKA, Bc. Tomáš. Bezpečnostní projekt využití dohledového videosystému v obci Palkovice. Otrokovice, 2017. Diplomová práce. Vysoká škola báňská - Technická univerzita Ostrava. Vedoucí práce Ing. Věra Holubová, Ph.D.

[5] HUSTVEDT. Wikipedia: Closed-circuit television. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2008, 27.1.2008 [cit. 2020-02-22]. Dostupné z: en.wikipedia.org/wiki

[6] SMEJKAL, Petr. Nejlepší webkamery: Testy, recenze a rady jak vybrat. Testado: Recenze, testy, žebříčky [online]. Malé náměstí 14/30 500 03 Hradec Králové: Affiliana, 2019, 24.9.2019 [cit. 2020-02-22]. Dostupné z: www.testado.cz

[7] Wirecutter: The Best Webcams. In: Wirecutter: The Best Webcams [online]. New York: A New York Times Company, 2019, 11.12.2019 [cit. 2020-02-22]. Dostupné z: thewirecutter.com

[8] KYNCL, Jaromír. KAMEROVÉ SYSTÉMY. ABAS Report: KAMEROVÉ SYSTÉMY [online]. Jankovcova 1569/2c, 170 00 Praha 7: ABAS Report © All rights reserved, (ČASOPIS 01) [cit. 2020-01-16]. Dostupné z: http://www.abasreport.cz/casopisy/2012-10-19-12-33-41/kamerove-systemy

[9] SABO, Bc. Martin. IPsecure.cz s.r.o.: IP kamerový systém vs. CCTV. In: IP-secure.cz s.r.o.: IP kamerový systém vs. CCTV [online]. Nuselská 211/120, 140 00 Praha 4 - Michle: IPsecure.cz s.r.o., Nuselská 211/120, 140 00 Praha 4 - Michle, 2012, 12.6.2012 [cit. 2020-02-22]. Dostupné z: www.ipsecure.cz

[10] How to hack a CCTV camera with primitive methods. Youtube [online]. San Bruno, California.: © 2020 Google, 2015, 17. 3. 2015 [cit. 2020-03-11]. Dostupné z: https://www.youtube.com/watch?v=rZoslioj1zg&list=PLuHnomT-dqVVJE_WpVufD-g52cKo8ZAEuw&index=2&t=0s

[11] Riziko. Ministerstvo vnitra České Republiky [online]. Praha: © 2019 Ministerstvo vnitra České republiky, 2019, 2003 [cit. 2020-03-11]. Dostupné z: https://www.mvcr.cz/clanek/riziko.aspx

[12] Hrozba: obecné pojmy. Ministerstvo vnitra České Republiky [online]. Praha: © 2019 Ministerstvo vnitra České republiky, 2019, 2003 [cit. 2020-03-11]. Dostupné z: https://www.mvcr.cz/clanek/hrozba.aspx

[13] ČERMÁK, Miroslav. Slabina vs. zranitelnost a jaký je mezi nimi vztah. Clever and smart [online]. © 2008 - 2020, Miroslav Čermák, 2008, 12. 07. 2018 [cit. 2020-03-11]. Dostupné z: https://www.cleverandsmart.cz/slabina-vs-zranitelnost-a-jaky-je-mezi-nimi-vztah/

[14] Kybernetická bezpečnost (Cyber Security): Standardy kybernetické bezpečnosti. Cybersecurity.cz: Kybernetická bezpečnost a obrana [online]. Copyright Cyber-Security.cz (c) 2010 - 2018, 2017, 1.11.2017 [cit. 2020-01-16]. Dostupné z: https://www.cybersecurity.cz/basic.html

[15] DŽUBÁK, Josef. Phishing: CO JE TO PHISHING. Hoax [online]. Copyright 2000-2020 Josef Džubák & HOAX.cz Code & design DIGITAL ACTION, 2000 [cit. 2020-03-11]. Dostupné z: https://www.hoax.cz/phishing/co-je-to-phishing

[16] KYSILKA, Radek. Jak vzniká spam a jak se mu bránit. Lupa.cz [online]. Copyright © 1998 – 2020 Internet Info, 2003, 26. 6. 2003 [cit. 2020-03-11]. ISSN 1213-0702. Dostupné z: https://www.lupa.cz/clanky/jak-vznika-spam-a-jak-se-mu-branit/

[17] DŽUBÁK, Josef. HOAX: HOAX. Hoax [online]. Copyright 2000-2020 Josef Džubák & HOAX.cz Code & design DIGITAL ACTION, 2000 [cit. 2020-03-11]. Dostupné z: https://www.hoax.cz/hoax/

[18] DŽUBÁK, Josef. MALWARE: MALWARE. Hoax [online]. Copyright 2000-2020 Josef Džubák & HOAX.cz Code & design DIGITAL ACTION, 2000 [cit. 2020-03-11]. Dostupné z: https://www.hoax.cz/hoax/

[19] Počítačový virus. AVAST: Avast Free Antivirus [online]. Praha: 1988-2016 Copyright AVAST Software, 2020 [cit. 2020-03-11]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus

[20] Spyware. AVAST: Avast Free Antivirus [online]. Praha: 1988-2016 Copyright AVAST Software, 2020 [cit. 2020-03-11]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus

[21] Keylogger. AVAST: Avast Free Antivirus [online]. Praha: 1988-2016 Copyright AVAST Software, 2020 [cit. 2020-03-11]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus

[22] Trojský kůň. AVAST: Avast Free Antivirus [online]. Praha: 1988-2016 Copyright AVAST Software, 2020 [cit. 2020-03-11]. Dostupné z: https://www.avast.com/cs-cz/c-computer-virus

[23] Co to je DDoS útok a jak se dělá? In: Diit: Deep in it [online]. Copyright © 1998-2020 CDR server, 2012, 24. 1. 2012 [cit. 2020-03-11]. ISSN 1804-5405. Dostupné z: https://diit.cz/clanek/co-to-je-ddos-utok-a-jak-se-dela

[24] OULEHLA, Ing. Milan. Hodnota informace, Firewally, Antiviry, spam a problematika uživatelského přístupu. Možnosti zabezpečení osobního počítače (Bios, OS, šifrování, Tokeny). Zlín.

[25] IPS: IPS. IT slovník [online]. © 2008 - 2020 IT-Slovnik.cz team, 2008 [cit. 2020-03-11]. Dostupné z: https://it-slovnik.cz/pojem/ips

[26] Zranitelnost (Vulnerability). In: ManagementMania.com [online]. Wilmington (DE) 2011-2020, 11.04.2016 [cit. 27.01.2020]. Dostupné z: https://managementmania.com/cs/zranitelnost-vulnerability

[27] Zranitelnost: Zranitelnost. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2019, 27. 4. 2019 [cit. 2020-01-27]. Dostupné z: cs.wikipedia.org

[28] ČÍŽEK, Jakub. Zive: IoT je děravý. Na webu jsou tisíce soukromých kamer a síťových krabiček. Živě: Počítače [online]. Czech News Center: Czech News Center, 2016, 21. ledna 2016 [cit. 2020-02-03]. Dostupné z: https://www.zive.cz/clanky

[29] Shodan [online]. © 2013-2020, All Rights Reserved - Shodan®, ©2013-2020 [cit. 2020-02-03]. Dostupné z: https://www.shodan.io/

[30] Google [online]. Menlo Park, Kalifornie, USA: Alphabet, 1998 [cit. 2020-02-03]. Dostupné z: https://www.google.com/

[31] Insecam [online]. [cit. 2020-02-03]. Dostupné z: www.insecam.org

[32] Bezpečnostní hrozby ve virtualizovaném prostředí. Systems Online: S přehledem ve světě informačních technologií [online]. Brno: © 2001 - 2020 CCB spol. s r.o., 2020, 2001 - 2020 [cit. 2020-03-30]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/virtualizace/bezpecnostni-hrozby-ve-virtualizovanem-prostredi.htm

[33] ING. MALÁNIK, David Ph.D. Bezpečnost ve firemním prostředí, Podnikové FW, Phishing, Pharming, Sociální inženýrství, Cross Site Scripting, DoS, DDoS, …: Cross site scripting. UTB Zlín. Zlín.

[34] RŮŽIČKA, Vojtěch. Zdrojak: 10 nejzávažnějších zranitelností webových aplikací podle OWASP. Zdrojak [online]. Praha: Devel.cz Labs, 2018, 26.4.2018 [cit. 2020-03-31]. ISSN 1803-5620. Dostupné z: www.zdrojak.cz/

[35] RYBKA, Jakub. Kybernetická bezpečnost: Kybernetickou bezpečnost dělíme na několik fází:. HCV: Kybernetická bezpečnost [online]. Chodská 1203, 756 61 Rožnov pod Radhoštěm [cit. 2020-01-16]. Dostupné z: https://www.hcvit.cz/bezpecnost?gclid=CjwKCAiA6vXwBRBKEiwAYE7iSzADJX0uDkqcAxO-OFRSOr14LWkKtjyWNBYtBZ844pdzZybSg-iG3cBoC_c8QAvD_BwE

[36] CHRISTENSSON, Per. Python Definition: Python. TechTerms: The Computer Dictionary [online]. © 2020 Sharpened Productions, 2005, 15. Června 2010 [cit. 2020-04-11]. Dostupné z: https://techterms.com

[37] CHRISTENSSON, Per. SQL Definition: SQL. TechTerms: The Computer Dictionary [online]. © 2020 Sharpened Productions, 2005, 6. března 2007 [cit. 2020-04-11]. Dostupné z: https://techterms.com

[38] Typy uživatelských rozhraní a jejich specifika/old: Uživatelské rozhraní - User interface. WikiSofia [online]. Česká republika: © 2013 ISSN: 2336-5897, 2013 [cit. 2020-04-11]. ISSN 2336-5897. Dostupné z: http://wikisofia.ff.cuni.cz/wiki/Typy_u%C5%BEivatelsk%C3%BDch_rozhran%C3%AD_a_jejich_specifika/old

[39] Webová aplikace (Web Application). In: ManagementMania.com [online]. Wilmington (DE) 2011-2020, 18.10.2018 [cit. 11.04.2020]. Dostupné z: https://managementmania.com/cs/webova-aplikace-web-application

[40] CO JE TO API (APPLICATION PROGRAMMING INTERFACE): API (APPLICATION PROGRAMMING INTERFACE). Topranker [online]. Praha, Pod pekárnami 245/10: Topranker.cz, 2019 [cit. 2020-04-11]. Dostupné z: https://topranker.cz/slovnik/co-je-to-api-application-programming-interface/

[41] What exactly is an Application Binary Interface (ABI)? Who defines it (the operating system, a programming language)?: 3 Answers. Quora [online]. 605 Castro St Mountain View, CA 94041, Spojené státy americké: © Quora Inc. 2020, 2013, 28. srpna 2013 [cit. 2020-04-11]. Dostupné z: https://www.quora.com/What-exactly-is-an-Application-Binary-Interface-ABI-Who-defines-it-the-operating-system-a-programming-language

[42] CO JE TO GUI (GRAFICKÉ UŽIVATELSKÉ ROZHRANÍ): GUI (GRAFICKÉ UŽIVATELSKÉ ROZHRANÍ). Topranker [online]. Praha, Pod pekárnami 245/10: Topranker.cz, 2019 [cit. 2020-04-11]. Dostupné z: https://topranker.cz/slovnik/gui-graficke-uzivatelske-rozhrani/

[43] SIVAK, Stanislav. Nmap - Ububtu Manpage Repository. Ubuntu manuals: Ubuntu Manpage Repository [online]. © 2019 Canonical Ltd. Ubuntu and Canonical, 2017, 31. července 2017 [cit. 2020-04-11]. Dostupné z: http://manpages.ubuntu.com/manpages/cosmic/sk/man1/nmap.1.html

[44] Security Headers. SSLmentor: TLS/SSL certifikáty pro kvalitní HTTPS zabezpečení webových stránek a internetových projektů. [online]. Nové sady 988/2 602 00 Brno: © 2016 - 2019 Web security s.r.o. | SSLmentor.cz, 2019, 2016 - 2019 [cit. 2020-04-11]. Dostupné z: https://www.sslmentor.cz/napoveda/security-headers

[45] Security Headers: Vše, co jste kdy chtěli vědět o Security Headers (ale báli jste se zeptat) na jednom místě. Security Headers [online]. Nové sady 988/2, 602 00 Brno-střed: Copyright © 2018 Web security, 2018 [cit. 2020-04-11]. Dostupné z: https://securityheaders.cz/

[46] Kali linux: Co je Kali linux. HackerLab: Hacking kurzy [online]. V Poli 547 517 71 České Meziříčí: © 2020 Hackerlab HackingKurzy.cz, 2020 [cit. 2020-04-11]. Dostupné z: https://www.hackingkurzy.cz/blog/kali-linux/

[47] KALI: By offensive security [online]. © OffSec Services Limited 2020 [cit. 2020-04-11]. Dostupné z: https://www.kali.org/

[48] QUINA, Antonio a Leonidas STAVLIOTIS. Sparta Package Description. KALI TOOLS: Kali Linux Penetration Testing Tools [online]. © OffSec Services Limited 2020 [cit. 2020-04-11]. Dostupné z: https://tools.kali.org/information-gathering/sparta

[49] SSL Labs. Qualys: SSL Labs [online]. Copyright © 2009-2020 Qualys, 2020 [cit. 2020-04-11]. Dostupné z: https://www.ssllabs.com/

[50] ROBOT FRAMEWORK: INTRODUCTION. ROBOT FRAMEWORK [online]. Pohjoinen Rautatiekatu 25, 00100 Helsinki [cit. 2020-04-11]. Dostupné z: https://robotframework.org/

[51] Introduction: Overview. ZAP: Zed Attack Proxy (ZAP) [online]. © Copyright 2020 the ZAP Dev Team [cit. 2020-04-11]. Dostupné z: https://www.zaproxy.org/docs/api/#introduction

[52] ING. BLÁBOLIL, Roman. Virtualizace VMware vSphere [online]. České Budějovice, 2014 [cit. 2020-04-11]. Dostupné z: http://www.soscb.cz/zabezpeceno2/opvk/vmware.pdf. Projekt OPVK „Vyškolený pedagog – záruka kvalitní výuky“. Střední odborná škola veterinární, mechanizační a zahradnická a Jazyková škola. Vedoucí práce Roman Blábolil.

[53] VMware Workstation 15 Player: VMware Workstation Player. VMware [online]. Palo Alto, Kalifornie, USA: © 2020 VMware [cit. 2020-04-11]. Dostupné z: https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html

[54] BIDELMAN, Eric. Introduction to Feature Policy. Web Fundamentals [online]. Červen 2018, 2018 [cit. 2020-07-01]. Dostupné z: https://developers.google.com/web/updates/2018/06/feature-policy

[55] NGINX. NGINX [online]. Copyright © F5 [cit. 2020-07-01]. Dostupné z: https://www.nginx.com/

[56] APACHE. APACHE [online]. Copyright © 1997-2020 The Apache Software Foundation., 1997 [cit. 2020-07-01]. Dostupné z: https://httpd.apache.org/

[57] JACKSON, Brian. Hardening Your HTTP Security Headers. Keycdn [online]. Švýcarsko: © 2020 proinity LLC Made in Switzerland, 2019, 19 Června, 2019, 2019 [cit. 2020-07-01]. Dostupné z: https://www.keycdn.com/blog/http-security-headers

[58] Referrer Policy: W3C Candidate Recommendation. In: W3C [online]. Copyright © 2019 W3C ® (MIT, ERCIM, Keio, Beihang)), 2019, 26. ledna 2017 [cit. 2020-07-01]. Dostupné z: https://www.w3.org/TR/referrer-policy/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Access Control System – Přístupové systémy
A/D Převodník	Analogově digitální převodník
BS	Bezpečnostní standart
BSI	Britský standardizační institut
CCD	Charge-coupled device - Elektronická součástka používaná pro snímání obrazové informace.
CCTV	Closed Circuit Television – Uzavřený televizní okruh
CD	Compact Disc – Kompaktní disk
CMOS	Complementary Metal–Oxide–Semiconductor - způsob vytváření logických členů
CPU	Central Processing Unit - Centrální procesorová jednotka
DDoS	Distributed Denial of Service - Distribuované odmítnutí služby
DPPC	Dohledové a Poplachové Přijímací Centrum
DRAM	Dynamic Random Access Memory - Dynamická paměť s náhodným Přístupem
DSP	Digital Signal Processor - Digitální signálový procesor
DVD	Digital Versatile Disc - Formát digitálního optického datového nosiče
DVR	Digital Video Recorder - Digitální rekordér
EPS	Elektrická požární signalizace
.exe	Přípona pro spustitelný soubor operačního systému Windows
FTP	File Transfer Protocol - Protokol přenosu souborů
GPS	Global Positioning System - Globální polohový systém
http	Hypertext Transfer Protocol - Internetový protokol určený pro komunikaci s WWW servery

https	Hypertext Transfer Protocol Secure - Protokol umožňující zabezpečenou komunikaci v počítačové síti.
IDS	Intrusion Detection System - systém pro odhalení průniku
IPS	Instrusion Prevention Systems - systém prevence průniku.
IP Kamera	Síťová kamera využívající internetový protokol
IoT	Internet Of Things – Internet věcí
I/O	Input/Output - Vstup/výstup
ISO	International Organization for Standardization - Mezinárodní organizace pro normalizaci
ISO / IEC 27002	Doporučovaná opatření nutná pro samostatná specifikace systému bezpečnosti informací
ISO / IEC 27001	Samostatná specifikace systému bezpečnosti informací
LAN	Local Area Network - lokální síť / místní síť
MTF	Modulation Transfer Function – Modulační funkce přenosu
OCTV	Open Circuit Television – Otevřený televizní okruh
OS	Operation system - Operační systém
OSINT	Open source intelligence - Zpravodajství z otevřených zdrojů
PC	Personal Computer - Počítač
PTZ	Pan Tilt Zoom - Posunout, naklonit, přiblížit
PZTS	Poplachový zabezpečovací a tísňový systém
SHZ	Stabilní hasicí zařízení
USB	Universal Serial Bus - Univerzální sériová sběrnice
VMS	Video Management System - Systém pro správu videa
VSS	Video surveillance System - Dohledový videosystém
Wi-Fi	Wireless Ethernet Compatibility Aliance - Bezlicenční frekvenční pásmo

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: OBSAH CD

Struktura obsahu přiloženého CD:

- Adresář text bakalářské práce – obsahuje text bakalářské práce ve formátu PDF.

- Adresář skripty – obsahuje jeden skript v jazyce Python s názvem GenerujTest-Komplet s příponou .py a tři skripty napsané v nástroji robot framework, který má příponu .robot. Tyto soubory se nazývají Keywords, Skript-LoginyAHeslo a Vars.

- Adresář přihlašovacích údajů – obsahuje 8 souborů typu textového dokumentu ve kterém jsou sepsány seznamy loginů a hesel. Tyto soubory se nazývají top10logins, top10pass, Defaultní údaje pro username, names, Seznam Defaultních hesel pro kamery, Slovnikrockyou, TOP100 nejpoužívanějších hesel a TOP10000, kde jejich přípona je .txt.