Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Známé a neznámé hrozby na počítačových sítích a nástroje pro jejich detekci

Bakalářská práce

Autor: Michal, Gruber
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mls Karel, Ing. Ph.D.

Hradec Králové srpen 2020

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 14.8.2020 Michal Gruber

Poděkování:

Mé poděkování patří vedoucímu bakalářské práce Karlovi Mlsovi, Ing. Ph.D. za metodické vedení, cenné rady, ochotu a trpělivost, kterou mi v průběhu zpracování práce věnoval.

Anotace

Práce se zabývá zabezpečením počítačových sítí. V teoretické části práce jsou popsány hrozby jak známé, tak dosud neznámé, ale očekávané, obrana proti nim, techniky, nástroje, prevence a zabezpečení zejména bezdrátových sítí. Dále je řešena otázka, zdali jsme připraveni na budoucí vývoj útoků. Praktická část spočívá v ukázce správy sítě základními nástroji v operačních systémech Windows a Android oproti možnostem správy pomocí aplikace Fing. Výsledky jsou porovnány a zhodnoceny na konci práce.

Annotation

Title: Known and unknown threats on computer networks and detection tools

The Bachelor thesis deals with the security of computer networks. The theoretical parts contain description of known and unknown threats, but expected ones, protection against them, techniques, tools, prevention and security especialy of wireless networks. The question of whether we are ready for the future development of attacks. The practical part consists of a demonstration of network management with basic tools in Windows and Android compared to the possibilities of management tool Fing. The results are compared and evaluated at the end of work.

Obsah

Seznam obrázků

1 Úvod

Tato práce se zabývá zabezpečením počítačové sítě proti různým druhům útoků. Jsou zde zmíněny hrozby, řešení detekce útoků a zabezpečení.

Internet je oblíbený zdroj informací a komunikace, kde však číhá mnoho nebezpečí. Nárůst počtu přístrojů s možností připojení k síti zvyšuje riziko jeho napadení. Technologicky se očekává, že postupně budeme mít z dnes obyčejných věcí, chytrá zařízení. Vyvíjejí se například autonomní programy pro roboty a dopravní prostředky či domovní asistenti, přes které se dá ovládat celý dům. Zatím se jedná především o prototypy, nebo nejsou tolik rozšířené, což je jen otázka času. Dále se začne řešit ochrana, která by v tomto případě při prolomení systému mohla ohrozit lidské životy, tudíž by ovlivnila rozšíření, případně zánik produktu.

Zajištění ochrany je náročná věc, proto jsou programy, praktiky a doporučení, které pomáhají předejít problémům. V následujících kapitolách budou zkoumány možnosti, jak nejlépe zabezpečit síť. Práce by měla poučil znalé i neznalé a zvýšit povědomí o hrozbách, což by mohlo v budoucnu dost pomoci snížit počet napadených zařízení.

2 Hrozby známé i dosud neznámé

Tato kapitola se bude zabývat škodlivými programy a praktikami na počítačových sítích. Zmínka bude i o zabezpečení a ochraně. Dále je třeba mít na paměti, že všechny zmíněné útoky jsou protizákonné a každý úspěšný útok může narušit příjmy a ovlivnit veřejnou reputaci ať už firmy, tak jedince.

Útočník se zpravidla nazývá hacker. Hackeři se dělí na různé skupiny podle toho, jakými útoky se zabývají. Existují i tzv. etičtí hackeři, kteří jsou najímáni, aby testovali počítačové sítě a nacházeli slabiny. Díky tomu se zvýší zabezpečení před reálnými hackery, kteří by dělali to samé, jen nelegálně a se zlým úmyslem.

2.1 Známé hrozby

Nejznámější síťové útoky, které jsou specifické svým chováním. Lze je dělit podle mnoha kritérií, ale zde si je rozdělíme na dvě hlavní skupiny, a to na aktivní a pasivní. U každé hrozby budou možnosti protiopatření.

2.1.1 Pasivní útoky

Tyto typy útoků aktivně neovlivňují chování sítě. Jsou prováděny za účelem sběru dat, tedy útočník monitoruje síťovou komunikaci nebo hledá mezery v zabezpečení. Tyto informace se následně využívají při aktivních útocích.

2.1.1.1 Odposlouchávání

Dochází k neoprávněnému sledování a zachytávání lokálního síťového provozu. Zaměřuje se na odchytávání paketů, které jsou zasílány v síti mezi počítači. Zde se snaží získat užitečné informace typu přístupových údajů nebo jiných citlivých dat, případně jak prolomit nebo poškodit danou internetovou síť. Využívá se techniky sniffing (čmuchání), která se běžně využívá při diagnostikách sítě, ale v nesprávných rukách může být použita jako útok [1]. Software se nazývá sniffer. Sniffing se často přirovnává k praktikám jako je keylogger nebo spyware, které ovšem nepatří mezi síťové hrozby. Keylogger slouží k zachytávání zmáčknutých kláves a spyware monitoruje aktivity na určitém počítači. Všechny tyto praktiky se snaží získat citlivé údaje o uživateli, aniž by je nějak pozměnily, ale každá praktika má svoji slabinu a jiné využití.

Nejjednodušší obranou proti odposlechu je šifrování dat [2]. Proto je dobré se vyvarovat nezabezpečeným bezdrátovým sítím, kde není zaručeno šifrování dat a je tedy nebezpečné se kamkoliv přihlašovat nebo skrze síť posílat citlivé údaje.

2.1.1.2 Skenování

Jedna z nejstarších a dodnes používaných praktik je založena na vyslání požadavků na adresové porty serveru s úmyslem zjistit, které porty jsou spuštěné [3]. Stav portu může být aktivní, zavřený nebo neodpovídá. Aktivní stav odpoví na požadavek, že zde zařízení běží. Zavřený port také odpoví, ale požadavek odmítne, což přesto poskytne útočníkovi informaci, že zde zařízení je. Pokud port neodpovídá, znamená to, že ho blokuje firewall. Některé firewally dokáží tento útok poznat a na základě podezřelé IP adresy port zablokovat. Bylo by jednoduché všechny porty zablokovat, aby se je nedalo skenovat, jenže to je proti pravidlům TCP/IP. V podstatě se nedá efektivně bránit proti tomuto útoku, ale dá se jednoduše zjistit pomocí firewallu, že jeden host skenuje různé porty. Dá se zde záměrně využít zranitelného portu, který naláká útočníka, aby na něj zaútočil, ale ve skutečnosti se dostane do honeypotu, což je software určený, pro sledování útočníkova chování, průběhu útoku a informací, jak se tam dostal a odkud [4].
Existuje 65 536 odlišných portů. Podle čísla portu se dá zjistit, o jakou službu se jedná, a tudíž využít její zranitelnosti. Porty se dělí na známé (0-1023), registrované (1024-49151) a dynamické/soukromé (49152-65535) [3].

Nejznámější porty:
20 FTP data (File Transfer Protocol)
21 FTP (File Transfer Protocol)
22 SSH (Secure Shell)
23 Telnet
25 SMTP (Send Mail Transfer Protocol)
53 DNS (Domain Name Service)
68 DHCP (Dynamic Host Control Protocol)
80 HTTP (HyperText Transfer Protocol)
110 POP3 (Post Office Protocol, version 3)

115 SFTP (Secure File Transfer Protocol)
119 NNTP (Network New Transfer Protocol)
123 NTP (Network Time Protocol)
143 IMAP (Internet Message Access Protocol)
161 SNMP (Simple Network Management Protocol)
220 IMAP3 (Internet Message Access Protocol 3)
443 SSL (Secure Socket Layer)

2.1.2 Aktivní útoky

Po získání dostatečných informací přichází čas na aktivní útoky. Ty způsobují neautorizované změny chování sítě [5]. Pachatel dokáže prolomit zabezpečení nebo ochromit zařízení od jeho funkčnosti. Díky tomu ohrozí uživatele sítě nebo danou síť znepřístupní. Často je cílem pozměnění dat nebo klamání druhé strany připojení.

2.1.2.1 Maškaráda

Při tomto útoku se převezme cizí účet pro vlastní prospěch. Útočník odcizil přihlašovací údaje a převzal cizí identitu. Účinnost útoku se zvyšuje podle oprávnění zneužitého uživatele. Čím vyšší oprávnění, tím hrozivější škody může útočník napáchat. Uživatel s minimem oprávnění je pro útočníka nezajímavý [6].
Obrana je velice složitá, protože záleží na opatrnosti jak uživatele, co účet využívá, tak i na zprostředkovateli softwaru, proto je obtížné zjistit, jestli někdo přihlašovací data získal přímo od konkrétní osoby nebo přes chyby v softwaru [6].

2.1.2.2 Opakované přehrání

Útočník zpomaluje nebo opakuje přenos dat. Po odeslání zakódovaných dat je útočník zachytí. Cílová destinace data očekává, ale dostane je opakovaně nebo upravené pro zvýhodnění pachatele. Tímto může uškodit firmě v opakování důležitého úkonu. Typickým případem je poslání peněz, v tomto případě tedy proces může rozmnožit a ještě upravit, aby peníze přišly útočníkovi [7].
Jednoduchou obranou je používání časových razítek, tzv. timestamps. Další možností je mít pro každou platbu náhodně vygenerované jednorázové heslo, kdy po odeslání dané heslo přestane fungovat [7].

2.1.2.3 Spoofing

Neznámý zdroj se maskuje jako známý a snaží se uživatele oklamat. Jsou různé techniky, které se snaží uživatele zlákat k činnosti, co má za následek odcizení dat nebo rozšíření malware. Může být spouštěčem jiných vážnějších útoků jako je Man in the middle (MITM) nebo přetrvávající hrozba. Nejčastěji se provádí přes e-mail nebo telefon, ale v kontextu této práce se bude jednat o síťových útocích, jako jsou spoofing IP adresy, webové stránky, ARP (address resolution protocol) nebo DNS (domain name system) [8].

Obrana spočívá v pozornosti. Většinou si lze všimnout gramatických chyb, překlepů nebo nelogických vět.

Webová stránka

Internetová stránka napodobuje již existující stránku. Uživatelé při pokusu o registraci nebo přihlášení předají svá data útočníkovi [9].

Obranou je pozorně si hlídat certifikáty. Certifikát slouží něco jako podpis, že se jedná o originální důvěryhodnou stránku. Také udává, že obsah stránky je šifrován. Není třeba se tedy obávat, že by zde někdo ukradl posílaná data. Hodně navštěvované weby většinou mají certifikát, ale není to pravidlo. Pomocí prohlížeče je jednoduché zjistit, zdali stránka certifikát má nebo nemá. U platebních stránek je certifikát samozřejmostí. Složitějším opatřením je prohlídnout si pečlivě stránku skrze adresní řádek, design a kód, kde se může skrývat řada detailů, které vám napoví, že se nejedná o pravou stránku. Certifikát je nejspolehlivější, ale bohužel ho nemá každý web.

IP adresa

Útočník si změní IP adresu, aby změnil svoji totožnost a tvářil se, že je součástí sítě. V síti, kde se ověřuje skrze IP adresu, mu mohou ostatní posílat data, která mu nenáleží [8]. Tato technika se často využívá v DoS útocích, kde se útočník podle IP adresy tváří jako bezpečný zdroj, ačkoli tomu tak není [9].

ARP

Address resolution protocol slouží k překládání IP adres na MAC adresy. Útočník se snaží zneužít tohoto protokolu a propojit svoji MAC adresu s IP adresou uživatele sítě. Při úspěchu jsou data, která by měla směřovat k uživateli, směřována k útočníkovi. Tento útok je omezený pouze na lokální sítě, které tento protokol využívají [9].

DNS

Domain name systém převádí doménová jména na IP adresy. Ulehčuje si pamatování webových stránek. Každá webová stránka je přiřazená ke své IP adrese. Toho lze využít a při změně IP adresy u dotyčného doménového jména si ani nemusíme všimnout, že nás to přesměrovalo na jinou stránku. Zde nás útočník může napadnout malwarem nebo odcizit data [9].

2.1.2.4 Člověk uprostřed

Man in the middle (MITM), jak již název napovídá, jedná se o zprostředkovanou komunikaci přes útočníka. Dá se označit za aktivní odposlouchávání [5].

Pachatel je napojen jak na uživatele, tak na cílové spojení a zachytává veškeré informace, které mezi nimi putují. S těmito daty může libovolně manipulovat nebo je analyzovat. Dokonce dokáže provést DoS útok nebo převzít kontrolu nad počítačem oběti [5].

Bránit se dá šifrovanou komunikací HTTPS. U firem by mělo být zabezpečeno vniknutí do sítě, a to i fyzicky, což znamená po připojení útočníkova kabelu k síťovému prvku.

2.1.2.5 Pokročilá přetrvávající hrozba

Označováno jako APT (advanced persistent treat) je technika, kdy je úkolem se dostat do systému, vydržet tam co nejdéle a napáchat co nejvíce škod, nejčastěji sběrem informací. Cílem jsou nejčastěji velké organizace nebo státy, ale i menší podniky by si měly dávat pozor, postihnout to může kohokoliv [10].

Je několik fází, kterými si musí útočníci projít, aby dosáhli svého. První je dostat se do sítě, kde se využívá infikovaných souborů, e-mailů nebo bezpečnostních děr.

Druhá fáze je vytvoření zadních vrátek, tzv backdoor, a tunelů, aby se malware mohl po síti pohybovat a byl těžko zjistitelný. Někdo využívá i přepisování kódu, aby to ztížilo dohledání. V třetí fázi se prolomí administrátorské heslo k získání kontroly nad systémem. Čtvrtá fáze je o pohybu v síti. S dostatečným oprávněním se může pohybovat libovolně v síti, což znamená na různé routery, případně další sítě. V poslední fázi si je útočník vědom bezpečnostních děr a využívá je k získávání informací. Po získání dat, které chtěl může nadále síť monitorovat nebo odejde. Kdyby se náhodou potřeboval vrátit, stále může využít backdoor [10].

2.1.2.6 Odmítnutí služby

Velmi účinný a zákeřný útok, proti kterému se těžko brání [11]. Cílem je narušit funkčnost webové služby tím, že se zahltí server. Nejčastěji používáno pro dočasné vyřazení webových stránek, čímž firma utrpí velké prodělky, ale hlavně ztrátu reputace. Konkurenci to naopak zvýhodní. Rozlišujeme, jestli se útok provádí z jednoho počítače (DoS) nebo z více (DDoS) [12].

Často se využívají chyby v softwaru zařízení, kde díky těmto chybám může útočník zatěžovat síť skrze zařízení přímo v síti nebo odstavit některé zařízení, čímž zpomalí síť nebo v horším případě zařízení nezvládnou nápor dat a systém se zhroutí. Nejjednodušším řešením je poslat ohromné množství požadavků na server. Router nezvládne tolik dat a zkolabuje [12].

Není vůbec jednoduché poznat, zdali je vaše zařízení pod útokem. Může se jednat pouze o jiné problémy s připojením, ale nejčastější projevy jsou pomalý internet (dlouhé načítání webových stránek nebo souborů), neschopnost načtení konkrétních webů nebo ztráta připojení k zařízením na stejné síti [13].

Jsou způsoby, jak se bránit proti DDoS, ale bohužel tato ochrana vyjde dost draze. U DoS je to jednodušší, moderní technologie se dokáží bránit proti většině z těchto útoků [14].

Botnet je nejčastěji využíván u DDoS útoku. Jedná se o skupinu počítačů infikovanou malwarem. Uživatel si nemusí být vědom infikování a bez jeho vědomí jsou páchány útoky z jeho zařízení. Díky tomuto lze vytvořit útok s libovolným počtem zařízení, tedy počty mohou jít do řádu stovek i tisíců. Výhoda je i různost IP adres [13].

Cena DDoS útoku se může pohybovat mezi $5 za 300vteřinový útok až $400 za 24hodinový útok. Záleží na velikosti botnetu a délce útoku [15].
Obrané softwary vyjdou na mnohem vyšší částky oproti útokům. Ceny se pohybují mezi $9,99 až $59 za měsíc. Jsou i dražší obrany a některé si ještě navíc účtují zpracovaná data za měsíc [16].

Denial of service (DoS)

Útok přichází z jednoho připojení, tedy zařízení. Složitost je vyšší a musí být co nejefektivnější, aby server nestihl zablokovat IP adresu, z níž se útok odehrává. Typicky se dělí na další dvě kategorie, kde jedna cílí na přetečení bufferu a druhá na datovou šířku. Využívají se zde nedokonalosti systému, o kterých si útočník může být vědom [13]

- **Buffer overflow útoky**

Způsobují, že zařízení začne používat veškeré dostupné zdroje (paměti, CPU, …) a způsobí tím neobvyklé chování. Následkem dojde ke zpomalování služby, kde ve finále dojde k pádu systému, což vede k nedostupnosti dané služby [13].

- **Flood útoky**

Dělí se na dva druhy: ICMP (internet control message protocol) a SYN. Využívá se zahlcení datové šířky, čímž zaměstnáme server zbytečnými věcmi a přestane se věnovat těm důležitým [14].
ICMP Flood zneužívá protokolu pro zjištění dostupnosti připojení mezi servery. Útočník zahlcuje server tím, že na něj pinguje. Server se snaží na všechny pingy odpovědět. Tímto útočník zahltí příchozí i odchozí šířku pásma serveru a zneschopní ho pro ostatní [12].
SYN Flood využívá způsob navazování spojení pomocí TCP three-way handshake protokolu. Útočník se opakovaně pokouší navázat spojení se serverem, ale nikdy ho nedokončí. Zahlcuje ho, dokud ho neznepřístupní i ostatním uživatelům [11].

Distributed denial of service (DDoS)

Složitost stačí nižší, protože zde je síla v počtu zařízení, z kterých se útočí. Útočníci generují požadavky tak dlouho, dokud nevyčerpají šířku pásma a paměť RAM, čímž odstaví server. Lze využít i složitějších praktik, ale je to zbytečné. Identifikovat zdroj útoku je skoro nemožné [14].

2.1.2.7 Fileless malware

Slouží k infikování počítače skrze známý software. Mnoho všedně používaných programů využívá skripty. Skrze ně se dá jednoduše infiltrovat, jelikož je to jako spuštění neznámé aplikace. Vytvořit ho je velice náročné, ale efektivní [17].

Vyskytuje se v paměti a běžné detekce ho nedokážou nalézt. Dokáže se infikovat do nástrojů, které mu umožní ovládat zařízení. Příkladem může být PowerShell nebo přímo operační systém. Pomocí těchto nástrojů může udělovat oprávnění k administrátorským činnostem nebo se dále přesouvat bez povšimnutí. Poté již stačí ovládnout důvěryhodný program. Nejtypičtějším je antivirový nebo jiný ochranný software, kde je již snadné udělit výjimky, aby se vykonalo něco, co by za normálních okolností bylo zablokováno [18].

Jedinou nynější ochranou jsou znalí analytici, kteří dokážou hrozbu ve skriptu identifikovat, ale problémem je umístění těchto souborů. Nejjednodušší ochranou je zakázaní skriptů a neotvírání cizích souborů, což v případě textových dokumentů může být složité, protože běžný uživatel je nebere jako hrozbu.

2.1.3 Fyzické útoky

Jedná se o odcizení zařízení nebo vniknutí do prostoru, kde se nechá manipulovat se sítí. Síťová zařízení by měla být zabezpečena před vstupem neoprávněných osob. Pokud i tak dojde ke kontaktu se zařízeními, měli by být dostatečně chráněny, aby i při manipulaci s kabely či pokusu o připojení přes volný port, nedošlo k proniknutí do sítě. To stejné platí pro krádež. Pokud pachatel odcizí nějaké zařízení, mělo by být natolik zabezpečené, aby mu bylo k ničemu.

2.2 Neznámé hrozby

Je těžké definovat neznámé hrozby, když jsou dosud neznámé. Zmínka bude i o nesíťových hrozbách, jelikož toho mají se síťovými hrozbami mnoho společného a většinou útočí ruku v ruce.

Spousta bezpečnostních produktů je vytvořeno na základě hrozby. Jakmile je na ni vytvořena obrana, dává to tvůrci důvod vytvořit novou dokonalejší hrozbu [19]. Bohužel se vyvíjí tolik hrozeb, že není možné na ně ihned vytvořit protiopatření [20]. Jediný způsob, jak vytvořit ochranu proti nějaké hrozbě je dostat se s ní do kontaktu. Kdo by však toto nebezpečí dobrovolně podstupoval a jak by donutil všechny útočníky k jednání.

Podle odborníků vychází nových hrozeb v řádu několik stotisíců denně. Samozřejmě na toto enormní číslo je v podstatě nemožné reagovat ihned ochranou. Už jenom z hlediska výkonu není možné implementovat milióny opatření proti každé jednotlivé hrozbě [21].

Dokud se hrozba nedostane na blacklist, je považována jako bezpečná. Jsme tedy proti ní bezbranní. Přesto se doporučuje používat Firewall a Antivir. Firewall může odhalit potencionální hrozby a zabránit jim. Antiviry poskytují možnost sandboxu, což je možnost izolovat aplikace nebo soubory od vašeho počítače a následně je otestovat, zdali jsou pro vás nebezpečné či nikoli. Mnoho lidí si myslí, že si stačí nainstalovat antivir a jsou chráněni. Důležitým faktorem jsou pravidelné aktualizace, a to nejen u antiviru, ale i u aplikací a operačního systému, který používáte. U antiviru se vám doplní nové hrozby a u OS nebo aplikací se opravují bezpečnostní chyby nebo se zvyšuje zabezpečení například přes certifikáty nebo silnější šifrování [20].

Nejlepším způsobem, jak se bránit je spolupracovat. Čím více společností bude spolupracovat, tím rychleji a efektivněji budou hrozby ztrácet na efektivitě [20].

Jsou tři způsoby, jak vytvářet hrozby. Každá má plusy a mínusy, a proto tu všechny představím [20].

Recyklace hrozby

Často využívaná metoda kvůli velké efektivnosti. Spočívá v tom, že se použije již zastaralá hrozba. Někdo by pomyslel, proč by to někdo dělal, když už byla jednou odhalena. To že již byla vytvořena ochrana neznamená, že hrozba nebude fungovat. Využívá se zde limitů paměti bezpečnostních prvků, kde obrana se vyvíjela podle toho, jak byla hrozba vylepšována. Samozřejmě se používá nejaktuálnější informace o hrozbě, a tudíž po čase může být tato hrozba použita s šancí, že ji ochrana nezachytí jako hrozbu, záleží na tom, jak moc se změnila od nejnovější verze [20].

Úprava hrozby

Útočníci musí hrozbu pozměnit. Ochrana ji detekuje na základě některých znaků. Pokud jsou pozměněny, nemusí být označena za hrozbu. V horším případě se vytvoří taková hrozba, která by se dalo nazvat, že mutuje. Nazývá se polymorfní. Jakmile je hrozba identifikovaná jako škodlivá, dokáže se upravit tak, aby byla opět klasifikovaná jako neškodná [20].

Nová hrozba

Nejnáročnější a nejdražší způsob, kde se vytvoří úplně nová hrozba [20].

3 Detekce abnormalit

Velký nárust útočných technik jako je DDoS, APT a hrozby, které obcházejí standardní zabezpečení, změnili způsoby IT zabezpečení. Zabezpečovat primárně koncové body a spoléhat se na ochranu skrze podpisy již nestačí. Tímto jsou zcela bezmocní, proti vnitřním útokům. Řešením je proaktivní detekce, zmírnění síťových anomálií a nežádoucího chování. Probíhá monitorování sítě pomocí umělou inteligencí zvanou NBAD (network behavior anomaly detection). Trvale se sleduje provoz a analyzuje se provoz za účelem odhalení netypického chování. To umožňuje reagovat na doposud neznámé hrozby nezjištěné jinými technologiemi [22]. Dalo by se to přirovnat k odstraňování šumu ze signálu, ačkoli je to jen podobné [23].

Ve firemních podmínkách má mnohé využití. Dá se zjistit narušení sítě, monitorovat stav systému, detekovat podvody v transakcích nebo chyb v operačním systému [23].

Anomálie se dá označit jako neobvyklé chování v síti. Je očekáváno nějaké chování, ale najednou se objeví odlehlé hodnoty, které jsou nazývány anomáliemi. Jsou různé druhy anomálií, o kterých si něco povíme [23].

Bodová anomálie

Jediná instance dat, která je odlehlá od ostatních. Typickým příkladem jsou platby, kde se liší částka od běžných plateb [23].

Kontextová anomálie

Jsou ovlivněny časovým obdobím. Příkladem je firma, která vyrábí sezónní věci. Při sezóně jsou vyšší náklady a celkově provoz ve firmě, než mimo sezónu [23].

Kolektivní anomálie

Soubor instancí dat na základě, kterého se dá vyvodit potencionální hrozba. Typicky nějaký pokus o zkopírování dat [23].

4 Nástroje a techniky

Tato část se bude zabývat softwarem. Budeme procházet nejznámější nástroje a techniky. Některé nástroje jsou pouze pro útok nebo obranu, ale dost těchto programů se dá využít k obojímu.

4.1 Fing

Rychlý a bezplatný nástroj pro správu sítě. Podpora operačních systémů jako jsou Android, IOS, MacOS a Windows. Dokáže detekovat vetřelce a posuzovat rizika zabezpečení. Vypíše všechna připojená zařízení k síti včetně MAC a IP adres. Lze využít základních příkazů jako je ping, trasování, skenování služeb (portů) a probuzení po síti LAN [24].

Osobně ho používám v mobilní verzi, kde je jednoduché si hlídat zařízení připojená k bezdrátové síti. Díky jednoduchosti aplikace a jejímu až profesionálnímu využití jsem si ji vybral jako praktickou část, proto více informací najdete v 8. kapitole.

4.2 Network mapper

Zkráceně Nmap, je multiplatformní open source nástroj pro prozkoumávání sítě. Lze ho spustit na Windows, Linux i MacOS. Je zcela zdarma.
Využívá raw pakety [25], které jsou podobné UDP paketům. Pouze se liší v několika věcech. Raw pakety je možné přiřadit k jakémukoliv protokolovému číslu, nemají protokolovou hlavičku, data obsahují IP hlavičku a jsou zasílána na všechny sokety určitého protokolu a IP adresy [26]. Díky těmto paketům je schopen zjisti všechny zařízení v síti, jaké služby jsou v síti včetně verzí, na jakém OS běží, jaké firewally zde jsou a mnoho dalšího. Nmap je v základu příkazová řádka, ale obsahuje i další užitečné nástroje jako jsou Zenmap, Ncat, Ndiff a Nping [25].

Zenmap

Oficiální uživatelské prostředí pro Nmap. Navržen, aby zjednodušil práci jak pro začátečníky, tak i pro pokročilé. Dají se zde ukládat často používané skeny a výsledky skenování [25].

Ncat

Čte, zapisuje, dešifruje a přesměrovává data v síti. Pro komunikaci využívá TCP i UDP. Není omezen pouze na IPv4 a IPv6, prakticky má neomezené využití. [25].

Ndiff

Pomáhá při porovnání dvou skenů. Vyžaduje dva XML soubory, kde vypíše rozdíly mezi nimi. Využíváno přes Zenmap [25].

Nping

Dokáže vytvářet pakety pro velké množství protokolů, analyzovat odpovědi a čas odezvy. Lze využít k jednoduché detekci zařízení, ale také k zátěžovým testům sítě jako například DoS útokům, trasování a další. Nping umožňuje uživatelům pozorovat, jak se pakety mění při přenosu mezi zdrojovým a cílovým hostitelem [25].

4.3 WireShark

Nejznámější a nejpoužívanější protokolový analyzátor a paketový sniffer na světě. Je zdarma a běží na Linux, MacOS, BSD, Solaris a Windows. Umožňuje velice detailní sledování sítě, které je standardem v mnoha organizacích. Obsahuje bohatou sadu funkcí jako například hlubokou inspekci stovek protokolů (pořád se přidávají nový), podporu dešifrování, výkonné zobrazovací filtry a mnoho dalšího [27].

4.4 Firewall

Blokuje nebo povoluje navazování komunikace na předem stanovených pravidlech. Tato pravidla mohou být napsána na pevno nebo se řídí dynamicky, což znamená, že se připojení dočasně povolí za určitých okolností [28].

Jedná se o filtrování příchozí i odchozí komunikace, aby ochránil zařízení v síti. Firewall může být fyzický nebo softwarový a dá se umístit mezi počítač a server nebo mezi server a internet. Doporučuje se spíše druhá možnost, kde se útok nedostane k routeru. Firewall může zabránit hrozbám zvenčí, tak i zevnitř [28]. Dělí se na 8 kategorií [29].

Paketové filtry

Nejzákladnější a nejstarší typ architektury. Ze switche nebo routeru se stane v podstatě kontrolní bod, který provádí jednoduchou kontrolu procházejících paketů. Kontroluje informace jako jsou IP adresy (zdrojová a cílová), číslo portu, typ paketu a další informace, aniž by otevíral paket, pro kontrolu jeho obsah. Pokud je paket podezřelý, je zahozen [29].

Obvodové brány

Další jednoduchý a rychlý typ firewallu, který ověřuje paket skrze handshake protokolu TCP. Opět nekontrolují obsah paketu, proto nejsou dostatečné pro ochranu sítě [29]. Hodí se spíše do vnitřních sítí.

Stavové firewally

Kombinace dvou předchozích firewallů. Kontrolují pakety i TCP handshake. Dosahují vyšší ochrany za cenu zatěžování zařízení, ale dochází k zpomalení toku

paketů [29]. Furt nedochází ke kontrole obsahu packetů, takže bezpečnost není dostačující.

Aplikační brány (proxy firewally)

Funguje na aplikační vrstvě a filtruje příchozí provoz mezi zdrojem provozu a vaší sítí. Jsou dodávány prostřednictvím cloudu nebo jiného proxy zařízení. Místo přímého připojení se prvně připojí firewall, který naváže spojení s cílovou destinací a zkontroluje příchozí pakety. Kontrola funguje stejně jako u stavového firewallu jen s tím rozdílem, že může provádět kontrolu obsahu paketu. Po dokončení kontroly se firewall připojí na vaši síť, aby vám schválené pakety předal. Tímto dochází k dalšímu zabezpečení, kde dochází k zprostředkování komunikace a tím zůstáváte v anonymitě oproti ostatním [29]. Velkou nevýhodou je pomalý přenos.

NGFW

Next generation firewall neboli firewall nové generace má detailnější přehled o aplikacích a hrozbách, které mohou síť ohrozit [30].

Podle firmy Gartner, což je přední světová společnost zabývající se výzkumem informačních technologií, by měl mít NGFW tyto funkce:

- Standardní funkce firewallu
- Integrovanou prevenci vniknutí
- Povědomí o aplikacích a blokování těch rizikových
- Zdroje o inteligentních hrozbách
- Vylepšovat cesty, aby zahrnovaly budoucí informační zdroje
- Techniky řešení vyvíjejících se hrozeb

Softwarové firewally

Jedná se o nefyzické typy firewallů. Typicky je nainstalován na místním zařízení. Užitečné pro vytvoření izolovaných koncových bodů od sebe. Velkou nevýhodou je obtížná a náročná údržba. Lze narazit i na nekompatibilnost [29]. Nemusí se za ně platit, je možné nalézt aplikace, které jsou zdarma a účinné.

Comodo

Firewall od známého tvůrce bezpečnostního softwaru Comodo. Poskytuje ochranu před útoky, nabízí kontrolu nad připojeními zařízenímu. Prostředí je jednoduché a uživatelsky přívětivé. Jeden z nejlepších firewallů zdarma. Obsahuje rovněž funkci Default Deny Protection (DDP), která pracuje se seznamem známých malware a zamezí jim přístup [31].

Hardwarové firewally

Opakem softwarových firewallů, zde je fyzické zařízení podobné routeru, které slouží jako firewall. Typický příklad firewallu, který chceme mít mezi routerem a internetem, kde v případě hrozby, zachytí útok firewall a neohrozí se koncový bod sítě. Největší slabinou jsou interní útoky, které tento firewall obejdou [29].

Cloudové firewally

Jakmile je u firewallu použito cloudové řešení, lze ho nazvat cloudovým firewallem nebo službou firewall (FaaS). Function as a service je způsob provádění operací bez serveru. To znamená vytváření nebo aktualizování kódů za chodu aplikace bez nutnosti restartování. Cloudové firewally jsou považovány za proxy firewally, kvůli častému využití cloud serveru při nastavení proxy firewallu, ačkoli proxy nemusí být nutně na cloudu. Velkou výhodou je škálovatelnost. Velmi vhodné mezi server a internet stejně jako hardwarové firewally [29].

4.5 VPN

Virtuální privátní síť slouží k šifrovanému připojení zařízení do sítě přes internet. Toto pomáhá zajistit bezpečný přenos citlivých dat. Zabraňuje odposlouchávání informací a umožňuje uživateli pracovat na dálku. Často se používá v podnikových prostředích, kde zaměstnanec se může bezpečně připojit do firemní sítě. Pro bezpečné připojení do firemní sítě se využívá VPN technologie kontrolující, zda zařízení splňuje určité požadavky, než mu povolí se připojit [32]. Zmíníme se o některých VPN protokolech.

Internet Security Protocol (IPSec)

Zabezpečuje IP komunikaci ověřováním relace a šifrováním všech dat během připojení. IPSec má dva režimy: Transport a Tunneling mode. Transport šifruje pouze zprávu v paketu. Tunneling šifruje celý paket [33].

Layer 2 Tunneling Protocol (L2TP)

Obvykle se kombinuje s jiným protokolem VPN, nejčastěji s IPSec. L2TP vytvoří tunel mezi připojovacími body a IPSec se stará o šifrování dat a zabezpečení přenosu [33]

Point-to-Point Tunneling Protocol (PPTP)

Jeden z nejpoužívanějších protokolů VPN. Vytvoří tunel a zapouzdřuje pakety. K šifrování se používá protokol PPP, který je podporován i na MacOS a Linuxu [33].

Secure Socket Layer (SSL) a Transport Layer Security (TLS)

Webový prohlížeč slouží jako klient a přístup uživatelů je omezen na konkrétní aplikace. Nejedná se o přístup do celé sítě, ale pouze k některým jejím prostředkům. Nejčastěji je používán poskytovateli služeb online. SSL spojení mají https místo http [33].

Secure Shell (SSL)

Vytvoří se šifrovaný tunel, přes který probíhá přenos dat. Připojení jsou vytvářena SSH klientem [33].

5 Budoucí vývoj hrozeb a možné ochrany

S vysokým nárůstem IoT (internet of things) se zvyšuje i počet potencionálních zařízení, na které se dá zaútočit. Dnes se již dá zakoupit mnoho zařízení s přístupem k síti jako jsou domácí spotřebiče, dopravní prostředky a jiné. V některých zemích využívají domácnosti i hlasových asistentů jako je Alexa, Siri a jiné. U nás to není moc rozšířené díky jazykové omezenosti, kde je většinou podpora jen pár jazyků. Ovšem podpora jazyků se postupně doplňuje a je možné, že jednou budou tito asistenti nezbytnou součástí domácností. Napomáhají myšlence budoucí autonomie, kde

pomocí rozhovoru s daným asistentem byste si mohli objednávat zboží, dozvídat se novinky, vařit nebo mnoho dalších věcích, o kterých se nám teď může jen zdát. Jak jsem již zmínil, každý očekává, že v budoucnosti bude mnoho zařízení autonomních. Nejedná se jen o chytré domácnosti, ale také například o dopravní prostředky, pracovní nástroje (sekačky, pily, …) a jiné.

Vidina tohoto všeho je krásná, ale zabezpečení těchto věcí bude velice náročné. Výrobce by si nemohl dovolit, aby jeho autonomní výrobek byl ovládnut a zneužit útočníkem. Když bychom se ohlédli na množství těchto zařízení, kde každé z nich by bylo potencionálně ovládnutelné, tak je až nemyslitelné, kolik nezákonných věcí by se mohlo dít.

V dnešní době mají lidé potíže i se známými hrozbami, proto mě udivuje, že někdo vyvíjí komplikované hrozby, aby překvapil organizace. Stačí využít známé hrozby a vždy se najde někdo, kdo se na ně chytí. Samozřejmě pokud se zaměří na konkrétní větší firmu, tak mu to nejspíš nevyjde, ale šance tam pořád je. Chci tím říct, že firma není zabezpečená pouze síťovými techniky, ale také informovaností zaměstnanců, kde neinformovaný zaměstnanec může způsobit obří škody, proto osobně vidím veliký problém v nedostatečném poučení koncových uživatelů. Měla by se zavést minimálně na školách bezpečnostní gramotnost, která by zvýšila povědomí o hrozbách, což by mohlo docílit k snížení úspěšných útoků. Stačilo by naučit úplné základy, jak se chovat na zařízení a na co si dávat pozor. Většina populace využívá mobilů nebo počítačů k přístupu na internet. Pro někoho je to denní samozřejmost, ale málokdo si uvědomuje, kolik nebezpečí mu hrozí.

Dalším velkým problémem je nedbalost uživatelů. Lidé se nechtějí učit nové věci nebo prostě nechtějí platit za věci, co jim přijdou zbytečné. Typickým příkladem je operační systém. Zaměřím se zde na Windows od Microsoftu, kde se dá krásně demonstrovat tato nedbalost. Osobně jsem znal dost lidí, co nadále používala Windows XP, ačkoli se ukončila podpora. Jejich obhajoba byla, že jsou na to zvyklí. To stejné jsem zažil s Windows 7. Již už nevím o nikom, kdo by měl Windows XP, ale tito uživatelé přešli na Windows 7 a jsou na něm doteď. Minimum lidí přešlo na nejnovější Windows 10. Klasické odůvodnění jsou, že si to přece nebudou platit, nebo že Windows 7 je lepší. Nemohu říct, který operační systém je nejlepší, protože každý má nějaké plusy a mínusy. Je to víc o zvyku, když přijde něco nového, tak tomu

holt musíme dát chvíli, abychom se to naučili a odvyknout si na staré. Nyní k tomu, co je špatného na používání operačních systémů bez podpory. Výrobce přestane vydávat aktualizace, které zabezpečují váš systém. Pro někoho, kdo tento systém zná, není problém na vaše zařízení zaútočit. Využije chyby, kterou by jinak vyřešila některá z aktualizací. Neznamená to, že ve Windows 10 nelze využít chyb v zabezpečení, ale u starších systému je to riziko vyšší. U nových systému se po zjištění bezpečnostní chyby udělá aktualizace, která by ji měla opravit. U starých chyba již zůstane na furt a časem se těch chyb může najít několik. Jsem rád, že na toto dbají i vývojáři aplikací a někteří z nich ukončili podporu systému také, což potencionálně může podpořit uživatele v změně OS. Zmínka byla o Microsoft Windows, ale toto platí pro veškerý software.

Poslední, o čem bych se rád zmínil, jsou aplikace. Každý používá několik programů, na které je zvyklý, ale udržovat je aktualizované není jednoduché. Samotnému mi to přijde otravné. Čím víc aplikací v počítači je, tím častěji na vás nějaká aktualizace vyskočí, a tím dříve se vám to znechutí. Bohužel je nutností tyto programy udržovat aktualizované, čímž se opět bráníte před chybami v zabezpečení. Řešení by bylo jednoduché, stačilo by buď mít jednu aplikaci, která by dokázala najednou aktualizovat veškerý software, nebo sama aplikace, aby měla funkci pro automatické aktualizace, nejlépe v pozadí, aby to nerušilo. Zde je i problém ve vývojářích, protože není jistota, že po novém updatu vám software bude fungovat, jak má. Na jednu stranu chcete mít co nejaktuálnější software, který by měl mít co nejméně chyb a být co nejspolehlivější a v případě objevení chyb mít co nejrychlejší aktualizaci na verzi bez chyb, ale na druhou stranu se vám může dobře fungující software aktualizovat na nefungující verzi.

Minimálně tyto zmíněné věci by se musely vyřešit, abychom mohli postoupit o krok dále, kde by nás čekalo zase něco dalšího. Těchto kroků bychom museli udělat několik, abychom se mohli dostat k zabezpečení autonomním zařízení.

5.1 Vývoj hrozeb

Nikdo si netroufá říct, jak se budou hrozby vyvíjet. Jediné Cisco se zmínilo o možnosti využití umělé inteligence. Spíše to vypadá, jako by nikdo nechtěl dávat nápady na vytváření útoků.

Proběhl průzkum, kterého se zúčastnilo 105 síťových expertů. Šokujících 72 % si myslí, že firmy nejsou připravené na budoucí hrozby. Při otázce na bezpečnost firmy odpovědělo 55 % expertů, že firmy přehlíží to, že jejich zaměstnanci nejsou poučeni o počítačové bezpečnosti a 16 % kritizuje zabezpečení dnešních IoT. Další otázka mířila na to, co bude cílem útoků. 34 % uvedlo IoT, 28 % kritická infrastruktura, 6 % pro mobilní, cloudové a sociálně inženýrské útoky a zbylých 30 % uvedlo jiné [34].

5.2 Vývoj ochrany

Žádný systém není bezpečný, proto vznikají hrozby. Kybernetická bezpečnost je neskutečně obtížná, protože nikdo neví, co kdy přijde. Ačkoli jsou tu principy, které vás udrží v bezpečí i v budoucnu. Jedním z nich je zvládnout dnešní základy. Pokud nezvládáte dnes úplné samozřejmosti jako je různorodost a složitost hesel, nezveřejňování svého hesla před ostatními a podobné věci, v budoucnu nebudete mít šanci. Dalším principem je učit se od ostatních. Pokud se stala nějaká firma útokem a je zveřejněno, jak se to stalo, bylo by dobré to zabezpečit i u sebe. Je tu i velký problém s odborníky, kde vzdělání je drahé [38].
Jsou různé názory, jak se bude obrana vyvíjet. Přední IT firmy mají svůj názor, v který doufají, že se vyplní.

5.2.1 Gartner

Společnost Gartner uvádí, že budoucnost zabezpečení je v cloudu. Cloudové aplikace jsou nyní dost oblíbené, ačkoli je to poměrně stará myšlenka. Vyvinuli cloudový koncept SASE, kde očekávají, že ho začne většina organizací využívat [35].

Secure Access Service Edge (SASE)
Nově vznikající koncept z roku 2019. Hledí se na moderní potřeby, jako je okamžité připojení odkudkoli. SASE sjednocuje WAN a síťové bezpečnostní služby jako jsou CASB, FWaaS a Zero Trust do jediného cloudového modelu [36].

CASB

Slouží k zprostředkování bezpečného připojení. Vynucuje bezpečnostní politiky cloudu [41].

FWaaS

Nový způsob, jak udělat firewall jako cloudovou službu. Zjednodušuje se bezpečnost, tím, že je celá organizace připojená k tomuto firewallu s jednotnou bezpečnostní politikou. Eliminují i hardwarové omezení, protože jsou přístupná odkudkoliv [40].

ZeroTrust

Nulová důvěra funguje na principu, že se každý požadavek ověřuje, jako by pocházel z otevřené sítě. Myšlenka je, nikdy nevěř, raději pokaždé prověřuj [39].

Výhod je hned několik:

- Flexibilita – může se implementovat a poskytovat jakákoli služba.
- Úspora nákladů – použití jedné platformy sníží náklady
- Snížení složitosti – minimalizování správy zabezpečení na jedno místo
- Vyšší výkon – připojení přímo ke zdrojům

Gartner očekává do roku 2024, že alespoň 40 % firem bude tento koncept využívat [36].

5.2.2 Cisco

Cisco zase zmiňuje obrovský počet hrozeb, proti kterým se člověk neubrání. Zmiňují možnost umělé inteligence, která by byla nasazena do kybernetické bezpečnosti. Muselo by umět zpracovat a analyzovat milióny dat vysokou rychlostí. Dále by musela kontrolovat data z každého připojeného zařízení. Problém je, že počty zařízení připojitelných k sítí neuvěřitelně rostou. K rozpoznání hrozby musí mít kybernetický team hlubokou znalost IT protokolů ve své síti, včetně chování stálých uživatelů a jiných toků v síti. Jednoduše se dá říct, že hrozba se projeví jako nestandardní tok v síti. Umělá inteligence by v tomto ohledu dost pomohla. Stačilo

by vytvořit vzory typických činností v síti. Následně pustit neustálé sledování sítě, které by hlídalo, aby nevznikali atypické činnosti v síty, které by mohlo blokovat. Umělá inteligence by časem mohla detekovat menší odchylky, kterých by si člověk nevšiml. AI v kombinaci s lidskými experty bude nejsilnějším bezpečnostním mechanismem v IT. Bohužel je tu i horší možnost, že umělou inteligencí budou posilněni hackeři. Pak už to bude souboj, kdo ji dokáže využít lépe [37].

6 Praktická část

Cílem této praktické části je se seznámit se síťovým nástrojem Fing, který slouží pro administrativu sítě. Přinese nám tato aplikace něco nového oproti integrovaným nástrojům v operačních systémech. Software tohoto typu by měl být samozřejmostí pro kohokoliv, kdo se zabývá problematikou správy sítě ať už na amatérské či profesionální úrovni. Rád bych touto praktickou částí ukázal všechny možnosti tohoto programu. Předvedu i nástroje předinstalované v operačních systémech a poučím o bezpečnosti na počítačových sítích v této souvislosti.

6.1.1 Stanovení otázek

Zde si definujeme otázky, na které v průběhu praktické části budeme hledat odpovědi. Odpovědi na otázky se budou řešit uspořádaně dle pořadí a jejich vyhodnocení bude na konci této kapitoly.

Výhody Fingu oproti OS nástrojům

Je opravdu Fing tak skvělý nástroj nebo ho dokážou základní nástroje operačních systémů zastoupit? V čem je tedy výjimečný?

Testování nástrojů

Jak se liší jednotlivé nástroje OS od Fingu? Testování a porovnání jednotlivých programů.

Co potřebuji pro používání Fingu?

Jaké jsou podmínky a požadavky pro využívání.

Vlastní zkušenost

Je toto dokonalý a bezchybný software? Popis využívání a spokojenosti OS nástrojů a Fingu.

6.1.2 Popis používaného prostředí

Testování bude probíhat na dvou zařízeních s různými operačními systémy. Prvním je notebook HP Pavilion s Windows 10 home ve verzi 2004. Druhým je LG G6

s Androidem 9 ve verzi softwaru V30b-EUR-XX a verzí jádra 3.18.120. Obě zařízení mají originál operační systém od výrobce, který jsem nijak neupravoval. Fing bude testován ve verzi 2.1.0.

6.1.3 Průběh

V této části budeme hledat odpovědi na výše zmíněné otázky. Pokusím se, co nejpřesněji testovat veškeré nástroje, a definovat jejich základní využití.

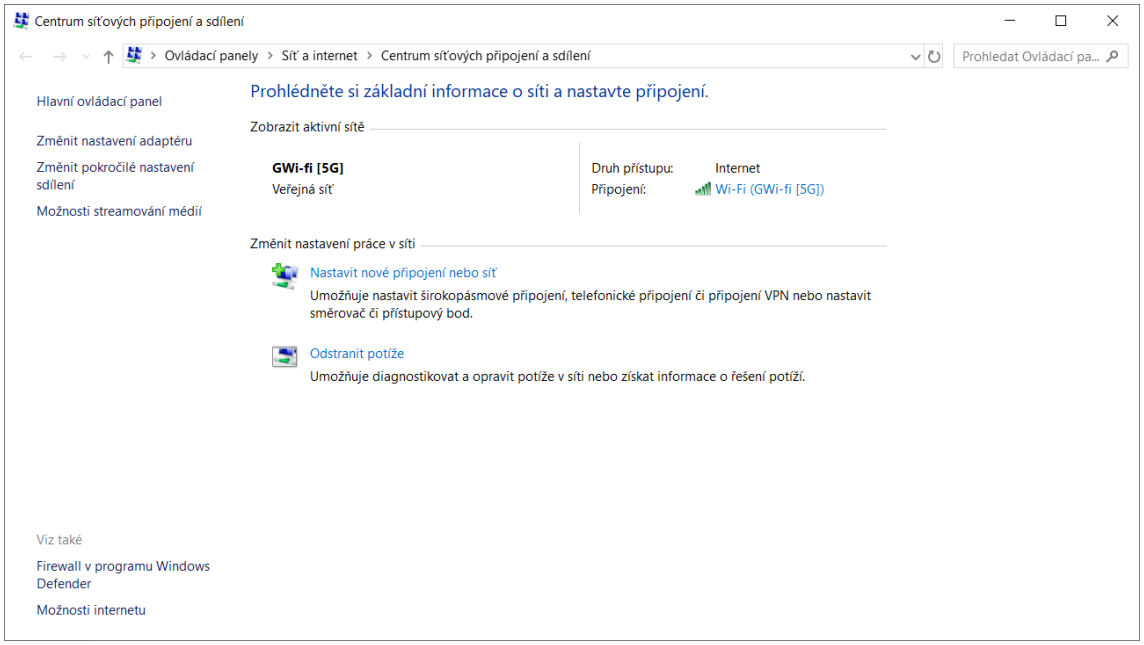
6.1.3.1 Windows

Převážná většina lidí na světě využívá Microsoft Windows, proto bude zajímavé zjistit, jaké informace, nástroje a zabezpečení má v sobě implementované. Zároveň se od toho dá odrazit a udělat první kroky za zlepšením zabezpečení sítí. Budeme procházet zvlášť grafické (GUI) a příkazové (CMD) rozhraní, jelikož grafické by mělo být spíše mířené pro neznalé nebo začátečníky, tedy uživatelsky přívětivější. Naopak příkazové míří na pokročilejší uživatele s jeho složitostí pamatovat si příkazy.

6.1.3.1.1 GUI

Jsou dvě mě známé možnosti, jak graficky najít informace o připojení. První způsob je typický od dřívějších verzí Windows, který najdete zde:

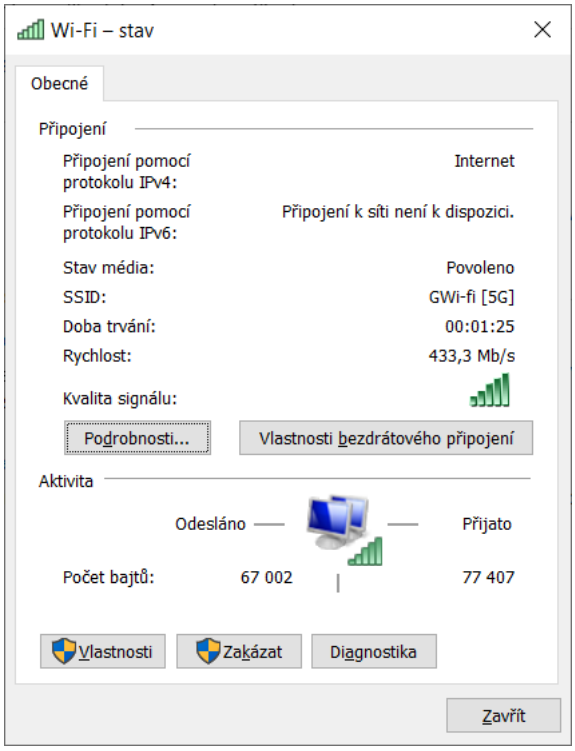
1. Ovládací panely\Síť a internet\Centrum síťových připojení a sdílení
2. Kliknete na modrý nápis, kde bude napsaný název bezdrátové sítě
3. Zde najdete veškeré informace



Obrázek 1: Windows ovládací panely

Na první pohled zde moc informací nezjistíme viz. obrázek 2. K těm nejdůležitějším informacím se musíme postupně proklikat.

Rozkliknutím podrobností se dostanete do okna (obrázek 3), kde uvidíte podrobnosti připojení. Zde můžete zjisti některé užitečné informace o připojeném zařízení jako je síťová karta, IP adresa, maska a jiné. Zde jsou pouze informace o konkrétním připojeném zařízení. Jediné, co lze zjistit, je adresa routeru, která je stejná jako výchozí brána.

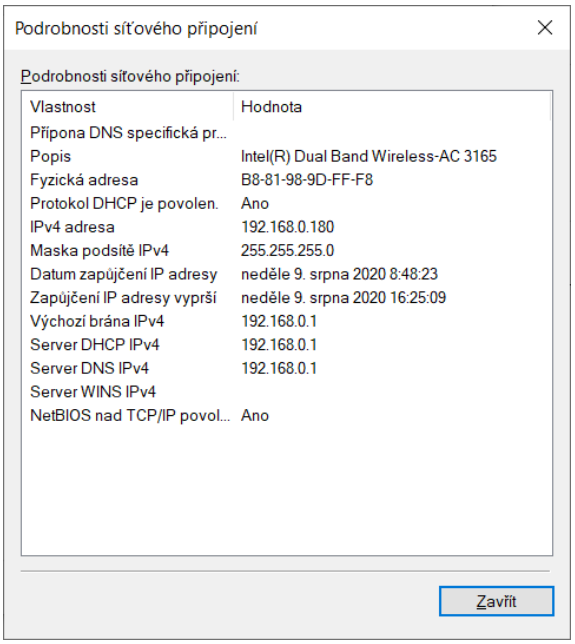


Obrázek 2: Windows stav sítě ovládací panely

Dále jsou zde vlastnosti bezdrátového připojení. Tady je možné nalézt klíč k síti, ale pro jeho zobrazení musíte mít administrátorskou pravomoc. Dávejte si tedy pozor, kdokoliv si může zjistit heslo z přihlášeného počítače.

Vlastnosti slouží pro konfiguraci sítě, touto možností se tu nebudu zabývat podrobně. Jednoduše řečeno si tam lze například ručně nastavit IP adresu, zapnout/vypnout IPV6 a další.

Zakázání slouží k vypnutí síťové karty. Nelze pak najít žádné sítě a chování se podobá, jako kdybyste neměli síťovou kartu. Nejčastěji se používá po změně nastavení, aby se síťová karta restartovala.



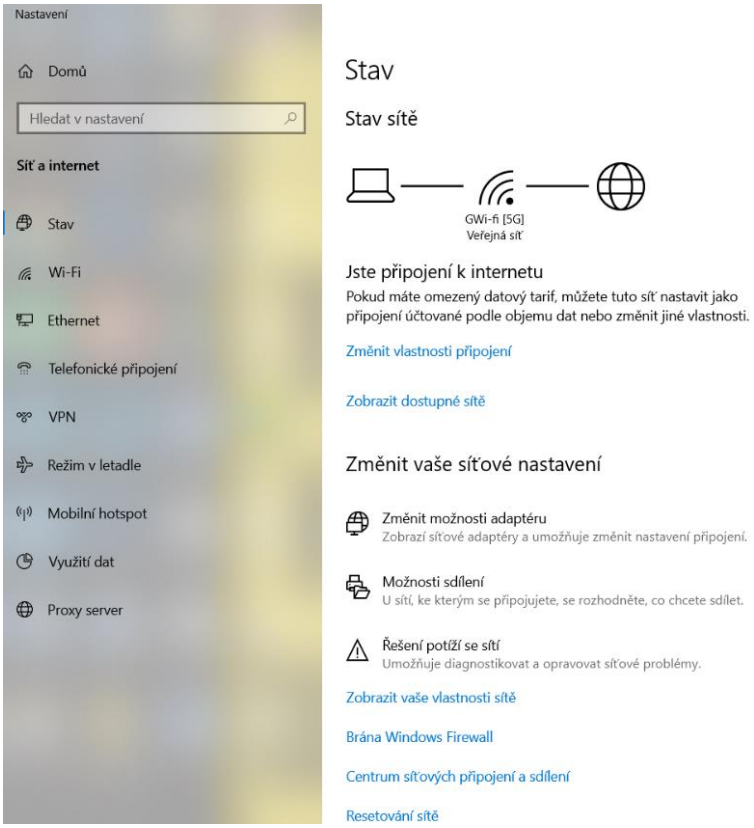
Obrázek 3: Windows podrobnosti sítě

Diagnostika se používá při problémech s připojením. Osobně s ní nemám dobré zkušenosti. Buď problém vyřeší, aniž bych zjistil příčinu, nebo to žádný problém nenajde i přesto, že připojení nefunguje.

Další způsob je nově vytvořený od Windows 8 přes nastavení:

1. Otevřít aplikaci nastavení
2. Kliknout na Síť a internet

Nyní jsme v okně stejného jako na obrázku 4. V levém sloupci se budeme zabývat pouze prvními dvěma body. Opět na první pohled nic důležitého nezjistíme, pouze to, že jsme připojeni k síti a ta je připojena k internetu. Změnit vlastnosti připojení nás dostane do nastavení připojené sítě Na konci najdeme informace viz. obrázek 5.



Obrázek 4: Windows stav sítě nastavení

Vlastnosti

SSID:	GWi-fi [5G]
Protokol:	Wi-Fi 5 (802.11ac)
Typ zabezpečení:	WPA2-osobní
Síťové pásmo:	5 GHz
Síťový kanál:	36
Adresa IPv4:	192.168.0.180
Servery DNS IPv4:	192.168.0.1
Výrobce:	Intel Corporation
Popis:	Intel(R) Dual Band Wireless-AC 3165
Verze ovladače:	19.51.28.1
Fyzická adresa (MAC):	B8-81-98-9D-FF-F8

Obrázek 5: Windows stav sítě vlastnosti

Zobrazením dostupných sítí se nám zobrazí všechny sítě v okolí s možností se na ni připojit.

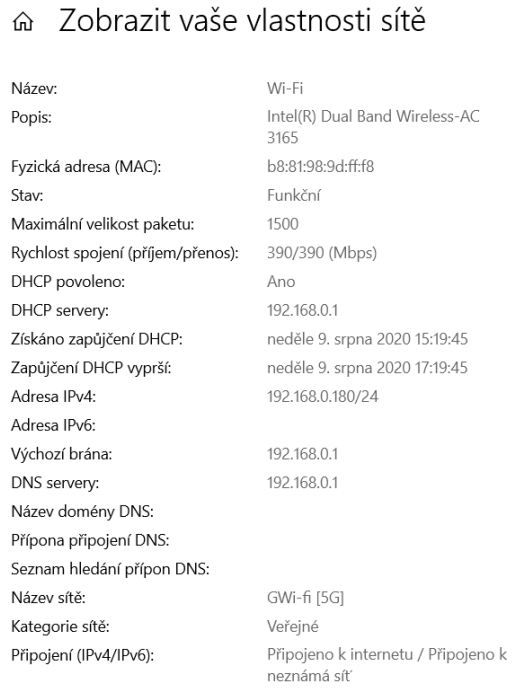
Změnit možnosti adaptéru nás zavede do ovládacích panelů, kde je seznam síťových karet. Zde se dá povolovat/zakazovat konkrétní síťové karty, případně rozkliknutím karty se dostaneme do stavu připojení viz. obrázek 2.

Zde se dá povolovat/zakazovat konkrétní síťové karty, případně rozkliknutím karty se dostaneme do stavu připojení viz. obrázek 2.

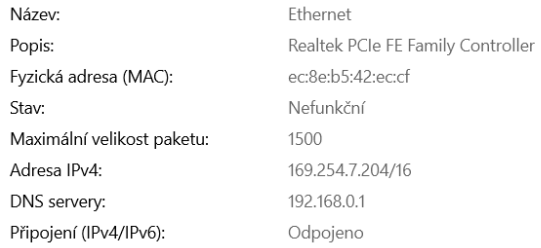
Možnosti sdílení nám umožňují ovládat viditelnost pro tiskárny nebo sdílené soubory a upravovat nastavení, které s tímto souvisí. Je to rozdělené podle tří kategorií: privátní, veřejné a všechny. Pokaždé, když se připojíte k nové síti, se vás Windows zeptá, zdali je připojení soukromé či veřejné. Podle toho se řídí nastavení sdílení, kde je vždy lepší vybrat veřejné, protože je zde toto zjišťování vypnuté nebo omezené. V konkrétních kategoriích si můžete toto nastavení upravovat.

Řešení potíží se sítí je ta stejná diagnostika, jako je v ovládacích panelech.

Zobrazit vaše vlastnosti sítě nás zavede k vypsaným síťovým kartám, kde u každé máme dost informací o stavu viz. obrázek 6 a 7.



Obrázek 6: Windows vlastnosti sítě Wi-Fi



Obrázek 7: Windows vlastnosti sítě Ethernet

Brána Windows firewall nám umožní zkontrolovat stav, či je vypnutá nebo zapnutá, a případně upravovat pravidla nebo jiné její funkce. Celkově vzato je tento firewall pro běžnou činnost dostačující. Dá se mu důvěřovat a svoji funkci vykonává dobře. Ve firmách se využívá pro maximální zabezpečení kombinace firewallů softwarových a hardwarových, kde tato kombinace je cenově nedostupná pro běžné uživatele.

Centrum síťových připojení a sdílení nás opět zavede do ovládacích panelů viz. obrázek 1, konkrétně sem:

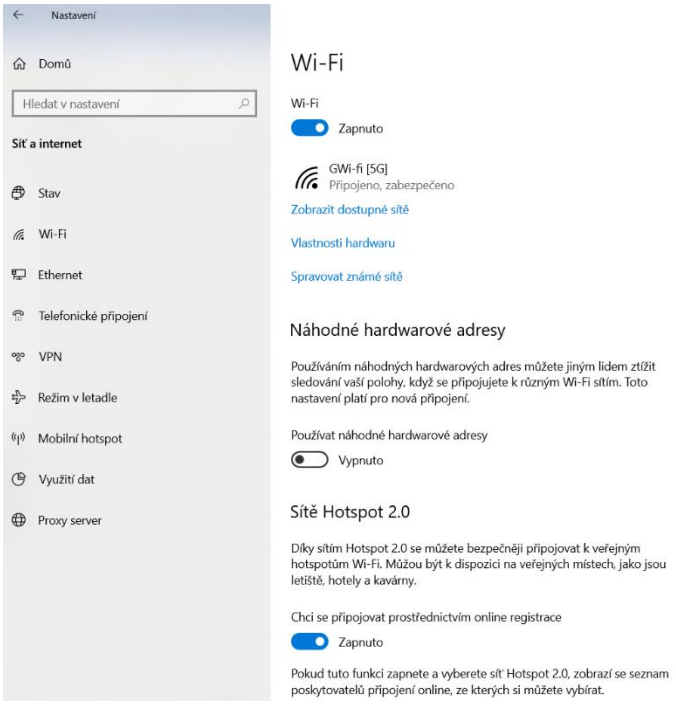
Ovládací panely\Síť a internet\Centrum síťových připojení a sdílení

Resetování sítě slouží k přeinstalování síťových adaptérů, veškerá data o sítích a nastavení se vymažou.

Posuneme se na další bod v levém sloupci. Zde je náhodné nastavení hardwarových adres, které přeskočím, stejně tak Hotspot 2.0. Zde vidíme, ke které síti jsme připojení a je možné bezdrátovou síť vypnout/zapnout.

Kliknutím na název připojené sítě nás dostane do stejného nastavení, jako když jsme v levém sloupci stav, kliknuli na změnit vlastnosti připojení.

Zobrazit dostupné sítě je úplně to stejné, jako dříve zmíněné ve stavu sítě viz. obrázek 4.



Obrázek 8: Windows Wi-Fi nastavení

Vlastnosti hardwaru nám ukážou to stejné, co obrázek 5.

Spravovat známé sítě nám ukáže seznam uložených sítí, na které jsme se někdy v minulosti připojili.

6.1.3.1.2 CMD

Command line neboli příkazový řádek. Umí většinu operací, které dokážeme udělat graficky, pouze musíte znát příkazy, tedy je to složitější. Novější verzí je PowerShell, který bych přirovnal k linuxovému terminálu. Dají se v něm použít všechny příkazy, které cmd obsahuje, ale naopak to nefunguje. Navíc poskytuje možnosti skriptů a prohlubuje možnosti, které příkazový řádek nezvládal. PowerShellem se tu zabývat nebudu kvůli jednomu prostému důvodu, kterým je jeho složitost.

Prvním krokem je spuštění příkazového řádku jako správce. Tím se ujistíme, že nám budou všechny příkazy fungovat a neodmítnou nás, že nemáme dostatečné oprávnění. V případě nejasností má cmd nápovědu, kde stačí zadat příkaz a za něj napsat /? a vypíše se vám, co příkaz dělá a jaké možnosti jsou pro jeho napsání.

Ping slouží k ověření dostupnosti zařízení. Vyšleme paket, který když dojde na danou adresu, tak se vrátí odpověď, která dá vědět o dostupnosti. Syntaxe je jednoduchá, napíše se ping a adresa. Vyšlou se 4 pakety, po kterých se ping ukončí a vyhodnotí se odeslané/vrácené pakety a jak dlouho to trvalo (obrázek 9). Když za tento příkaz připíšeme -t, docílíme nekonečného pingování, které ukončíme pomocí ctrl+c (obrázek 10).

```
C:\WINDOWS\system32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=44ms TTL=114
Reply from 8.8.8.8: bytes=32 time=57ms TTL=114
Reply from 8.8.8.8: bytes=32 time=27ms TTL=114
Reply from 8.8.8.8: bytes=32 time=33ms TTL=114

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 27ms, Maximum = 57ms, Average = 40ms
```

Obrázek 9: Windows cmd ping

```
C:\WINDOWS\system32>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=82ms TTL=114
Reply from 8.8.8.8: bytes=32 time=26ms TTL=114
Reply from 8.8.8.8: bytes=32 time=61ms TTL=114
Reply from 8.8.8.8: bytes=32 time=30ms TTL=114
Reply from 8.8.8.8: bytes=32 time=54ms TTL=114
Reply from 8.8.8.8: bytes=32 time=44ms TTL=114

Ping statistics for 8.8.8.8:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 82ms, Average = 49ms
Control-C
^C
```

Obrázek 10: Windows cmd ping -t

Tracert slouží k zjištění všech zařízení, přes které se dostaneme k cílové adrese. Zjednodušeně řečeno se pinguje na všechny body, přes které procházíte k určité adrese. Stačí napsat tracert a adresu. Můžete vidět na obrázku 11 krok 1 je router v síti a z něho to pokračuje přes poskytovatele až na google DNS.

```
C:\WINDOWS\system32>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1     2 ms    <1 ms    <1 ms  ArcherC6v2 [192.168.0.1]
  2     3 ms     2 ms     2 ms  192.168.254.251
  3    76 ms    74 ms    93 ms  10.64.52.1
  4    87 ms    78 ms    96 ms  10.11.160.177
  5    84 ms    80 ms    81 ms  rcpha2-rlhb0.unet.cz [86.61.255.153]
  6    78 ms   110 ms    50 ms  rlpha1-rcpha1.unet.cz [86.61.255.34]
  7    73 ms    90 ms    71 ms  static-774870005.poda.cz [46.47.147.245]
  8   107 ms    77 ms   109 ms  static-3248824331.poda.cz [193.165.32.11]
  9    91 ms    87 ms    76 ms  static-3248824321.poda.cz [193.165.32.1]
 10   107 ms    68 ms    96 ms  google.peering.cz [91.213.211.170]
 11    93 ms    60 ms    95 ms  108.170.245.49
 12    90 ms    68 ms    84 ms  108.170.238.233
 13   131 ms    20 ms    35 ms  dns.google [8.8.8.8]

Trace complete.
```

Obrázek 11: Windows tracert

Nslookup slouží k dotázaní na DNS server. Vypíše IP adresu a doménové jméno.

```
C:\WINDOWS\system32>nslookup
Default Server:  ArcherC6v2
Address:  192.168.0.1
```

Obrázek 12: Windows nslookup

Ipconfig příkaz nám vypíše všechny síťové adaptéry. Při dopsání -all nám vypíše podrobné informace. Jsou to stejné informace, které lze najít v grafickém prostředí.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 3165
   Physical Address. . . . . . . . . : B8-81-98-9D-FF-F8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.0.180(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : neděle 9. srpna 2020 8:48:23
   Lease Expires . . . . . . . . . . : neděle 9. srpna 2020 22:46:53
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Obrázek 13: Windows cmd ipconfig

Netstat zobrazí, které programy komunikují se službami. Pomocí -a -b -f docílíme detailnějšího výpisu viz. obrázek 15.

```
C:\WINDOWS\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.0.180:50278    10:https               ESTABLISHED
  TCP    192.168.0.180:50310    52.114.159.22:https    TIME_WAIT
  TCP    192.168.0.180:50311    a-0001:https           TIME_WAIT
  TCP    192.168.0.180:50313    204.79.197.222:https   TIME_WAIT
  TCP    192.168.0.180:50319    a-0001:https           ESTABLISHED
  TCP    192.168.0.180:50321    13.107.246.10:https    ESTABLISHED
  TCP    192.168.0.180:50322    13.107.6.254:https     ESTABLISHED
  TCP    192.168.0.180:50323    a95-100-196-73:https   CLOSE_WAIT
  TCP    192.168.0.180:50324    204.79.197.222:https   ESTABLISHED
  TCP    192.168.0.180:56223    51.105.249.223:https   ESTABLISHED
  TCP    192.168.0.180:56230    wa-in-f188:https       ESTABLISHED
  TCP    192.168.0.180:62168    a2-19-195-67:https     CLOSE_WAIT
  TCP    192.168.0.180:62169    a2-19-195-67:https     CLOSE_WAIT
  TCP    192.168.0.180:62170    a2-19-195-67:https     CLOSE_WAIT
  TCP    192.168.0.180:62173    a92-122-48-48:https    CLOSE_WAIT
  TCP    192.168.0.180:62174    a92-122-48-48:https    CLOSE_WAIT
  TCP    192.168.0.180:62175    a92-122-48-48:https    CLOSE_WAIT
  TCP    192.168.0.180:62176    a92-122-48-48:https    CLOSE_WAIT
  TCP    192.168.0.180:62177    a92-122-48-48:https    CLOSE_WAIT
  TCP    192.168.0.180:62178    a92-122-48-48:https    CLOSE_WAIT
  TCP    192.168.0.180:62179    a95-100-198-11:https   CLOSE_WAIT
  TCP    192.168.0.180:62180    a95-100-198-11:https   CLOSE_WAIT
  TCP    192.168.0.180:62181    a95-100-197-169:https  CLOSE_WAIT
  TCP    192.168.0.180:62182    a95-100-197-169:https  CLOSE_WAIT
```

Obrázek 14: Windows netstat

```
C:\WINDOWS\system32>netstat -a -b -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-603H08Q:0      LISTENING
  RpcEptMapper
 [svchost.exe]
  TCP    0.0.0.0:445            DESKTOP-603H08Q:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:2008           DESKTOP-603H08Q:0      LISTENING
 [ABService.exe]
  TCP    0.0.0.0:5040           DESKTOP-603H08Q:0      LISTENING
  CDPSvc
 [svchost.exe]
  TCP    0.0.0.0:6045           DESKTOP-603H08Q:0      LISTENING
 [ABService.exe]
  TCP    0.0.0.0:7680           DESKTOP-603H08Q:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49664          DESKTOP-603H08Q:0      LISTENING
 [lsass.exe]
  TCP    0.0.0.0:49665          DESKTOP-603H08Q:0      LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49666          DESKTOP-603H08Q:0      LISTENING
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49667          DESKTOP-603H08Q:0      LISTENING
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49668          DESKTOP-603H08Q:0      LISTENING
  SessionEnv
 [svchost.exe]
  TCP    0.0.0.0:49669          DESKTOP-603H08Q:0      LISTENING
 [spoolsv.exe]
  TCP    0.0.0.0:49682          DESKTOP-603H08Q:0      LISTENING
 [fingagent.exe]
  TCP    0.0.0.0:49719          DESKTOP-603H08Q:0      LISTENING
 Can not obtain ownership information
  TCP    127.0.0.1:3213         DESKTOP-603H08Q:0      LISTENING
 [OriginWebHelperService.exe]
  TCP    127.0.0.1:48080        DESKTOP-603H08Q:0      LISTENING
 [fingagent.exe]
  TCP    127.0.0.1:49733        DESKTOP-603H08Q:0      LISTENING
```

Obrázek 15: Windows netstat -a -b -f

Pathping je nástroj pro monitorování ztráty paketů. Napíšeme pathping a adresu. Vykoná se nám tracert, kde to po dobu 325 vteřin měří ztrátu paketů.

```
           Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           DESKTOP-603H08Q [192.168.0.180]
                                    0/ 100 =  0%   |
  1    1ms     0/ 100 =  0%     0/ 100 =  0%  ArcherC6v2 [192.168.0.1]
                                    0/ 100 =  0%   |
  2    3ms     0/ 100 =  0%     0/ 100 =  0%  192.168.254.251
                                    0/ 100 =  0%   |
  3   87ms     0/ 100 =  0%     0/ 100 =  0%  10.64.52.1
                                    0/ 100 =  0%   |
  4   ---    100/ 100 =100%   100/ 100 =100%  10.11.160.177
                                    0/ 100 =  0%   |
  5   94ms     1/ 100 =  1%     1/ 100 =  1%  rcpha2-rlhb0.unet.cz [86.61.255.153]
                                    0/ 100 =  0%   |
  6   77ms     0/ 100 =  0%     0/ 100 =  0%  rlpha1-rcpha1.unet.cz [86.61.255.34]
                                    0/ 100 =  0%   |
  7   61ms     0/ 100 =  0%     0/ 100 =  0%  static-774870005.poda.cz [46.47.147.245]
                                    0/ 100 =  0%   |
  8   81ms     0/ 100 =  0%     0/ 100 =  0%  static-3248824331.poda.cz [193.165.32.11]
                                    0/ 100 =  0%   |
  9   73ms     1/ 100 =  1%     1/ 100 =  1%  static-3248824321.poda.cz [193.165.32.1]
                                    0/ 100 =  0%   |
 10   66ms     0/ 100 =  0%     0/ 100 =  0%  google.peering.cz [91.213.211.170]
                                    0/ 100 =  0%   |
 11   66ms     0/ 100 =  0%     0/ 100 =  0%  108.170.245.49
                                    0/ 100 =  0%   |
 12   ---    100/ 100 =100%   100/ 100 =100%  108.170.238.233
                                    0/ 100 =  0%   |
 13   83ms     0/ 100 =  0%     0/ 100 =  0%  dns.google [8.8.8.8]
```

Obrázek 16: Windows Pathping

Route print nám vypíše síťové adaptéry s MAC adresama a následně routovací tabulku.

```
C:\Users\grubmi>route print
===========================================================================
Interface List
 23...ec 8e b5 42 ec cf ......Realtek PCIe FE Family Controller
 19...00 ff d5 a2 a7 13 ......TAP-ProtonVPN Windows Adapter V9
 18...b8 81 98 9d ff f9 ......Microsoft Wi-Fi Direct Virtual Adapter #3
 14...ba 81 98 9d ff f8 ......Microsoft Wi-Fi Direct Virtual Adapter #4
 21...00 ff ea 55 34 33 ......TAP-Windows Adapter V9
 20...b8 81 98 9d ff f8 ......Intel(R) Dual Band Wireless-AC 3165
  1...........................Software Loopback Interface 1
 22...7a 79 19 42 7c 0a ......LogMeIn Hamachi Virtual Ethernet Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0         25.0.0.1              16    9256
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.0.180      35
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     331
      192.168.0.0    255.255.255.0         On-link     192.168.0.180     291
    192.168.0.180  255.255.255.255         On-link     192.168.0.180     291
    192.168.0.255  255.255.255.255         On-link     192.168.0.180     291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     331
        224.0.0.0        240.0.0.0         On-link              16    9256
        224.0.0.0        240.0.0.0         On-link     192.168.0.180     291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     331
  255.255.255.255  255.255.255.255         On-link              16    9256
  255.255.255.255  255.255.255.255         On-link     192.168.0.180     291
===========================================================================
```

Obrázek 17: Windows route print

Arp -all vypíše tabulku, kde jsou IP adresy namapovány na MAC adresy.

```
C:\Users\grubmi>arp -a

Interface: 192.168.0.180 --- 0x14
  Internet Address      Physical Address      Type
  192.168.0.1           cc-32-e5-df-ea-3e     dynamic
  192.168.0.107         02-e0-20-09-88-83     dynamic
  192.168.0.111         02-e0-20-09-88-83     dynamic
  192.168.0.129         68-57-2d-33-bb-a1     dynamic
  192.168.0.144         2c-2b-f9-b1-93-ac     dynamic
  192.168.0.165         0c-9a-42-bc-f0-cd     dynamic
  192.168.0.174         b4-f7-a1-ea-23-e6     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Obrázek 18: Windows arp -all

Mezi posledními tu zmíním příkaz pro zobrazení hesel u uložených sítí. Dříve to šlo zobrazit graficky, ale od Windows 8 to lze složitěji akorát přes příkazový řádek. Pomocí příkazu netsh wlan show profiles si zobrazíme všechny uložené sítě. Následně netsh wlan show profile name="jméno" key=clear. Na obrázku 18 vidíme různé informace o síti včetně hesla, které zde je 123321deh.

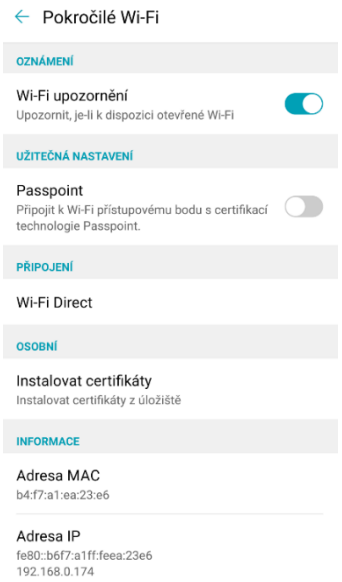
```
C:\WINDOWS\system32>netsh wlan show profile name="protected" key=clear

Profile protected on interface Wi-Fi:
=======================================================================

Applied: All User Profile

Profile information
-------------------
    Version                : 1
    Type                   : Wireless LAN
    Name                   : protected
    Control options        :
        Connection mode    : Connect manually
        Network broadcast  : Connect only if this network is broadcasting
        AutoSwitch         : Do not switch to other networks
        MAC Randomization  : Disabled

Connectivity settings
---------------------
    Number of SSIDs        : 1
    SSID name              : "protected"
    Network type           : Infrastructure
    Radio type             : [ Any Radio Type ]
    Vendor extension          : Not present

Security settings
-----------------
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Authentication         : WPA2-Personal
    Cipher                 : GCMP
    Security key           : Present
    Key Content            : 123321deh

Cost settings
-------------
    Cost                   : Fixed
    Congested              : No
    Approaching Data Limit : No
    Over Data Limit        : No
    Roaming                : No
    Cost Source            : User
```

Obrázek 19: Windows netsh

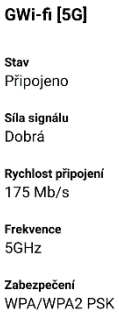
Příkazů zde je velmi mnoho a nemluvě o možnostech napsání jednoho příkazu s několika atributy. Proto jsem tu zmínil pouze příkazy, které mi přijdou důležité a neřeším dopodrobna všechny jejich možnosti.

6.1.3.2 Android

Android jako open-source software má mnoho výhod i nevýhod. Základ mají všechny zařízení stejný, pouze se mění nebo přidávají některé funkcionality podle výrobce. Proto je dobré si zjistit tyto výhody před výběrem přístroje. Některé zařízení mohou mít minimum funkcí povolených a některá zase jsou doplněna o nová vylepšení. V základu toho neumí moc. V nastavení se můžete připojit k síti, zobrazit si IP a MAC adresu nebo si zobrazit pár informací o připojené síti viz. obrázek 21. Případně je možné resetovat celé nastavení, čímž si smažete historii uložených sítí.



Obrázek 20: Android pokročilé Wi-Fi



Obrázek 21: Android informace o síti

Někteří výrobci mají tyto rozšířená nastavení schovaná a není lehký se k nim dostat. Viděl jsem servisní nástroje, ke kterým se dalo dostat pouze při zapínání telefonu nebo dokonce po vytočení určitého kódu, ale co se tam dalo najít, byl maximálně ping. Proto je tu obchod, kde se dá stáhnout cokoliv, co androidu chybí. Je jednodušší si nainstalovat aplikace, které vám chybí než složitě hledat, jestli je výrobce implementoval, případně kam je ukryl. Navíc si můžete vybrat konkrétní, která vám bude vyhovovat, jelikož je mnoho vývojářů, a tak není o podobné aplikace nouze.

6.1.3.3 Fing

Bezplatný nástroj pro správu sítě. Multiplatformní, takže ho lze využívat na nejpoužívanějších operačních systémem jakou jsou Windows, MacOS, IOS nebo Android. Nemusíme tedy využívat na každém OS jiný nástroj, stačí se nám naučit tento. Fing pracuje s databází, díky které dokáže rozpoznávat spoustu zařízení na základě MAC adres. Aplikace je zdarma, ale pro plné využití se dá platit 6,99€ měsíčně. Vyzkouším verzi zdarma, která bude pro naše účely dostačující. Bohužel byla nedávno aktualizace mobilní verze, která je uživateli hodnocena negativně. Přibyly reklamy a změnil se vzhled aplikace. Osobně se přikláním na stranu uživatelů, kde reklamy jsou rušivé a některé funkce, které dříve fungovaly, již pro mě nefungují. Samozřejmě je obtížné optimalizovat aplikaci pro všechna zařízení, ale zrovna při skenování zařízení mi často přestává aplikace pracovat.

Fing je možné využívat i bez registrace, ale přijdete o některé užitečné funkcionality jako jsou upozornění na e-mail, historie sítí včetně všech zařízení (obrázek 40) a další.

Na oficiálních stránkách je možnost zakoupení Fingboxu, což je síťový prvek, který vám zjednoduší správu sítě. Po připojení do sítě si můžete vytvořit profily jednotlivých uživatelů, kterým přidělíte zařízení. Sleduje všechna nová zařízení v síti, která dokáže ihned zablokovat, případně vás dokáže upozornit e-mailem. Většinu těchto funkcí dokáže sama aplikace, Fingbox pouze tyto věci usnadňuje a automatizuje. Jeho cena je £99.

Fing nabízí i možnost implementace do příkazové řádky nebo terminálu skrze Fing CLI. Tohoto lze využít dokonce i u Linuxu. Získáte přesně tyto funkce: informace o síti, sken sítě, sken servisů, ping, tracerout a probuzení po LANu. Tudíž ty stejné nástroje, které poskytuje mobilní verze.

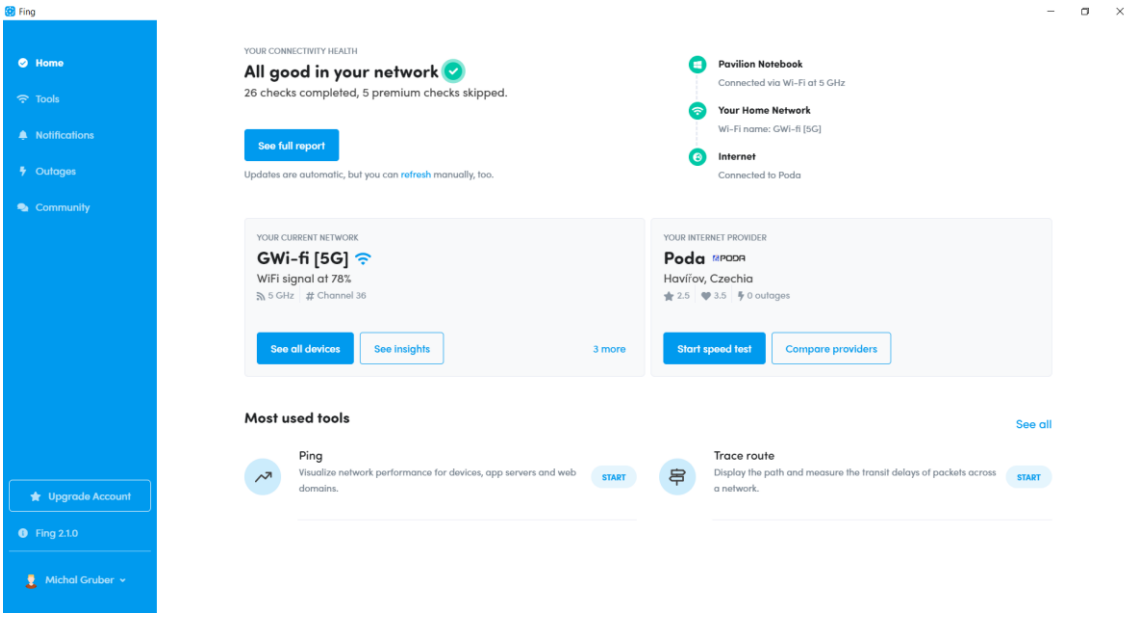
6.1.3.3.1 GUI

V této části prozkoumáme grafické prostředí Fingu viz. obrázek 22. Hned na první obrazovce máme celkem přehledné a užitečné informace. Vlevo nahoře se hned dozvíme, zdali je naše síť zabezpečená a v pořádku. Po rozkliknutí see full report se dozvíme veškeré technické informace, jako že je na PC synchronizovaný čas, DNS server je nastaven, síla signálu dobrá a mnoho dalšího (obrázek 23).

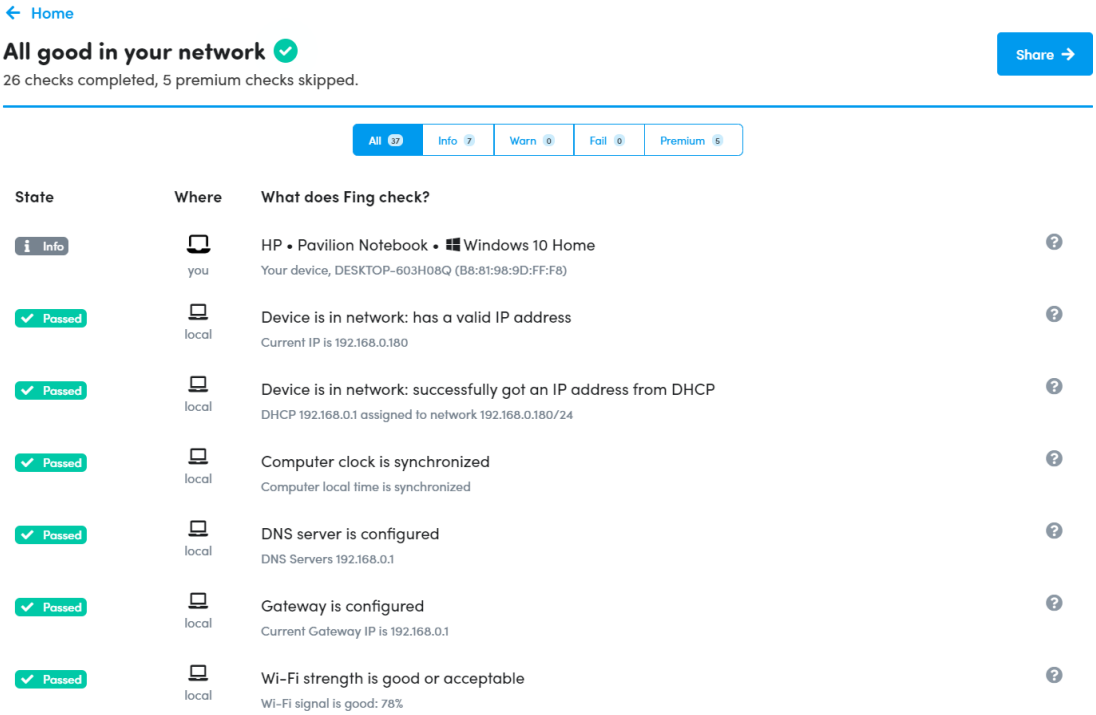
Dále vpravo nahoře vidíme (obrázek 22), že naše zařízení je připojené k routeru a ten je připojen k internetu.

Níže spatříme poskytovatele internetu včetně jeho hodnocení. Lze zde využít test rychlosti (obrázek 24) nebo si otevřít podrobnosti o poskytovateli (obrázek 26).

Vlevo máme to nejzajímavější a tím je naše síť. See insights slouží ke grafickému zobrazení statistik sítě. Například zde vidíme počet zařízení podle výrobce nebo operačního systému. See all devices nám ukáže veškerá zařízení na síti (obrázek 27).

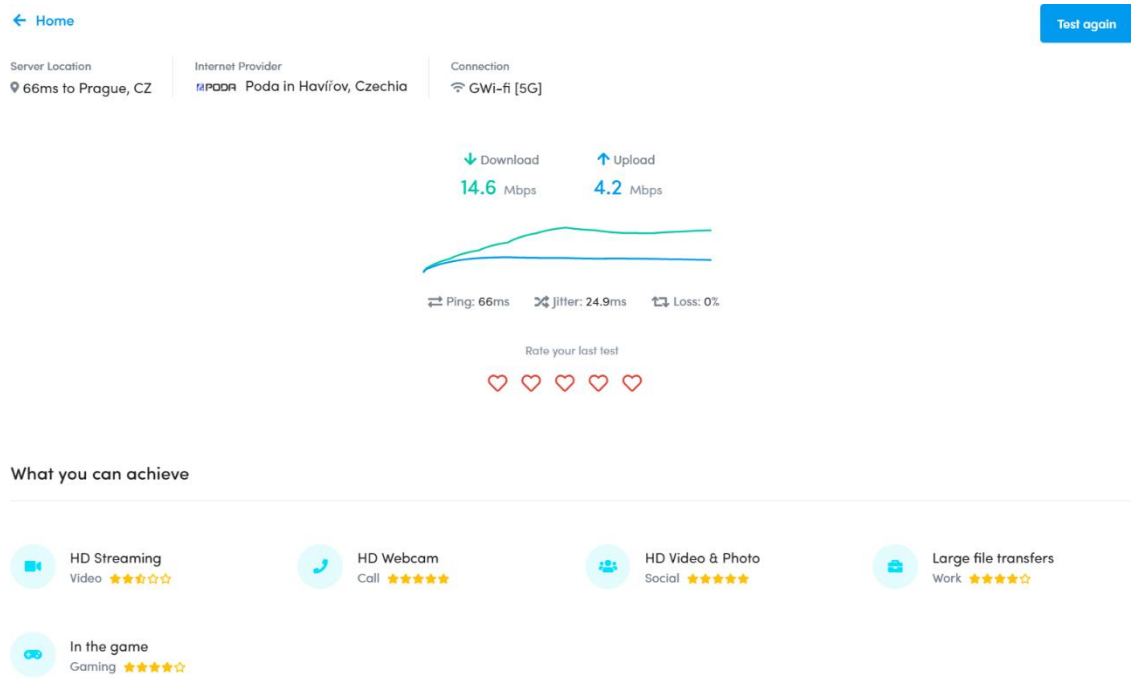


Obrázek 22: Fing úvodní obrazovka

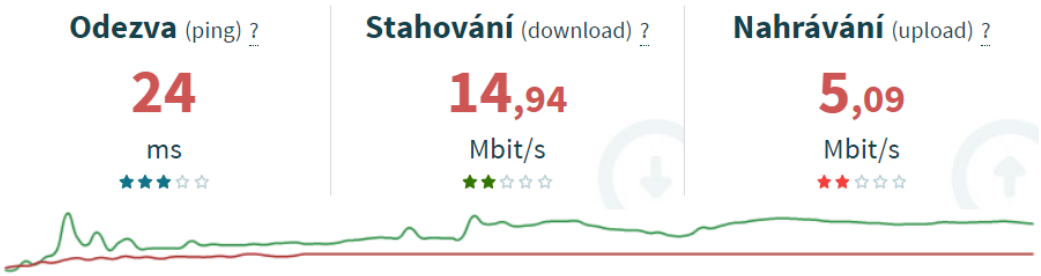


Obrázek 23: Fing technické informace v síti

Test rychlosti Fingu (obrázek 23) v porovnání s testem na webu rychlost.cz (obrázek 24). Tento test nejde nikdy zopakovat na stejné hodnoty. Pouze zde chci ukázat podobnost hodnot, kde se nijak výrazně od sebe neliší. Navíc Fing má i graficky zpracované hodnocení, na co je váš internet vhodný.

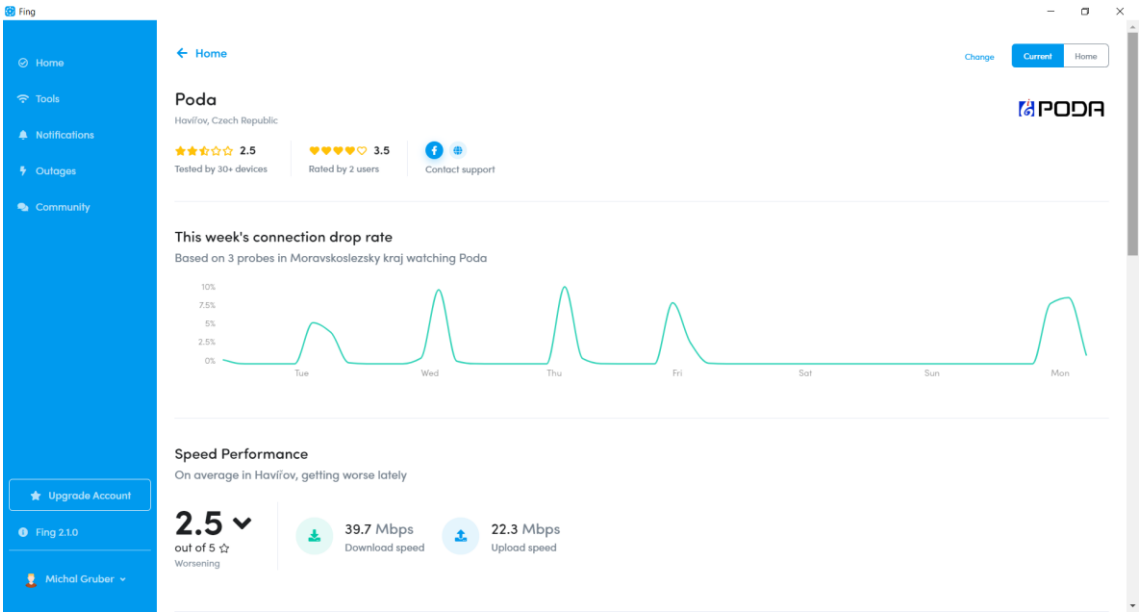


Obrázek 24: Fing speed test



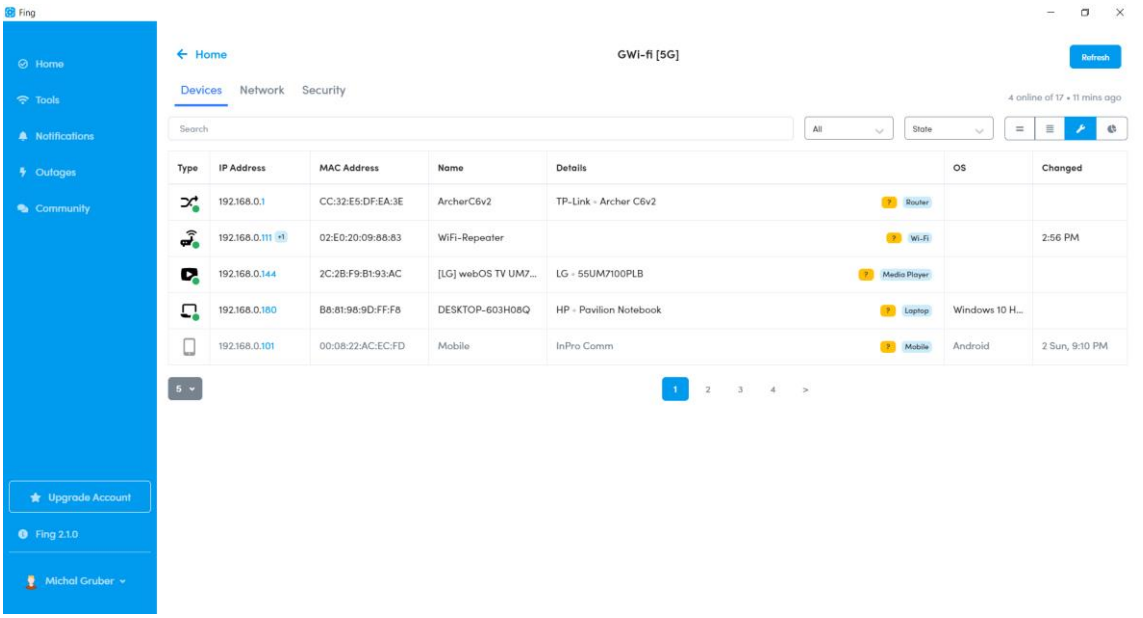
Obrázek 25: Rychlost.cz speed test

Zde lze vidět, jak lidé hodnotí vašeho poskytovatele. Je zde dokonce i kontakt na něho, jakých rychlostí dosahuje a graficky znázorněné klesání rychlost v určité dny.



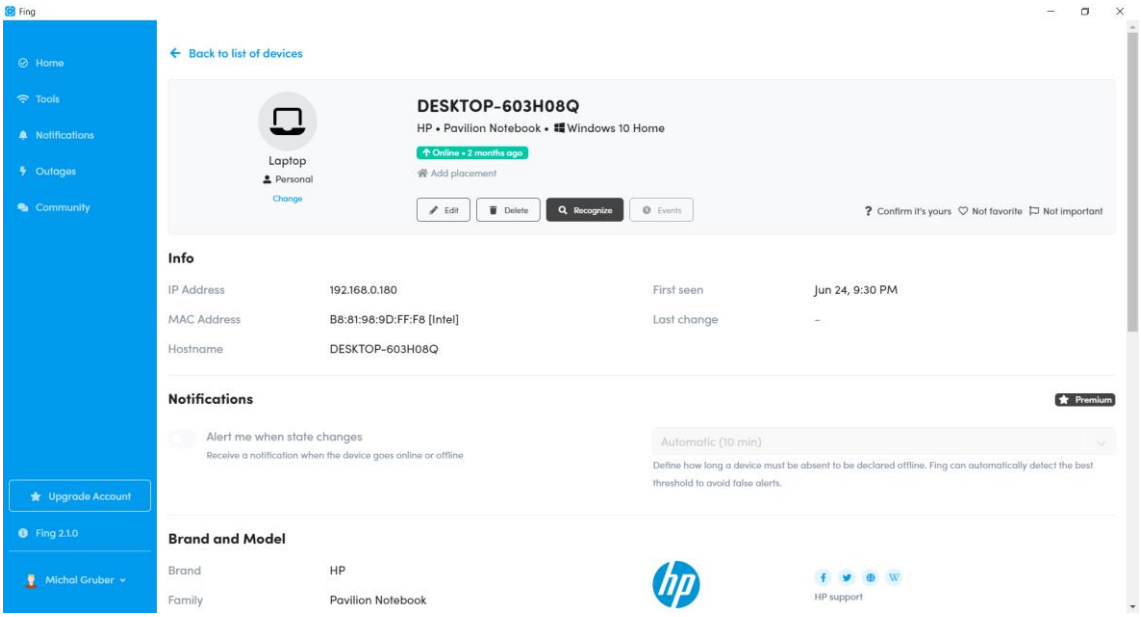
Obrázek 26: Fing poskytovatel internetu

Nejlepší funkce tohoto programu je výpis všech zařízení v síti. Díky rozsáhlé databázi dokáže pomocí MAC adres identifikovat i výrobce. Dokáže identifikovat i operační systém.



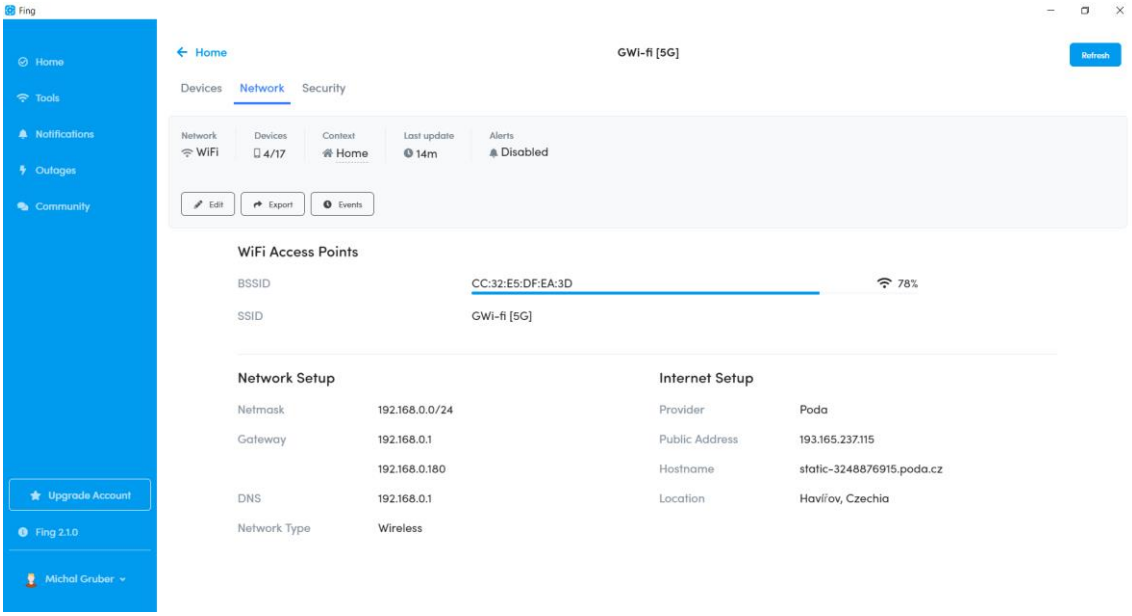
Obrázek 27: Fing see all devices

Po rozkliknutí kteréhokoliv zařízení se nám ukážou veškeré jeho informace. Zde je možnost si zařízení pojmenovat, odstranit, označit jako známé nebo v případě špatné identifikace změnit typ zařízení. Jsou tu i informace typu prvního připojení k síti nebo užitečných odkazů na výrobce daného zařízení. V dolní části jsou nástroje, které se dá ihned aplikovat na vybrané zařízení. Všechny nástroje budou probrány dále, ale výhoda tu je, že nemusíme opisovat adresu pro vykonání například pingu.

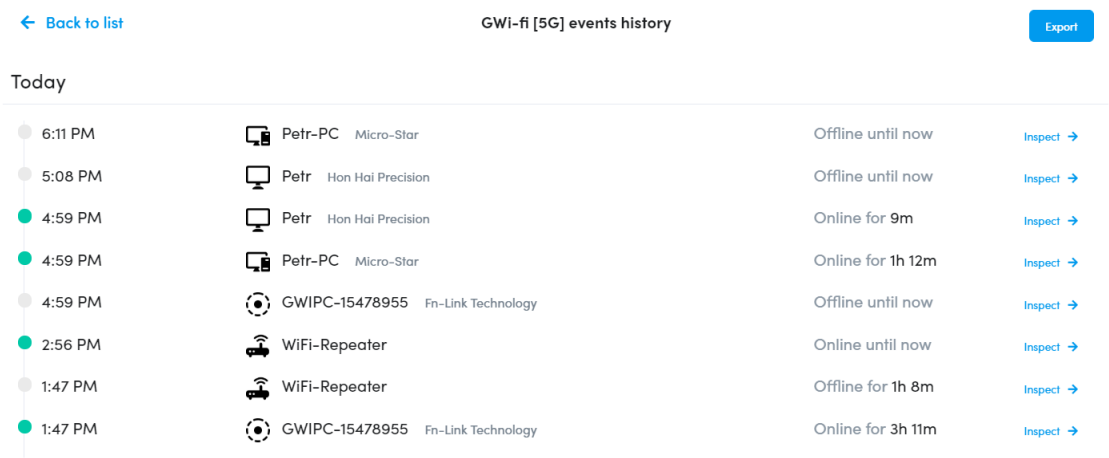


Obrázek 28: Fing detaily zařízení

Z devices se přepnutím na network dostaneme k informacím o síti. Zde jsou veškeré potřebné informace, které potřebujete vědět o vaší síti. Zajímavá je historie provozu sítě, kdy po kliknutí na events dostanete výpis aktivity zařízení (obrázek 30).

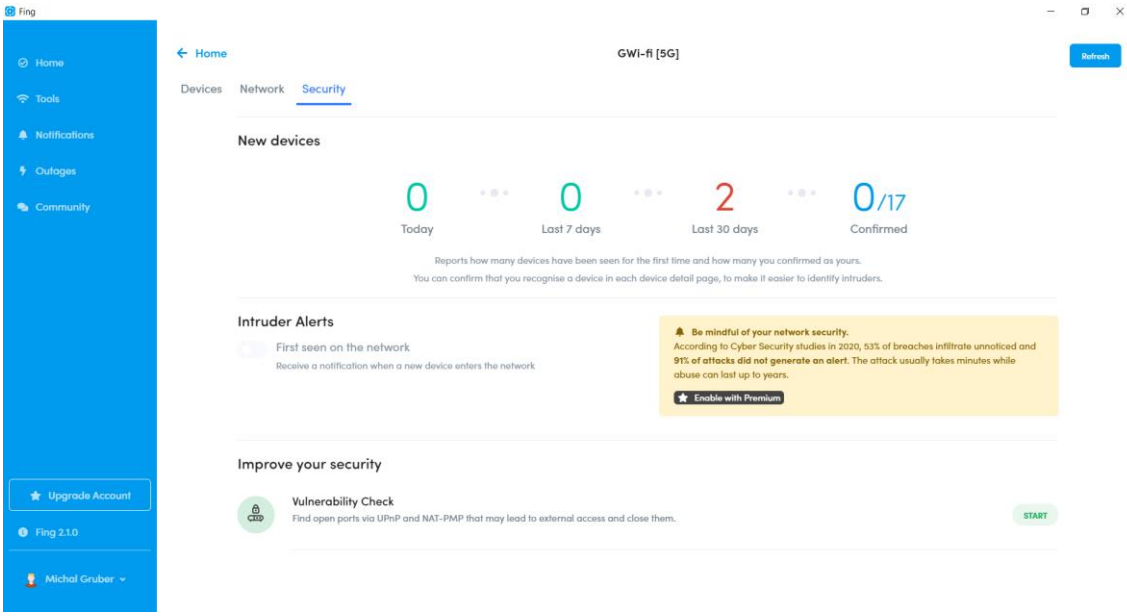


Obrázek 29: Fing detaily network



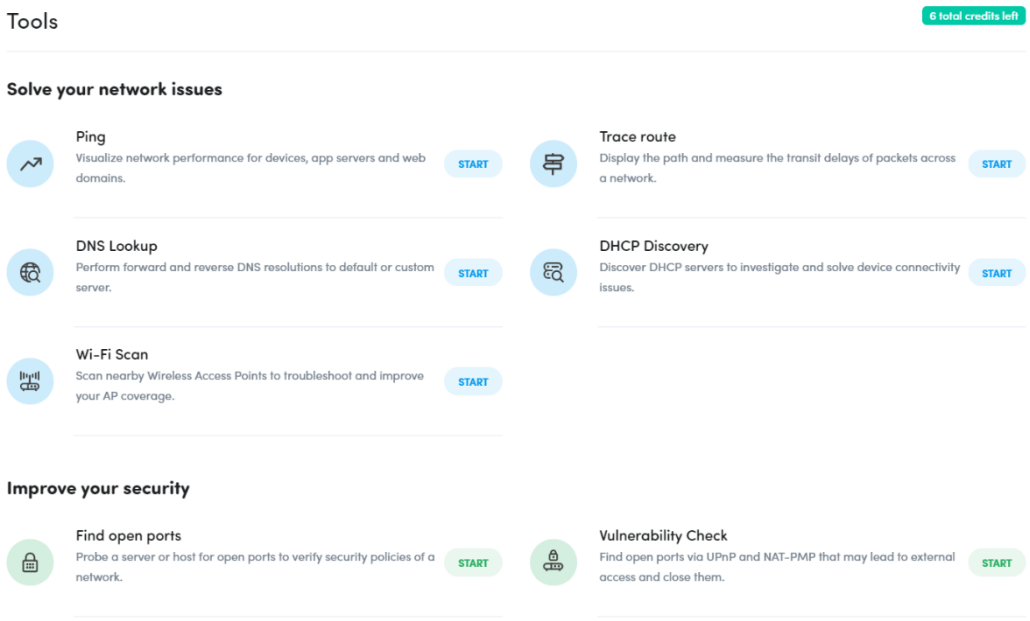
Obrázek 30: Fing wifi events

V další záložce security můžete sledovat nová zařízení (obrázek 31). Osobně v sítí nemám aktivních tolik zařízení najednou, že bych nepoznal, které do sítě nepatří, proto nemam zařízení nastavené jako známé. V případě většího množství zařízení by se to jistě vyplatilo.



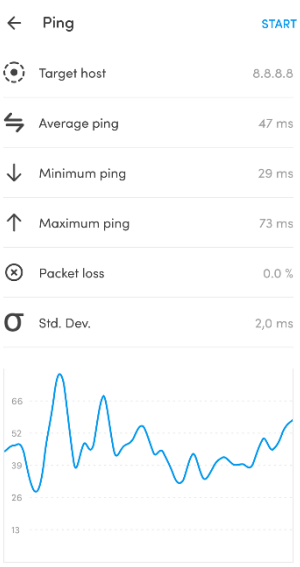
Obrázek 31: Fing device security

Nyní k nástrojům, co Fing poskytuje. Bohužel nechápu, proč Windows verze je omezena 6 kredity (1 kredit = 1 použití nástroje). Kredity můžete vidět v pravém horním rohu obrázku 32. Mobilní verze žádné tyto limitace nemá, ale zase tam chybí některé nástroje. Zelené nástroje jsou ještě specifické. Hledat porty můžete po jednom za den. Na androidu to jde bez problému najít najednou a kolikrát chci. Vulnerability check zase můžete využít jenom v prémiové verzi a v mobilní verzi vůbec není.

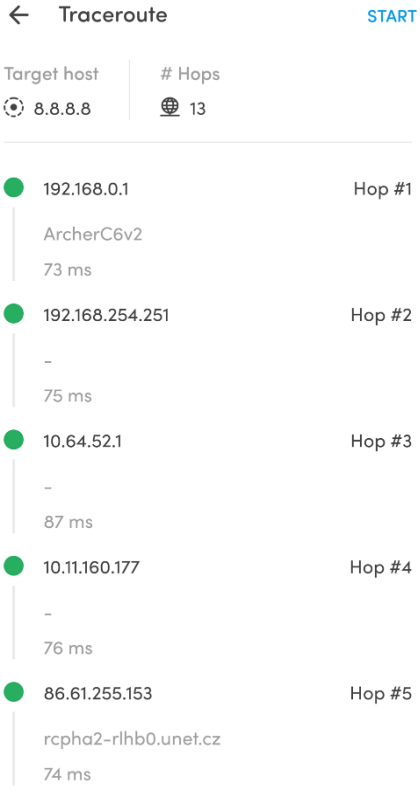


Obrázek 32: Fing nástroje

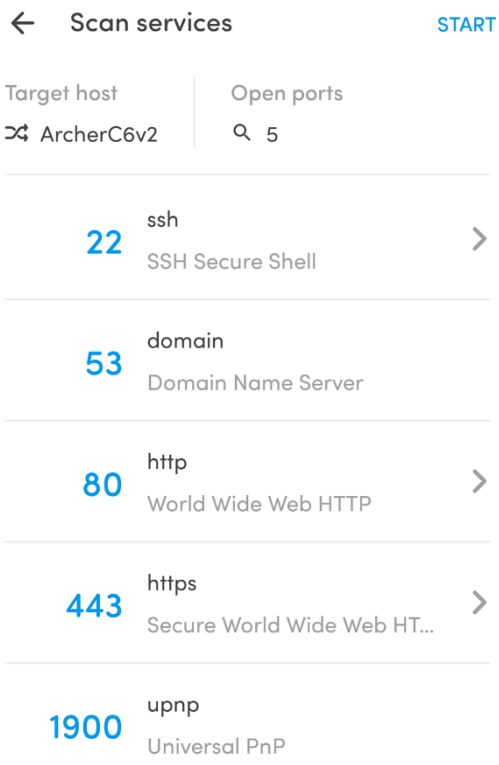
Jak jsem již zmínil, velikou výhodou je, že si mohu najít zařízení v síti a využít na něj některý z nástrojů bez nutnosti opisu adresy. Podobné je to u využití přímo určitého nástroje, kde nám to hned nabízí již vyhledávané adresy. Toto dost urychluje práci, kde například dám ping na 8.8.8.8, a při přejití na traceroute, nám to hned nabízí adresu 8.8.8.8, jelikož jsme ji teď používali.



Obrázek 33: Fing adroid ping

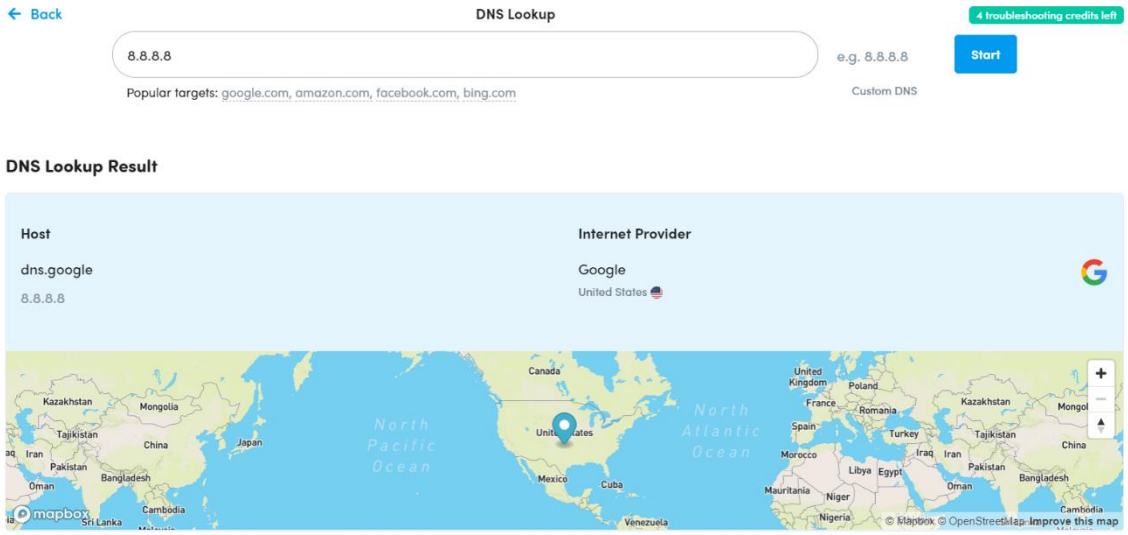


Obrázek 34: Fing android traceroute



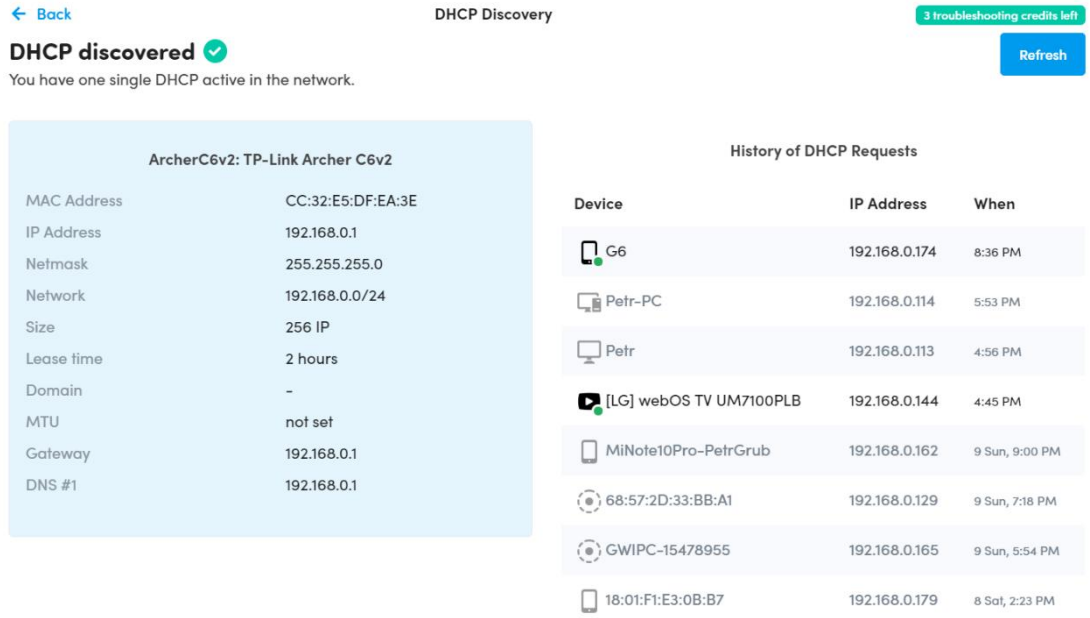
Obrázek 35: Fing android scan services

Dotázání na DNS server.



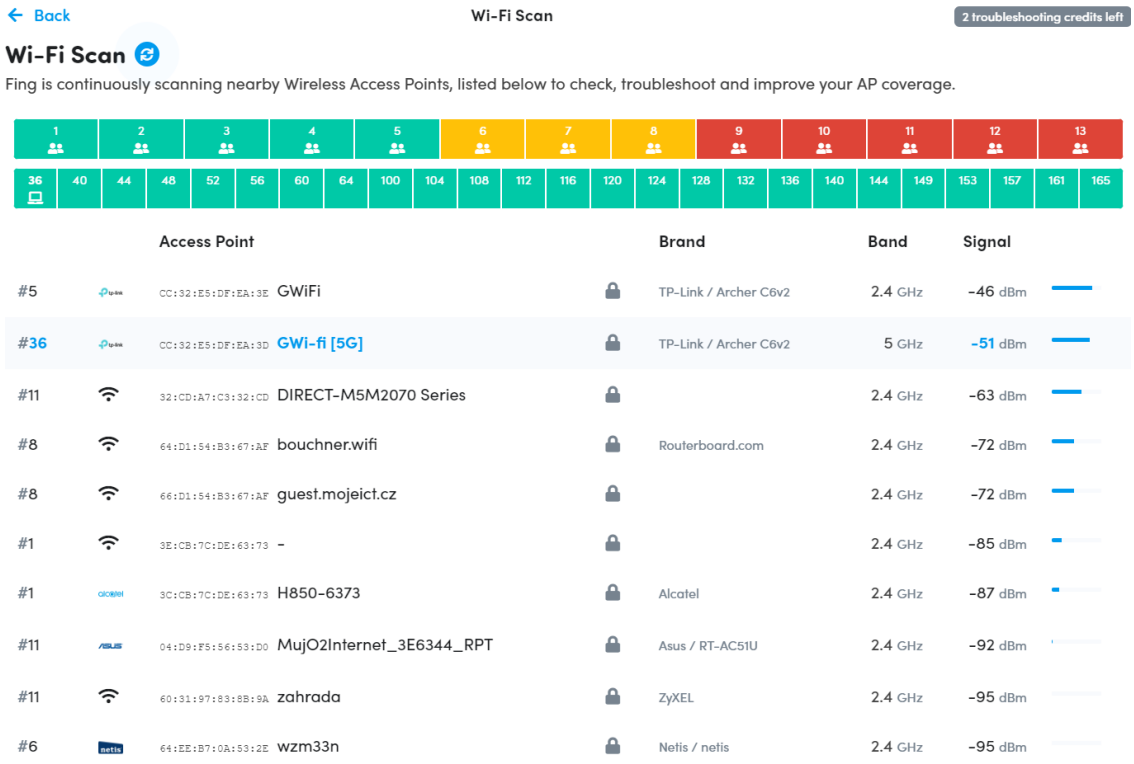
Obrázek 36: Fing Windows DNS Lookup

Zde je historie zařízení, které žádali router o IP adresu.



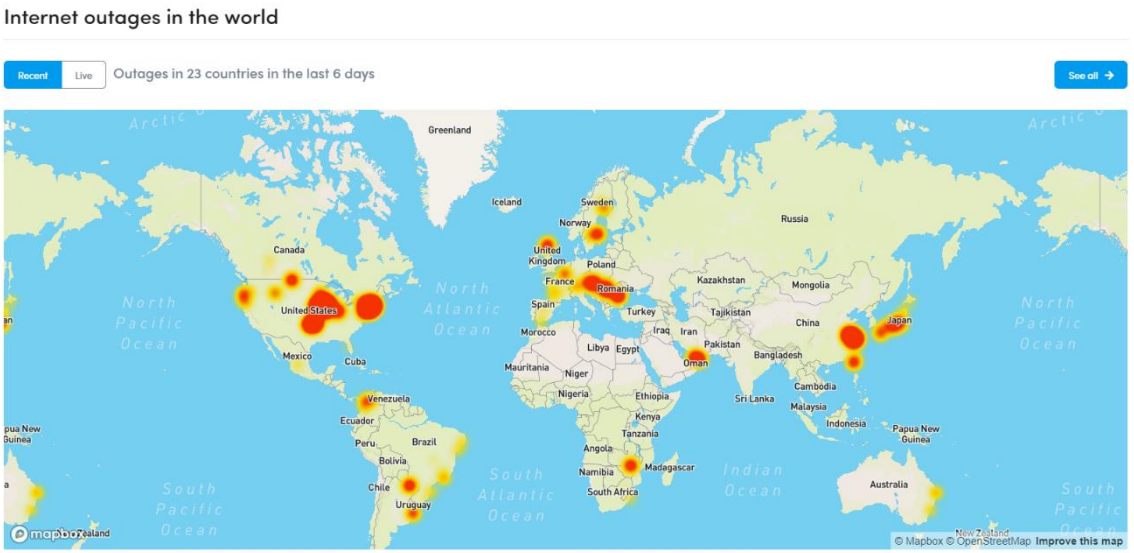
Obrázek 37: Fing Windows DHCP

Hledání sítí v okolí, včetně MAC adres, frekvencí, signálů a pásem.



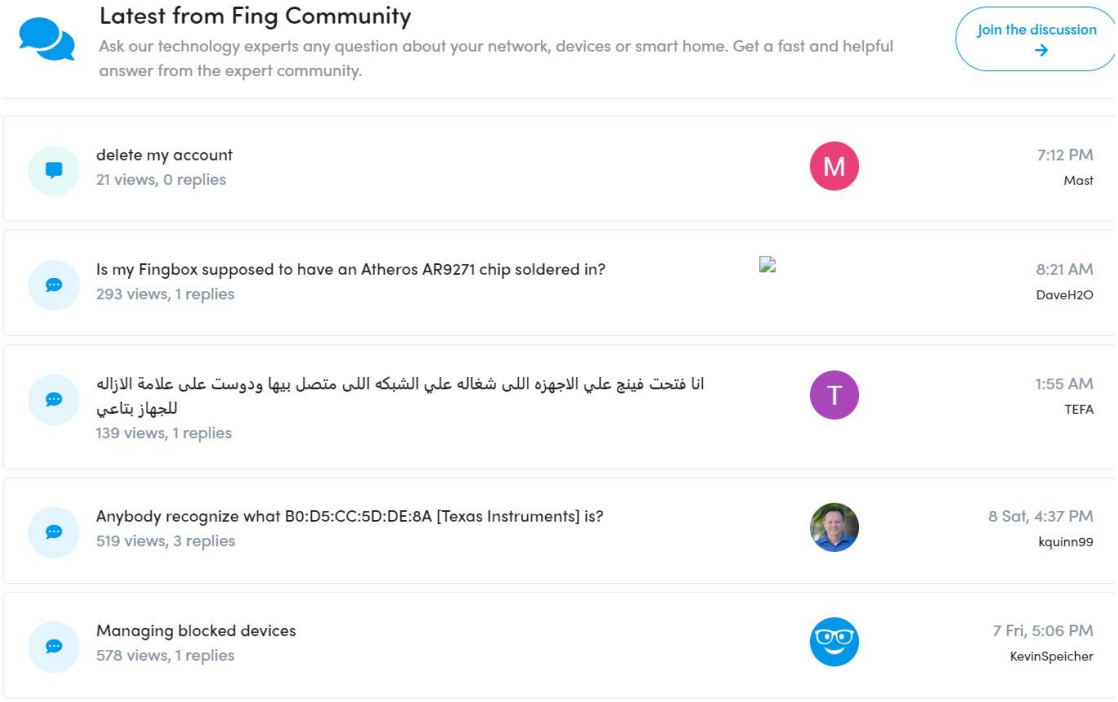
Obrázek 38: Fing Windows Wi-Fi scan

Dále je tu funkce pro sledování výpadků ve světě. Lze přepínat mezi živým přenosem a nedávným.



Obrázek 39: Fing výpadky internetu

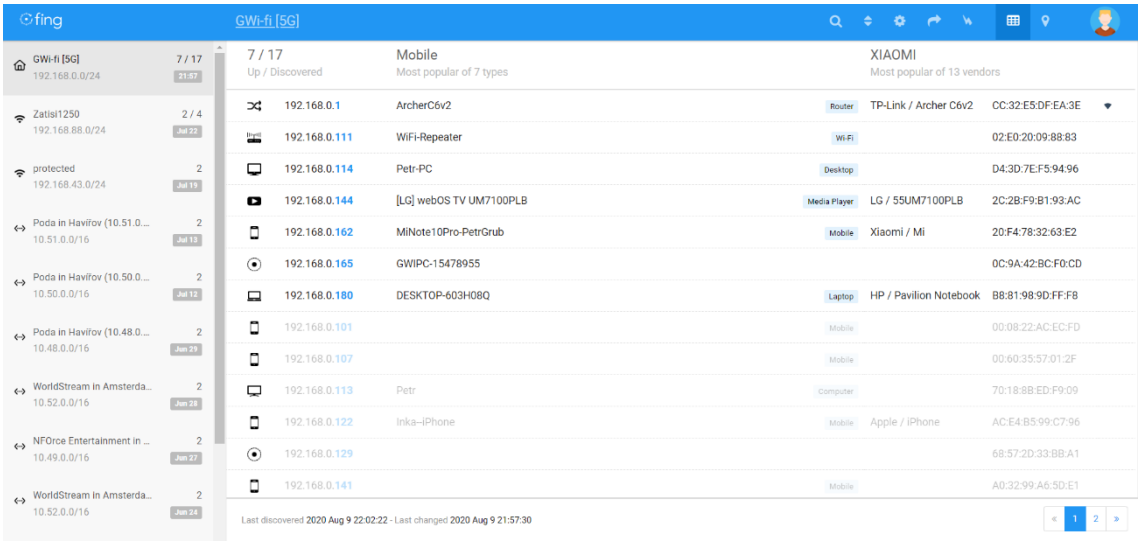
Poslední, co stojí za zmínku je komunita. V aplikaci je přímo chat, kde se dá komunikovat o problémech nebo radách. Aktivita je tu vysoká, tudíž se nemusíte bát, že by vám nikdo neodpověděl.



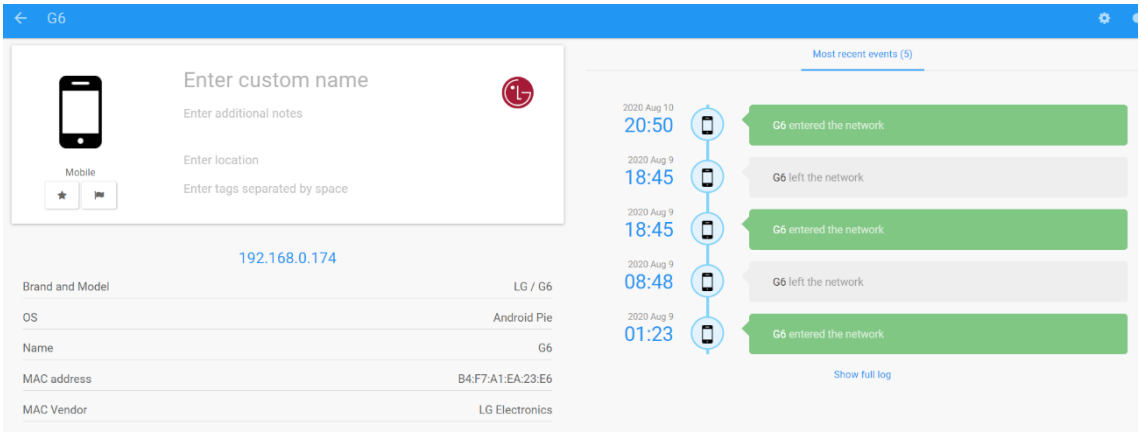
Obrázek 40: Fing komunita

Web

Webová verze slouží převážně k procházení historie sítí. Je zde možnost různě seřazovat zařízení, případně sítě mazat. Nejužitečnější věc je tu historie připojení zařízení, takže můžete sledovat, kdy určité zařízení bylo připojeno (obrázek 42).



Obrázek 41: Fing web app



Obrázek 42: Fing web zařízení

6.1.4 Výsledky otázek

Nyní si vyhodnotíme položené otázky. Na všechny se dá najít odpověď v průběhu praktické části.

Výhody Fingu oproti OS nástrojům

Windows v grafické verzi neposkytuje možnost správy sítě, od toho tu je příkazový řádek, který zvládá základní správu. Diagnostický nástroj sice svůj účel plní, ale mnohdy ani nevíme, co bylo příčinou nedostupnosti sítě nebo jaké kroky podnikl k vyřešení problému.
Android není přizpůsobený na jakoukoliv práci se sítí. V podstatě se spoléhá pouze na aplikace, které si sami doinstalujeme.
Fing je efektivní nástroj pro správu sítě. Obsahuje vše potřebné pro práci se sítí. V případě výpadku sítě lze zjistit, zdali je problém u nás nebo u poskytovatele, případně lze vypsat podrobnosti, kde nastal problém. Největší výhodou je, že je graficky zpracovaný, tedy nebudou s ním mít problém ani úplní začátečníci.

Testování nástrojů

Přijde mi, že Fing je ve všech nástrojích o krok napřed. Sice některé nástroje vykonávají stejnou činnost, tak i přesto Fing podává buď stejné nebo rozšiřující informace. Hlavně všechny tyto informace získáme během krátké doby, kdy nemusíme nikde nic hledat nebo si něco pamatovat.

Co potřebuji pro používání Fingu?

Pro využívání Fingu vám stačí zařízení s podporovaným OS. Nemusíte se ani registrovat, ale přijdete tím o některé možnosti aplikace.

Vlastní zkušenost

Ve Windows jsem se správou sítě neměl nikdy problém. Nejspíše je to zapříčiněno podrobnější znalostí IT. Využíval jsem převážně příkazový řádek.
V Androidu jsem již několikrát hledal základní možnosti pro správu sítě, ač marně.
Fing využívám několik let v mobilní verzi. Je to skvělá a jednoduchá aplikace, která přehledně informuje uživatele o síti a dává mu pokročilejší možnosti pro její správu. Kvůli testování jsem aktualizoval Fing na nejnovější verzi, kde se objevily nově

reklamy a některé testování dováděli aplikaci k nečekaným vypnutí. Dříve jsem tyto problémy neměl. Také jsem si prvně vyzkoušel i počítačovou verzi. Na první pohled bych neřekl, že je zde nějaký rozdíl, krom toho, že se musíte přihlásit, jinak vás to do aplikace nepustí. Počítačová aplikace je omezena na využívání nástrojů, skrze kredity, které se denně obnovují. I přesto bych tuto aplikaci doporučil, protože přináší něco, co nám operační systémy neposkytují.

6.1.5 Shrnutí výsledků a diskuze

Windows jako nejpoužívanější operační systém by mohl implementovat mnohem jednodušší a dostupnější správu sítě. Spoléhá se stále na příkazový řádek, který není pro každého. Grafické nastavení je pouze proklikávání se hromadou nepřehledných tlačítek. V dnešní době, kdy každá domácnost má alespoň jeden router, je třeba mít síť pod kontrolou, což nám Windows neumožňuje. Soustředí se spíše na dané zařízení než na síť jako celek. Od Windows 8 je nové nastavení, které je bohužel místy repetitivní nebo nás odkazuje na staré nastavení. Očekával bych minimálně pokročilejší nastavení nebo přehledněji zpracované to staré. Na mě toto nastavení působí zmatečně.

Android nikdo nepovažuje jako potencionální nástroj pro správu sítě. Velké množství firem si vyvíjí své verze pro své konkrétní značky telefonů. Opět nikdo nebere v potaz, že správa sítě by dnes měla být již samozřejmostí, a ne nástrojem pouze pro techniky. Mělo by i pomoci, že dnes mobilní zařízení značně zastupují mnohé funkce počítačů. Třeba se jednou dočkáme správy sítě přes mobil i od odborníků, ačkoli si myslím, že tuto možnost by převážně využívali lidé pro správu svých domácností.

Fing jako nástroj pro správu sítě dělá svoji práci dobře. Přehledně dokáže zobrazovat informace o síti, kde v případě problému nás upozorní na problém. S mobilní aplikací jsem byl naprosto spokojen roky, proto mě zaráží, jak ji dokázali vývojáři za posledních pár měsíců pokazit. Ohlasy jsou i v recenzích, kde poslední dobou jsou uživatelé nespokojeni. Největší nepochopení mám ale pro počítačovou verzi. Pro přístup do desktop aplikace se musíme prvně přihlásit. Poté zjistíme, že nástroje jsou limitované kredity, kde se ještě liší, co za druh nástroje to je. Některé spadají pod 6 kreditů za den, některé pod 1 kredit a další jsou zase přístupný pouze

v prémiové verzi. Dávalo by smysl, že máme omezený, kolikrát si za den necháme vypsat zařízení, tedy využíváme funkci, kterou jen tak některá aplikace nemá. Kupodivu si zařízení můžeme vypisovat do nekonečna, ale omezení platí na funkce jako ping nebo traceroute. Neomezené vypisování zařízení přisuzuji FingBoxu, který je závislí na aplikaci a při omezeném skenování by byl k ničemu. Naopak základní operace, které lze využívat libovolně v příkazovým řádku jsou omezené. Nelogické je i to, že v mobilní verzi žádné kredity nejsou. Možná vývojáři plánují zavést kredity i do mobilní verze, kde při vývoji počítačové aplikace s tím již počítali.

7 Závěr a doporučení

Cílem této práce bylo seznámit se zabezpečením počítačových sítí proti různorodým útokům. V druhé kapitole byly představeny hrozby jak známé, tak neznáme. Kromě jejich praktik, byla zmíněna i obrana a protiopatření. Pachatelé vymýšlí postupem času sofistikovanější metody. Začínali na jednoduchém odposlechu a dnes již mají prostředky k vytvoření vyspělých kódů, které bez povšimnutí parazitují na síti nebo systému. Na tento problém navazovalo další téma, kterým byla detekce abnormalit. Třetí kapitola tedy řešila anomálie a jejich detekci. Firmy se snaží zabezpečit počítačovou síť zvenčí, ale nemají ochranu proti již infikované síti. Pro tento účel je tu software pro sledování sítě v reálném čase. Čtvrtá kapitola byla o seznámení se softwarem spojeným se zabezpečením. Zmínka byla o ochranných nástrojích, jako je například VPN nebo firewall. Dále byly řešeny detekční nástroje. Typickými zástupci jsou WireShark a NMap, které lze využít jak k útoku, tak k ochraně sítě. Pátá kapitola se zabývala budoucím vývojem hrozeb a ochrany. Budoucí bezpečnost je dosti řešené téma. Nikdo si netroufne říct, jak se budou vyvíjet hrozby. Jsou některé návrhy na budoucí zabezpečení sítí, ale vždy se ochrana přizpůsobovala novým hrozbám, proto je velmi pravděpodobné, že se vše může změnit. Šestá kapitola byla zaměřena na praktickou část. Zde byla testována aplikace Fing a základní nástroje pro správu sítí operačních systémů Windows a Android. Fing dopadl nejlépe z testovaných nástrojů. Je vhodný pro administraci celé sítě a přehledně předává informace uživateli. Windows některé základy zvládá, ale je spíše vhodný pro správu daného zařízení než pro správu celé sítě. Naproti tomu Android skončil nejhůře, jelikož žádnými nástroji nedisponuje.

V této práci je zmíněno mnoho témat, které by si zasloužili svoji vlastní práci, která by je zpracovala více dopodrobna. Nejvýznamnějším zmíněným tématem je detekce abnormalit. Nástroje pro detekci abnormalit jsou současným kandidátem pro budoucí ochranu sítě. Momentálně nedokážou sami identifikovat abnormalitu, proto je potřeba odborníka, který ji dokáže rozeznat. Dalším námětem, úzce souvisejícím, je bezpečnostní software. Zmapovat a rozdělit do kategorií moderní software a popsat jeho funkčnost.

8 Seznam použité literatury

[1] What is Eavesdropping Network Attack? - HackersOnlineClub. Home - HackersOnlineClub [online]. Copyright © 2011 [cit. 28.04.2020]. Dostupné z: https://hackersonlineclub.com/what-is-eavesdropping-network-attack/

[2] Top 10 Most Common Types of Cyber Attacks. Netwrix Blog | Insights for Cybersecurity and IT Pros [online]. Copyright © 2020 Netwrix Corporation. All rights reserved. [cit. 28.04.2020]. Dostupné z: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks

[3] Port Scan attacks and its detection methodologies (Theory) : Virtual Intrusion Detection Lab : Computer Science & Engineering : Amrita Vishwa Vidyapeetham Virtual Lab . Amrita Vishwa Vidyapeetham Virtual Lab [online]. Dostupné z: http://vlab.amrita.edu/?sub=7&brch=199&sim=362&cnt=1

[4] TTI | Defending Against Port Scan Attacks. TTI | Home [online]. Copyright © 2020 Turn [cit. 28.04.2020]. Dostupné z: https://www.turn-keytechnologies.com/blog/article/defending-against-port-scan-attacks/

[5] PATHAN, Al-Sakib Khan (ed.). Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press, 2016. ISBN 9780367383527.

[6] Masquerade attack: A wolf in sheep's clothing | Cyware Alerts - Hacker News. Cyber Fusion & Threat Intelligence Solution Company | Cyware [online]. Copyright © 2020 [cit. 28.04.2020]. Dostupné z: https://cyware.com/news/masquerade-attack-a-wolf-in-sheeps-clothing-93393863

[7] What is a Replay Attack and How to Prevent it | Kaspersky. Kaspersky Cyber Security Solutions for Home & Business | Kaspersky [online]. Copyright © [cit. 28.04.2020]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/replay-attack

[8] What is Spoofing? Definition and Explanation | Forcepoint . Forcepoint | Human-Centric Cybersecurity [online]. Copyright © 2020 Forcepoint [cit. 28.04.2020]. Dostupné z: https://www.forcepoint.com/cyber-edu/spoofing

[9] Protection Against Spoofing Attack: IP, DNS & ARP | Veracode. Use Veracode to secure the applications you build, buy, & manage [online]. Copyright © 2020 VERACODE, All Rights Reserved 65 Network Drive, Burlington MA 01803 [cit. 28.04.2020]. Dostupné z: https://www.veracode.com/security/spoofing-attack

[10] What Is an Advanced Persistent Threat (APT)? | Kaspersky. Kaspersky Cyber Security Solutions for Home & Business | Kaspersky [online]. Copyright © [cit. 28.04.2020]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

[11] Jin, David & Lin, Sally. (2011). Advances in Computer Science, Intelligent System and Environment. ISBN 978-3-642-23753-9.

[12] What Is a DDoS Attack? Distributed Denial of Service - Cisco. Cisco - Global Home Page [online]. Dostupné z: https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html

[13] What is a denial-of-service attack? | Cloudflare. [online]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

[14] What is a denial of service attack (DoS)? - Palo Alto Networks. Global Cybersecurity Leader - Palo Alto Networks [online]. Copyright © 2020 Palo Alto Networks, Inc. All rights reserved. [cit. 28.04.2020]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

[15] How much cost a DDoS attack service? Which factors influence the final price?Security Affairs. 302 Found [online]. Dostupné z: https://securityaffairs.co/wordpress/57429/cyber-crime/cost-ddos-attack-service.html

[16] The 5 Best Web Application Firewalls (WAFs) Compared | Sucuri. Sucuri - Complete Website Security, Protection & Monitoring [online]. Copyright © 2020 Sucuri Inc. All rights reserved. [cit. 28.04.2020]. Dostupné z: https://sucuri.net/comparison/best-waf/?utm_term=firewall%20dos%20protection&utm_content=&hsa_src=g&hsa_ver=3&hsa_grp=69154362397&hsa_ad=356131446131&hsa_kw=firewall%20dos%20protection&hsa_mt=b&hsa_cam=1055881594&hsa_acc=8341176033&hsa_tgt=aud-341861865759:kwd-314190508029&hsa_net=adwords

[17] Sudhakar, Kumar, S. An emerging threat Fileless malware: a survey and research challenges. Cybersecur 3, 1 (2020). [cit. 28.04.2020]. Dostupné z: https://doi.org/10.1186/s42400-019-0043-x

[18] What Is Fileless Malware? | McAfee. 302 Found [online]. Copyright © [cit. 12.08.2020]. Dostupné z: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html

[19] What Are Unknown Cyberthreats? - Palo Alto Networks. Global Cybersecurity Leader - Palo Alto Networks [online]. Copyright © 2020 Palo Alto Networks, Inc. All rights reserved. [cit. 28.04.2020]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-are-unknown-cyberthreats

[20] Unknown Threats | How To Stay Ahead Of Unknown Threats?. Endpoint Protection | Enterprise Security Solutions [online]. Copyright © Comodo Group, Inc. 2020. All rights reserved. [cit. 28.04.2020]. Dostupné z: https://enterprise.comodo.com/security-solutions/unknown-threats.php

[21] 2020: The year of unknown cyber threats. Are you cyber-ready? [online]. Dostupné z: https://tehtris.com/en/2020-the-year-of-unknown-cyber-threats-are-you-cyber-ready/

[22] Network Behavior Analysis & Anomaly Detection | Flowmon. [online]. Copyright ©2020 Flowmon Networks a.s. [cit. 28.04.2020]. Dostupné z: https://www.flowmon.com/en/solutions/security-operations/network-behavior-analysis-anomaly-detection

[23] Pramit Choudhary. (2017). Introduction to Anomaly Detection [online]. Dostupné z: https://blogs.oracle.com/datascience/introduction-to-anomaly-detection

[24] Fing Desktop | Network toolkit and scanner | Fing. Fing - IoT device intelligence for the connected world | Fing [online]. Copyright © 2020 Fing. All rights reserved [cit. 12.08.2020]. Dostupné z: https://www.fing.com/products/fing-desktop

[25] LYON, Gordon. Nmap. Nmap [online]. [cit. 2020-08-12]. Dostupné z: https://nmap.org/

[26] IP Packet Types. Embedded RTOS for x86 Embedded Systems [online]. Copyright © 1996,2020 On Time [cit. 12.08.2020]. Dostupné z: http://www.on-time.com/rtos-32-docs/rtip-32/programming-manual/tcp-ip-networking/ip-packet-types.htm

[27] Wireshark · Go Deep.. Wireshark · Go Deep. [online]. Dostupné z: https://www.wireshark.org/

[28] Co je firewall? | ESET. Malware Protection & Internet Security | ESET [online]. Copyright © 1992 [cit. 12.08.2020]. Dostupné z: https://www.eset.com/cz/firewall/

[29] What is a Firewall? The Different Firewall Types & Architectures. Compuquip Cybersecurity | Enterprise IT Security Solutions [online]. Copyright © 2020 Compuquip Cybersecurity. All Rights Reserved. [cit. 12.08.2020]. Dostupné z: https://www.compuquip.com/blog/the-different-types-of-firewall-architectures

[30] What Is a Next-Generation Firewall (NGFW)? - Cisco. Cisco - Global Home Page [online]. Dostupné z: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html#~choose-an-ngfw-firewall

[31] Comodo Firewall | Get Best Personal Firewall Software for $17.99 A Year. Comodo Firewall | Get Best Personal Firewall Software for $17.99 A Year [online]. Copyright © [cit. 12.08.2020]. Dostupné z: https://personalfirewall.comodo.com/

[32] What Is a VPN? - Virtual Private Network - Cisco. Cisco - Global Home Page [online]. Dostupné z: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.htmlSd

[33] Types of VPN. VPNOneClick [online]. Dostupné z: https://www.vpnoneclick.com/types-of-vpn-and-types-of-vpn-protocols/

[34] Resources » Radar Cyber Security. Radar Cyber Security – Safeguard your digital journey [online]. Copyright © RadarServices Smart IT [cit. 12.08.2020]. Dostupné z: https://www.radarcs.com/resources/Geg

[35] Gartner: The Future of Network Security Is in the Cloud. Zscaler Cloud Security — Secure Your Digital Transformation [online]. Copyright ©2008 [cit. 12.08.2020]. Dostupné z: https://www.zscaler.com/blogs/corporate/new-report-gartner-research-future-network-security-cloud

[36] What Is SASE? - Palo Alto Networks. Global Cybersecurity Leader - Palo Alto Networks [online]. Copyright © 2020 Palo Alto Networks, Inc. All rights reserved. [cit. 12.08.2020]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-sase

[37] AI and the Future of Network Security | Network Computing. Network Computing | [online]. Copyright © 2020 Informa PLC. Informa PLC is registered in England and Wales with company number 8860726 whose registered and head office is 5 Howick Place, London, SW1P 1WG. [cit. 12.08.2020]. Dostupné z: https://www.networkcomputing.com/networking/ai-and-future-network-security

[38] Future of Cybersecurity Threats – Looking Ahead So We Can Prepare Now - Security Boulevard. Home - Security Boulevard [online]. Copyright © 2020 [cit. 12.08.2020]. Dostupné z: https://securityboulevard.com/2020/03/future-of-cybersecurity-threats-looking-ahead-so-we-can-prepare-now/

[39] Zabezpečení na bázi nulové důvěry (zero trust). [online]. Dostupné z: https://www.microsoft.com/cs-cz/security/business/zero-trust

[40] Firewall as a Service (FWaaS) | Cato Networks. Cato Networks | The Network for Whatever's Next [online]. Dostupné z: https://www.catonetworks.com/glossary-use-cases/firewall-as-a-service-fwaas/

[41] CASB: What is a Cloud Access Security Broker? | Netskope. Netskope Cloud Security: Next Gen SWG, Private Access, CASB [online]. Copyright © 2020, All rights reserved. [cit. 12.08.2020]. Dostupné z: https://www.netskope.com/about-casb

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2018/2019

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Gruber Michal	Ing. Kašpara 1143, Havlíčkův Brod	I1600531

TÉMA ČESKY:

Známé a neznámé hrozby na počítačových sítích a nástroje pro jejich detekci

TÉMA ANGLICKY:

Known and unknown threats on computer networks and detection tools

VEDOUCÍ PRÁCE:

Ing. Karel Mls, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cíl: Zmapovat současný stav a trendy bezpečnostních rizik v počítačových sítích a navrhnout způsoby detekce nových hrozeb

Osnova:
Úvod
Hrozby známé i dosud neznámé
Detekce abnormalit
Nástroje a techniky
Budoucí vývoj hrozeb a možné ochrany
Závěr
Zdroje

SEZNAM DOPORUČENÉ LITERATURY:

PATHAN, Al-Sakib Khan (ed.). Security of self-organizing networks: MANET, WSN, WMN, VANET. CRC press, 2016.
STALLINGS, William. Network Security Essentials: Applications and Standards. Pearson, 2016.
HAMED, Tarfa; ERNST, Jason B.; KREMER, Stefan C. A survey and taxonomy of classifiers of intrusion detection systems. In: Computer and network security essentials. Springer, Cham, 2018. p. 21-39.
CHELLI, Kahina. Security issues in wireless sensor networks: Attacks and countermeasures. In: Proceedings of the World Congress on Engineering. 2015. p. 1-3.

Podpis studenta: ..... **Datum:** 17. 10. 2018

Podpis vedoucího práce: ..... **Datum:** 17.10.2018