Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Odposlech síťové komunikace

Tomáš Fišer

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Tomáš Fišer

Informatika

Název práce

Odposlech síťové komunikace

Název anglicky

Interception of network traffic

Cíle práce

Cílem práce je zmapování metod odposlechu komunikace na počítačových sítích, jejich dopadu na bezpečnost uživatelských dat a demonstrace možností jejich zneužití za pomoci programu Wireshark. Dílčím cílem práce je stanovit postupy pro zamezení analyzovaných metod odposlechu.

Metodika

Metodika řešení práce spočívá ve studiu odborných informačních zdrojů. Na základě analýzy získaných poznatků budou vypracovány možnosti odposlechu komunikace na počítačových sítích. Dle teoretické části této práce budou demonstrovány praktické ukázky odposlechu. Zároveň bude poukázáno na možnosti obrany proti odposlechu.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

sniffing, bezpečnost počítačových sítí, wireshark, ethereal, tcpdump

---

Doporučené zdroje informací

BATES,Regis J. Securing VoIP: Keeping Your VoIP Network Safe. First edition. Waltham: Syngress, 2015, 220 pages. ISBN 9780124170391.

BURIAN, Pavel. Internet inteligentních aktivit. Vyd. 1. Praha: Grada, 2014, 332 s. Průvodce (Grada). ISBN 978-80-247-5137-5.

HATCH, Brian, James LEE a George KURTZ. Hacking bez tajemství: Linux. Vyd. 1. Brno: Computer Press, 2003, xiv, 644 s. ISBN 80-7226-869-4.

KUROSE, James F a Keith W ROSS. Počítačové sítě. 1. vyd. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0.

MARAS, Marie-Helen. Computer forensics: cybercriminals, laws, and evidence. Second edition. xv, 2014, 408 pages. ISBN 1449692222.

SANDERS, Chris. Analýza sítí a řešení problémů v programu Wireshark. 1. vyd. Brno: Computer Press, 2012, 288 s. ISBN 978-80-251-3718-5.

Předběžný termín obhajoby

2015/16 ZS – PEF

Vedoucí práce

Ing. Alexandr Vasilenko

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 30. 12. 2015

Čestné prohlášení

Prohlašuji, že svoji bakalářskou práci Odposlech síťové komunikace jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14. března 2016 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Alexandru Vasilenkovi za vedení této práce, cenné rady poskytnuté při konzultacích a čas, který mi při zpracování práce věnoval. Dále bych rád poděkoval Bc. Janu Peterkovi za trpělivost při konzultacích práce.

Odposlech síťové komunikace

Interception of network traffic

Souhrn

Bakalářská práce se věnuje možnostem narušení bezpečnosti komunikace na počítačových sítích a principům jejich odposlechu. Práce je rozdělena na dvě části a to na teoretickou část, která obsahuje samotné principy fungování počítačových sítí a popisuje metody nabourání se do sítě, a na praktickou část, kde jsou demonstrovány pokusy o zachycení dat za použití popsaných metod. Také je zde ukázána nebezpečnost nešifrovaných protokolů. K těmto pokusům byl použit program Ettercap a pro odposlech dat byl použit program Wireshark.

Summary

The bachelor thesis deals with possibilities of security breaches of network communication and principles of its interception. The thesis is divided into two parts, the theoretical part, which contains the principles of computer networking and describes the methods of hacking into the network, and on the practical part, which demonstrates capturing of data using the methods described above. There is also shown the danger of using unencrypted protocols. Program called Ettercap was used for this demonstrations and for the interception of data was used program called Wireshark.

Klíčová slova: sniffing, bezpečnost počítačových sítí, Wireshark, tcpdump, Ettercap

Keywords: sniffing, computer network safety, Wireshark, tcpdump, Ettercap

Obsah

1 Úvod 8
2 Cíl práce a metodika 9
2.1 Cíl práce 9
2.2 Metodika 9
3 Přehled řešené problematiky 10
3.1 Referenční model ISO/OSI 11
3.2 Síťová média 14
3.3 Síťové prvky 15
3.4 Sniffing 17
3.5 Techniky odposlechu 20
3.6 Obrana proti odposlechu 25
4 Vlastní zpracování 27
4.1 Použitý software 27
4.2 ARP Cache poisoning 30
4.3 MAC Flooding 33
4.4 DNS Spoofing 36
4.5 Paralelní připojení k lince 38
4.6 Protokoly HTTP a HTTPS 40
4.7 Odposlech IMAP 42
4.8 Sledování manipulace s ARP Cache 44
5 Zhodnocení výsledků 46
6 Závěr 48
7 Seznam použitých zdrojů 49

1 Úvod

Síťové komunikace jsou dnes nedílnou součástí života. Každoročně stoupá počet prodaných chytrých zařízení, která se připojují na několik druhů sítí najednou, někdy i bez našeho vědomí. (1) O to důležitější je dávat si pozor, která data dáváme volně na síť a která je záhodno dobře zabezpečit.

Tato práce se zaměřuje na bezpečnost počítačových sítí. Veškeré prvky k nim připojené, ať už se jedná o počítače, tiskárny, telefony a další, komunikují pomocí výměny dat mezi sebou. Tato data putují uzly od počátečního ke koncovému zařízení. Ovšem cestou mezi počátečním a koncovým zařízením hrozí, že data mohou být někým odposlechnuta a případně i zneužita. Při dnešním neustálém rozšiřování sítí je někdy potřeba data zachytávat a analyzovat cíleně při řešení problémů například s výkonností nebo k obraně sítě před jejím narušením a nechtěným odposlechem.

Bakalářská práce je věnována možnostem tohoto odposlechu a způsobům jeho dosažení. K porozumění problematice je nejprve potřeba nastínit principy fungování počítačových sítí a samotné způsoby odposlechu. Odposlechnutá data jsou bezcenná, pokud z nich uživatel nedokáže vyčíst informace, která hledá. Proto se práce bude věnovat i příkladům interpretace dat pomocí programu pro operační systémy Windows a Linux. Další důležitou součástí práce jsou možnosti detekce narušení bezpečnosti sítě.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je zmapování metod odposlechu komunikace na počítačových sítích, jejich dopadu na bezpečnost uživatelských dat a demonstrace možností jejich zneužití za pomoci programu Wireshark. Dílčím cílem práce je stanovit postupy pro zamezení analyzovaných metod odposlechu.

2.2 Metodika

Metodika řešení práce spočívá ve studiu odborných informačních zdrojů. Na základě analýzy získaných poznatků budou vypracovány možnosti odposlechu komunikace na počítačových sítích. Dle teoretické části této práce budou demonstrovány praktické ukázky odposlechu. Zároveň bude poukázáno na možnosti obrany proti odposlechu.

3 Přehled řešené problematiky

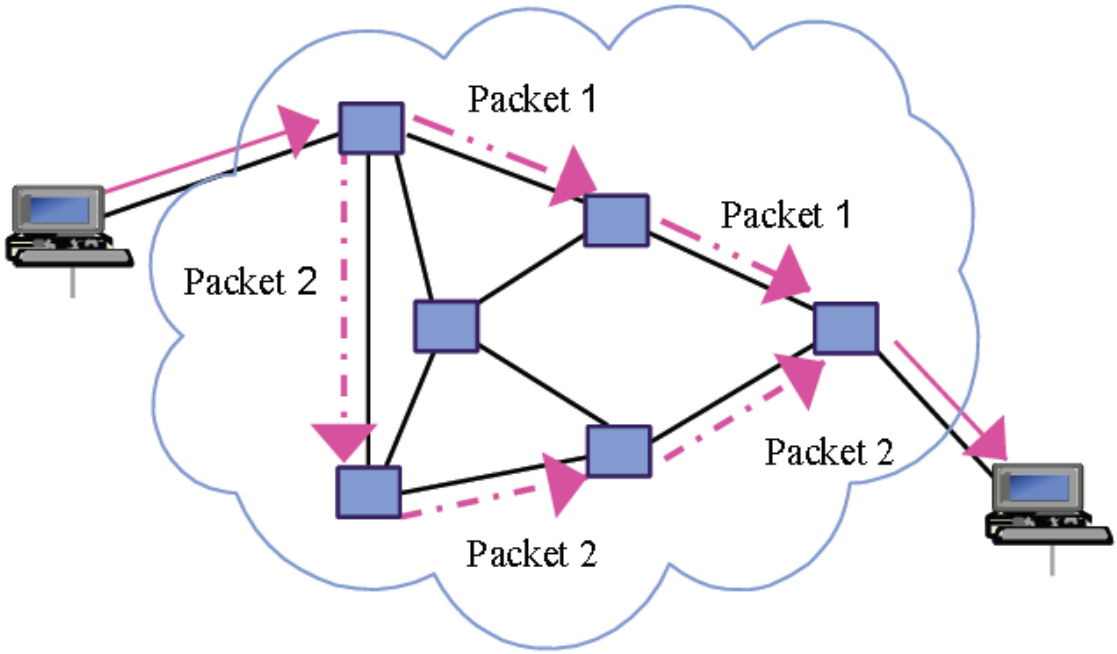
Počítačová síť je skupina počítačů a hardwarových zařízení, která jsou spolu propojena prostřednictvím komunikačních kanálů s cílem usnadnit komunikaci a sdílení prostředků širokému spektru uživatelů. Sítě jsou rozděleny do kategorií na základě jejich vlastností.

Jedním z prvních příkladů počítačové sítě byla komunikace počítačů použitých v americkém radarovém systému SAGE. V roce 1969 byla spuštěna počítačová síť ARPANET, která byla prvním předchůdcem toho, čemu dnes říkáme internet. Byly do ní zapojeny čtyři americké univerzity. University of California Los Angeles, Stanfordský výzkumný institut, University od California Santa Barbara a University of Utah. Síť měla sloužit pro vzdálený přístup k nejvýkonnějším počítačům té doby a měla prověřit funkčnost bez centrální složky, aby byla síť provozuschopná i při výpadku některé části infrastruktury a tudíž byla prakticky nezničitelná. Později byl v ARPANETu poprvé použit protokol TCP/IP, který se v novější verzi využívá dodnes.

Dnešní počítačové sítě se rozdělují zpravidla dle jejich rozlohy a využití. Existuje mnoho druhů a mezi ty nejpoužívanější patří:

- PAN – Personal area network
- LAN – Local area network
- MAN – Metropolitan area network
- WAN – Wide area network

Dnešní počítačové sítě fungují na systému přepojování paketů (packet switching). Tento systém funguje na principu rozdělení zprávy na více menších částí, takzvaných paketů, které jsou po průchodu sítí spojeny na straně příjemce zpět do celistvé zprávy dle čísla paketu. Pro řízení provozu sítě bylo dále nutné zavést adresování, aby síťová zařízení věděla, kam pakety směrovat a odkud byly poslány. Poté o směrování paketů rozhodují prvky na síťové vrstvě dle své směrovací tabulky.



Obrázek 1:Packet switching

3.1 Referenční model ISO/OSI

Řízení komunikace na síti je vcelku složité, proto se pro fungování sítě používají modely. Ty rozdělují jednotlivé činnosti na vrstvy. Každá vrstva má jasně daný účel, který plní při řízení komunikace a proto je důležité tomuto modelu porozumět, aby tyto znalosti mohly být později využity při analýze komunikace. Základním modelem je referenční model OSI/ISO.

Referenční model OSI/ISO je určen ke standardizaci komunikace na počítačových sítích a v roce 1984 byl přijat jako mezinárodní norma. Je rozdělen na 7 vrstev, kdy každá z nich využívá služby své sousední nižší vrstvy a své služby pak poskytuje další vyšší vrstvě v pořadí.

Jednotlivé vrstvy jsou:

- 7. Aplikační
- 6. Prezentační
- 5. Relační
- 4. Transportní
- 3. Síťová
- 2. Linková (spojová)
- 1. Fyzická

Komunikace zdrojové a cílové stanice se musí řídit jasně definovanými pravidly. K této funkci existují pro každou vrstvu protokoly. Na každé vrstvě existuje spousta protokolů, které zajišťují stejnou interpretaci dat mezi zařízeními, definují například způsob kódování, formát dat a další parametry.

3.1.1 Fyzická vrstva

Fyzická vrstva je zodpovědná za přenos bitů informací. Pro zařízení na fyzické vrstvě je nutné nastavit normu pro reprezentaci booleovských hodnot 1 a 0, typicky v podobě rozmezí napětí a délky trvání signálu, než začne reprezentace dalšího bitu. Na rozdíl od ostatních vrstev je fyzická vrstva řešena hardwarově, takže místo protokolů je stanovena technickými normami organizací jako IEEE, ITU a ISO.

3.1.2 Linková (spojová) vrstva

Hlavním úkolem linkové vrstvy je zajištění spojení mezi dvěma sousedícími systémy. Jejími dalšími úkoly jsou zajištění přístupu k médiu, zapouzdření paketů do rámců (frame) přiměřené velikosti pro použité médium, fyzické adresování, výměnu rámců mezi uzly v místní síti a detekci a hlášení chyb. Linková vrstva vezme informace od vyšší vrstvy a opatří je MAC adresami odesilatele a příjemce (jedinečný identifikátor sousedního zařízení) a předá fyzické vrstvě. Když vrstva přijme příchozí rámec, zkontroluje MAC adresu a kontrolní součet a rámce, které nejsou určeny jí, zahazuje.

3.1.3 Síťová vrstva

Linková vrstva zajišťuje spojení pouze dvou přímo propojených zařízení. Pokud ale vede spojení přes jeden nebo více mezilehlých uzlů, přichází na řadu vrstva síťová, která zajišťuje směrování (routování) dat po síti, na této vrstvě označovaných pakety. Úkolem této vrstvy je tedy hledání optimální trasy (route) a samotné směrování paketů jednotlivými uzly až ke koncovému příjemci. Nejznámějším protokolem na síťové vrstvě je protokol IP (Internet protocol). Využívá označení každého koncového zařízení unikátní IP adresou, aby bylo možno odesílat data na určité zařízení. Zatím je stále nejrozšířenější IPv4, ovšem kvůli nedostatku adres se postupně přechází na IPv6 (32bitová vs. 128bitová adresa).

3.1.4 Transportní vrstva

Transportní vrstva díky vrstvě síťové vidí komunikaci již jako přímou, ať se spojují jakékoliv uzly. Proto se tato vrstva může zabývat již jen komunikací koncových účastníků (end-to-end), tzn. mezi odesilatelem a příjemcem. Úkolem transportní vrstvy je rozdělit přenášená data do paketů a při příjmu je zase spojit, takže lze po síti přenášet libovolně velká data i přes omezení maximální velikosti paketů. Nejdůležitějšími protokoly v této vrstvě jsou TCP (Transmission control protocol) a UDP (User datagram protocol). TCP zajišťuje spolehlivý přenos s detekcí chyb. Při příjmu kontroluje pořadová čísla paketů a také kontrolní součty, případně používá i další způsoby zajištění spolehlivosti přenosu. Tento protokol se využívá například u webových aplikací. Naopak UDP je nespolehlivý protokol. Nelze u něho zaručit, zda a v jakém pořadí pakety dojdou. Jeho využití je u časově citlivých účelů, jako u VoIP telefonie, streamování médií a online her.

3.1.5 Relační vrstva

Relace (Sessions) mezi koncovými zařízeními je potřeba navazovat, udržovat a rušit. Základními prvky relační vrstvy jsou bezpečnostní mechanismy, například přihlašování k relaci a další podoby dialogu s uživatelem

Síťový provoz proudí relační vrstvou buď jednosměrně (half-duplex) nebo obousměrně (full-duplex). V poloduplexním režimu se na relační vrstvě předává tzv. token. Data může vysílat pouze vlastník tokenu. Jakmile jej uvolní a předá protistraně, informace mohou proudit opačným směrem.

Relační vrstva také k datům připojuje značky pro kontrolní body nebo oddělovače, takže pokud je přenos přerušen, lze relaci obnovit bez přeposlání všech jejích předchozích dat. Synchronizací datových toků je docíleno spolehlivosti a efektivity vysílaných relací. (2 str. 52)

3.1.6 Prezentační vrstva

Prezentační vrstva má na starost prezentaci dat na koncových systémech. Jednotlivé počítače mohou používat odlišnou vnitřní reprezentaci dat a právě tato vrstva má za úkol převod přenášených dat, aby byla srozumitelná pro cílové aplikace. Význam dat zůstane zachován, pouze se změní jejich struktura.

3.1.7 Aplikační vrstva

Aplikační vrstva aplikacím poskytuje přístup aplikací ke komunikačnímu systému. Jako jediná se zajímá významem dat a ne jejich strukturou. Díky ní mohou spolu síťové aplikace na zdrojovém a cílovém zařízení spolupracovat. Na této vrstvě je spousta známých protokolů jako například FTP, SSH, DHCP a další.

3.2 Síťová média

Síťové médium je nositelem informace mezi dvěma body počítačové sítě. Dělí se dle použitého materiálu a interpretace logických hodnot v médiu.

Metalická vedení

Nejpoužívanějším přenosovým médiem jsou měděné kabely neboli tzv. metalická vedení. Zpočátku se používaly koaxiální kabely, ale dnes jsou nejčastěji metalická vedení realizována tzv. kroucenou dvoulinkou, neboli UTP (Unshielded twisted pair). Kabel UTP je sestaven ze čtyř párů kroucených vodičů. Páry nejsou vůči sobě odstíněny a jsou krouceny pro zlepšení elektrických vlastností a minimalizaci přeslechů mezi páry. Pokud by byly vodiče vedeny souběžně, chovaly by se jako anténa a vyzařovaly do okolí elektromagnetické vlny. Kroucením je tento efekt výrazně potlačen. Koncové konektory jsou označeny RJ-45 a mají přesně dané zapojení dle použité technologie a její rychlosti. Signály po metalickém vedení putují ve formě elektrických impulsů. Vlivem útlumu a zkreslení signálu je pro kabel kategorie CAT5e, který je pro gigabitový Ethernet dnes nejpoužívanější, maximální délka přenosu bez obnovení signálu 100 metrů. Při větších vzdálenostech je již signál pro stranu příjemce velmi často nečitelný.

Bezdrátový přenos

Mikrovlnné a rádiové frekvence se se používají k bezdrátovému přenosu pomocí elektromagnetických signálů. K bezdrátovému přenosu nejsou potřeba žádná fyzická média, pouze zařízení pracující se standardy k tomu určenými. Ovšem každá překážka snižuje sílu a kvalitu signálu a také použití této technologie skýtá bezpečnostní rizika z důvodu jednoduchého přístupu k síti a její snadné dosažitelnosti. Pro pokrytí budov a přilehlých oblastí se používají sítě Wifi na frekvencích 2,4GHz a 5GHz. Při použití všesměrové antény je dosah této sítě přibližně 50 metrů, dle překážek v cestě signálu. (2 str. 195) Dosah mezi dvěma body lze zvýšit použitím směrové antény. Ta však vyžaduje přesně zaměření a jakákoliv překážka včetně listů stromu dokáže signál rušit. Maximální vzdálenost dvou bodů při použití směrových antén může být až jeden kilometr.

Méně známou technologií jsou sítě WiMAX. Ty jsou spíše zaměřeny na venkovní bezdrátové spoje a pracují v pásmech 2-11GHz. Díky vyššímu vysílacímu výkonu a použití směrových antén nabízí při přímé viditelnosti teoretický dosah až 50km, v zástavbě až několik kilometrů. Další vlastností je zabudovaná podpora QoS, řízení kvality služeb. To umožňuje na WiMAX spojích provozovat například IP telefonii nebo přenášet video v reálném čase. (3)

3.3 Síťové prvky

Nároky kladené na dnešní počítačové sítě jsou čím dál větší. K místní síti se kromě PC připojuje již mnoho druhů chytrých zařízení, například i periferie jako tiskárny. O propojení systému do jedné sítě a její připojení do internetu se starají síťové prvky. Ty lze dále dělit na aktivní a pasivní. Pasivní se podílejí na přenosu dat sítí, ale data nemodifikují ani nemění. Naopak aktivní prvky pracují s daty a různě je vyhodnocují, modifikují nebo zesilují. Příkladem pasivních síťových prvků mohou být konektory, kabely, rozvaděče a další. Mezi aktivní síťové prvky patří routery, switche, huby, bridge a další. Nejvíce skloňovanými vrstvami v oblasti síťových prvků jsou vrstvy síťová, linková a fyzická.

Switch

Switch je aktivní síťové zařízení, které slouží k propojení částí sítě, přičemž využívá druhé vrstvy modelu OSI. V rámci jsou zapouzdřená data, která obsahují zdrojovou a cílovou fyzickou adresu. Fyzická adresa se používá pro směrování v lokálních sítích. Je to unikátní

48 bitový hexadecimální identifikátor síťové karty nebo síťového zařízení. Databáze fyzických adres je po zapnutí switche prázdná. Do ní se zapisují jednotlivé zdrojové adresy příchozích dat s porty, ze kterých přišly. Poté když switch obdrží rámec, porovná cílovou fyzickou adresu se svými záznamy a pokud takovou adresu nezná, odešle data na všechny své porty kromě toho, ze kterého data přišla. K jednomu portu může být přiřazeno více adres, pokud je k němu připojen rozvětvený segment sítě, ovšem jedna fyzická adresa nesmí být přiřazena k více portům současně. Tato tabulka se nazývá CAM (Content addressable memory) tabulka a její velikost je omezená. Switch je také schopen zajišťovat integritu dat pomocí CRC kontrolního součtu.

Router

Úkolem routeru je zajistit komunikaci mezi rozdílnými sítěmi a propojovat je. Router pracuje na třetí vrstvě modelu OSI. Router pracuje s pakety, přesněji s IP adresami v nich obsaženými. Úkolem IP adresy je určit do jaké sítě nebo podsítě koncové zařízení patří a také určit konkrétní koncové zařízení. Router má svou routovací tabulku. Routovací tabulka obsahuje informace důležité pro směrování posílaných paketů. Těmi jsou: cílová IP adresa paketu, maska sítě, next hop IP adresa (IP adresa dalšího zařízení na které je paket poslán), rozhraní na kterém je dostupné next hop zařízení, případně metriku (cena cesty). (4) Každý router se rozhoduje podle obsahu své vlastní tabulky. Na jejím základě ví pouze, kde se nachází zařízení s next hop adresou. Kde se konkrétně nachází cílová síť, neví a nezná ani kompletní cestu. Adresa next hop zařízení se poté využívá pouze k získání jeho fyzické adresy. Cílová IP adresa v hlavičce paketu zůstává nezměněna. Pokud zná router více cest do určité sítě, lze využít load-balancing. Při něm je provoz rozdělen dle metrik jednotlivých cest, aby byla síť rovnoměrně zatížena.

Routovací tabulka obsahuje statické a dynamické záznamy. Statické záznamy se hodí pro malé sítě, ve kterých se nemění topologie nebo pro úpravu dynamických záznamů. Dynamické protokoly zajišťují výměnu informací o přímo připojených sítích k ostatním routerům. Každý router zná po spuštění pouze své přímo připojené sítě. Proces výměny informací pomocí směrovacích protokolů se nazývá proces konvergence sítě. Důležitým úkolem směrovacích protokolů je automatické udržování směrovací tabulky. (5) Mezi nejznámější routovací protokoly ve vnitřních sítích patří RIP, EIGRP a OSPF. Prakticky jediným v současnosti používaným vnějším směrovacím protokolem je BGP. Ten zajišťuje

směrování mezi autonomními systémy pomocí hraničních routerů. V BGP se směrovací informace vyměňuje mezi sousedními routery s použitím protokolu TCP k zajištění spolehlivosti.

3.4 Sniffing

Paketový sniffing (odposlech), nebo paketová analýza je proces zachytávání dat proudících lokální sítí a hledání užitečných informací, které by mohla data obsahovat. Systémoví administrátoři často používají paketový sniffing k řešení síťových problémů (například nedostupnosti připojení), k detekci vniknutí cizího narušitele do sítě nebo odhalení napadeného koncového zařízení. K těmto účelům byl původně tento druh analýzy navržen. Jenže s postupným zneužíváním odposlechu síťové komunikace se z paketových snifferů staly spíše bezpečnostní nástroje než pomůcka pro zlepšení provozu. Pokud není síť řádně zabezpečena například vhodným šifrováním, dávají nástroje jako Wireshark, NetworkMiner a další možnost komukoliv pouze s minimem zkušeností a základními znalostmi odposlouchávat, co se na síti děje. Tyto nástroje se staly čím dál více uživatelsky přívětivými, což jim zajistilo širokou uživatelskou základnu.

Paketový sniffing je pasivní technikou. Koncové zařízení při něm není nijak napadáno, data v něm uložena zůstávají nedotčena. Sniffující počítač pouze naslouchá konverzaci mezi koncovým zařízením a výchozí bránou. Toto ovšem platí pouze na nepřepínaných sítích, kde se vyskytují huby.

3.4.1 Legislativa

Neoprávněný odposlech komunikace je sice činnost pasivní, ale i tak je naplněním trestného činu podle §182 Trestního zákoníku – porušování tajemství dopravovaných zpráv. Trestní sazba jsou v tomto případě až dva roky odnětí svobody. Pokud je útočník zaměstnancem poskytovatele telekomunikačních služeb, je sazba dokonce až 5 let odnětí svobody. Dopadnout pachatele však bývá často prakticky nemožné, pokud se nejedná o soustavné dlouhodobé odposlouchávání, například s cílem získání konkurenční výhody.

Zákon č. 40/2009 Sb., trestní zákoník

§ 182 Porušení tajemství dopravovaných zpráv

(1) Kdo úmyslně poruší tajemství

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,
b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo
c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.
(2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch

a) prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo
b) takového tajemství využije.

(5) Zaměstnanec provozovatele poštovních služeb, telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, který

a) spáchá čin uvedený v odstavci 1 nebo 2,
b) jinému úmyslně umožní spáchat takový čin, nebo
c) pozmění nebo potlačí písemnost obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem,

bude potrestán odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti. (6 str. 394)

3.4.2 Promiskuitní režim

Promiskuitní režim je jeden z režimů, ve kterých může pracovat síťová karta. Jejím úkolem je v normálním režimu předávat vyšším vrstvám jen data jí určená (na základě cílové fyzické adresy). Při provozu v promiskuitním režimu je tento filtr deaktivovaný a vyšší vrstvy obdrží veškerá přicházející data. Defaultně je karta v režimu normálním a do režimu promiskuitního musí být přepnuta, k čemuž normálně nedochází. Kartu do tohoto režimu mimo útočníků mohou přepnout například přístroje pro diagnostiku sítě nebo systémy detekce průniku, o kterých ovšem správce sítě nebo uživatel ví.

Detekce karty v promiskuitním režimu

Při zjišťování, zda se v místní síti nachází karta v promiskuitním režimu, se vychází z odlišného chování karty od normálního režimu, protože paket, který by jinak hardwarový filtr karty odmítl, bude přijat. Dále ještě existuje softwarový filtr, který zajišťuje operační systém. Tento filtr odposlech neovlivňuje, protože sniffovací program ho nevyužívá. Softwarový filtr ovšem zabrání zpracování dat, proto je třeba ho obejít. Lze toho docílit například nastavením cílové fyzické adresy na FF:FF:FF:FF:FF:FE, kterou SW filtr špatně vyhodnotí a považuje ji za broadcast adresu a na rozdíl od HW filtru paket propustí dále.

Na Ethernetu směrovaném IP adresami jsou pakety odesílány a přijímány za pomoci fyzických adres. Pakety nelze posílat pouze za použití IP adres a z toho důvodu je potřeba mechanismus, který zjistí k cílové IP adrese její fyzickou adresu. K tomu se používají Address Resolution Protokol (ARP) pakety. ARP pakety pracují na linkové vrstvě, neovlivňují tedy IP adresu. Tento protokol je vhodným pro testování cílového zařízení na zapnutý promiskuitní režim.

Je vznešen požadavek na překlad IP adresy na adresu fyzickou testovaného zařízení. Odešle se ARP request paket s cílovou fyzickou adresou FF:FF:FF:FF:FF:FE (standardně se odesílá s broadcast adresou FF:FF:FF:FF:FF:FF). Softwarový filtr neporovnává celou fyzickou adresu a takto lehce pozměněnou adresu považuje za broadcast adresu. Jelikož switch tuto adresu ve své tabulce nemá, rozešle paket na všechny své porty. Když bude síťová karta v normálním režimu, paket zahodí, jelikož dle cílové fyzické adresy nebude určen jí. Jenže karta v promiskuitním režimu paket přijme a odpoví na něj ARP reply paketem. Že je tedy karta v promiskuitním režimu se dozvíme díky tomu, že odpoví na zprávu, která není určena jí. (7)

3.5 Techniky odposlechu

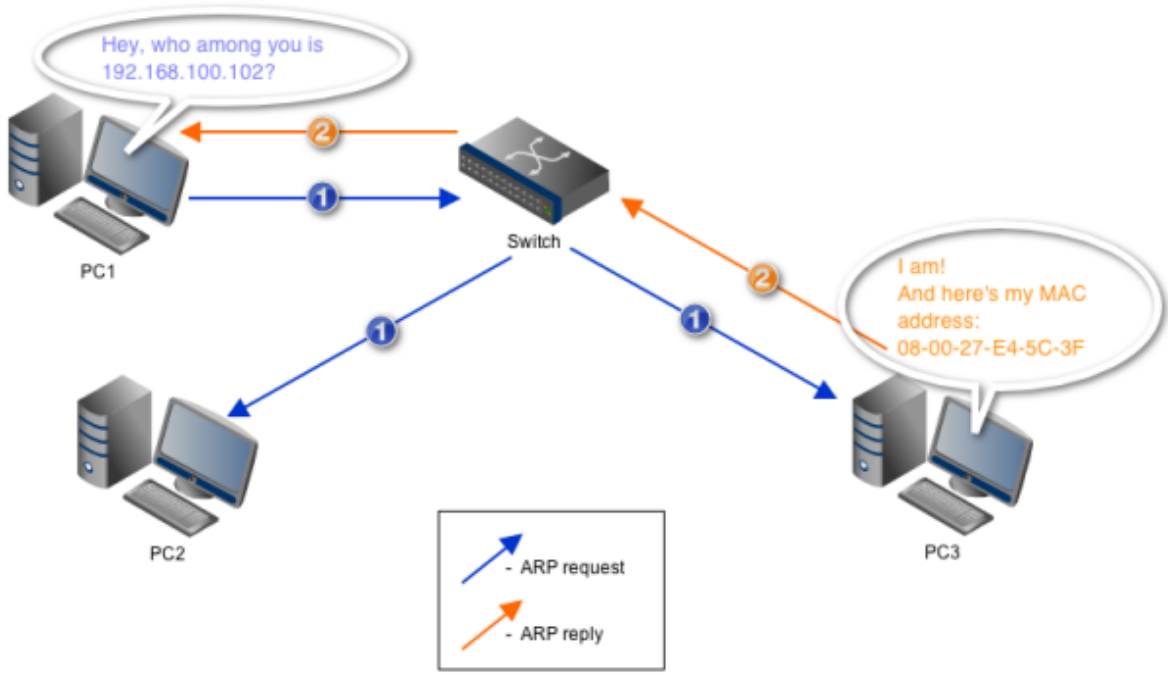
Na nepřepínaných sítích se pro odposlech stačilo pouze připojit do místní sítě. Síťové prvky, typicky HUBy, nerozlišovaly, komu jsou pakety určeny, a proto veškerou komunikaci odesílaly všem zařízením. Díky tomu byla velmi lehce dostupná komunikace všech počítačů připojených k HUBu. Kvůli neoddělování kolizních domén se HUBy přestaly vyrábět a používat a nahradily je switche pracující na linkové vrstvě, které již rozlišují cílové zařízení dle fyzické adresy a oddělují kolizní domény. Pro sniffera to znamená, že nejprve musí zařízení přesvědčit, aby poslalo data jemu a on je mohl odposlechnout.

3.5.1 ARP Cache poisoning

Cílem této techniky je přimět switch posílat cílovému zařízení data určená někomu jinému. Využívá se při ní slabin protokolu ARP. Uvažujme místní síť propojenou switchem. Switch využívá adresace pomocí fyzických adres, protože pracuje na linkové vrstvě. Když switch přijme pakety, podívá se na cílovou fyzickou adresu, tu vyhledá ve své tabulce a data pošle portem, který má u této adresy přiřazen.

ARP Cache

Počítač pošle paket ARP request. Cílovou fyzickou adresu musí počítač teprve získat z odpovědního paketu ARP reply, proto je v datové části request paketu nastavena na 00:00:00:00:00:00. Cílová fyzická adresa v adresové části je FF:FF:FF:FF:FF:FF, neboli broadcast adresa, takže je paket poslán na všechny porty. Z paketu ARP reply si počítač vezme hledanou fyzickou adresu cíle. Nyní počítač ví, jakou fyzickou adresu má cílový počítač a vytvoří si proto záznam do paměti s těmito adresami. Tento záznam má určitou životnost, po které opět proběhne ARP request. Paměť těchto adres se nazývá ARP Cache.



Obrázek 2: Funkce ARP

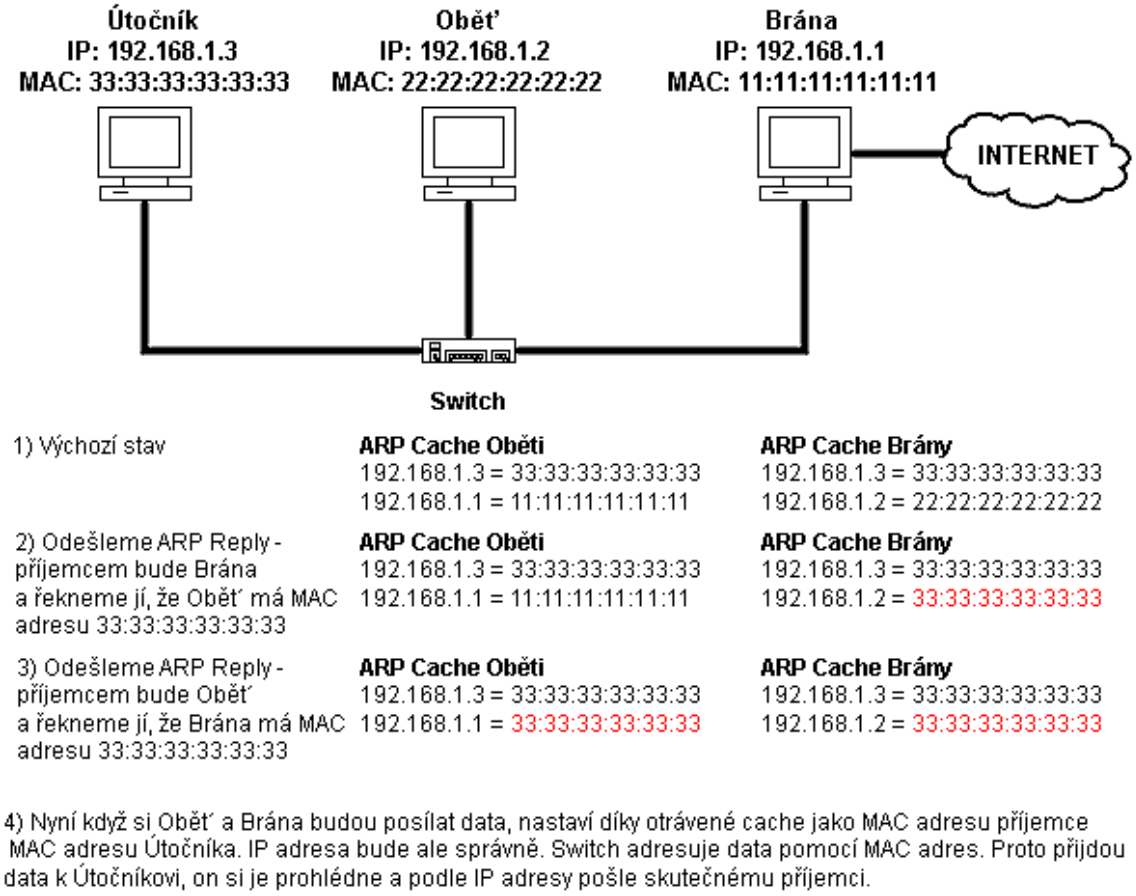
Teorie útoku

Protokol ARP nedisponuje ochrannými mechanismy, protože pochází z doby, kdy se na bezpečnost nehledělo. To z něho činí snadno napadnutelný cíl. Postrádá jakoukoliv formu autentifikace, takže není možné ověřit, zda fyzická adresa v ARP reply paketu opravdu patří zadané IP adrese. Další chybou je příjem ARP reply paketů bez ověření, zda byl nějaký ARP request odeslán. (8)

Mějme síť, ve které jsou 3 počítače vzájemně propojené switchem. Pro přehlednost můžeme pojmenovat počítače Útočník, Oběť a Brána. Brána je připojena k internetu a všechny ostatní počítače k internetu musí přistupovat přes ni.

Útočník pošle ARP reply paket Oběti, ve kterém tvrdí, že Brána má stejnou fyzickou adresu jako útočník. Díky absenci ověření odeslání ARP request paketu oběť reply přijme a změní záznam ve své cache. Poté útočník pošle ARP reply paket bráně a v něm bude tvrdit, že oběť má stejnou fyzickou adresu jako útočník. Nyní pokud chce Oběť poslat data do internetu přes Bránu, dosadí jako cílovou fyzickou adresu Útočníkovu adresu a ten data přepošle Bráně. Díky tomu Oběť nic nepozná, protože její požadavek bude vyřízen a Útočník má přístup k veškeré konverzaci mezi nimi. Už zbývá jen zajistit, aby neuplynula doba, po

které by byl záznam z ARP cache smazán. Toho lze docílit opětovným posíláním ARP reply paketů v určitém intervalu. (9)



Obrázek 3: ARP Cache poisoning

Detekce

Detekovat ARP Cache poisoning není vůbec jednoduché. Nejpřístupnější metodou jsou programy určené k porovnávání obsahu ARP Cache. Tyto programy si po spuštění zkopírují aktuální cache. Poté dělají pravidelné kontroly cache, a když dojde ke změně fyzické adresy u nějaké z již uložených adres, upozorní uživatele. Nevýhodou je nutnost provozovat takovýto software na každém počítači v doméně zvlášť. Lze použít i aktivní detekci, kdy počítač požádá o ARP překlad a pokud se odpověď bude lišit od záznamu uloženého v cache, je někde jistě chyba.

3.5.2 MAC Flooding

Útok známý jako MAC Flooding se zaměřuje na slabiny v CAM tabulce switche. Do té jsou ukládány záznamy o tom, která fyzická adresa je připojena ke kterému portu switche. Tyto adresy se čerpají z příchozích dat do switche. Záznamy jsou po určité době nebo delší neaktivitě smazány. Pokud switch obdrží paket s pro něj neznámou cílovou fyzickou adresou, odešle jej na všechny porty kromě toho, ze kterého paket přišel.

Teorie útoku

Úspěch tohoto druhu útoku velmi závisí na chování switche po zaplnění CAM tabulky. Prvním krokem je zaplnění CAM tabulky. Lze ji zaplnit pakety s náhodně generovanými adresami. Switch obdrží paket s pro něj neznámou adresou a odešle ho na všechny ostatní porty, díky čemuž se tyto adresy naučí všechy další switche připojené k infikovanému. Pokud není žádoucí infikovat i další switche a zvýšit tím riziko odhalení, stačí paketům nastavit cílovou fyzickou adresu na vlastní adresu, tudíž se budou vracet a switch je nebude odesílat dále do sítě. Kapacita CAM tabulek se dost liší od tisíců položek až po statisíce. Po jejím zaplnění je více možných scénářů. Buď se switch přepne do režimu, kdy se chová jako hub, nebo dále normálně funguje dle obsahu tabulky a na všechny porty posílá pouze pakety, pro které nemá v tabulce záznam jejich cílové fyzické adresy. I toto lze ovšem obejít. Záznamy v CAM tabulce mají určenou životnost a jsou po nějaké době vymazány. V tu chvíli je třeba rychleji než ostatní PC obsadit uvolněné místo v CAM tabulce. Díky tomu se záznamy o ostatních PC nevejdou co CAM tabulky a data pro ně jsou posílána na všechny porty, tudíž i k odposlouchávajícímu útočníkovi. Tomu již jen stačí mít síťovou kartu v promiskuitním režimu a zachytávat pakety. (10)

Detekce

Ve chvíli, kdy útočník teprve zaplňuje CAM tabulku pouze na jediném switchi, není detekce možná. Po zaplnění tabulky lze pasivní detekcí útok odhalit sledováním příchozích dat na síťovou kartu. Pokud přichází data určená jiným fyzickým adresám, vypovídá to o tom, že switch neví kam data posílat kvůli přeplněné CAM tabulce a rozesílá je všem. Při útoku na všechny switche v síti lze stejným způsobem útok detekovat ještě před zaplněním CAM tabulky, protože switch bude rozesílat spoustu dat s neznámými MAC adresami ještě před zaplněním tabulky své.

3.5.3 Port stealing

Kradení portů opět využívá CAM tabulku switche, přesněji toho, že si při přijetí paketu switch tabulku aktualizuje. Prvním krokem je zjištění fyzické adresy oběti. Poté stačí switchi posílat pakety se zdrojovou fyzickou adresou oběti a svou adresou jako cílovou. Switch si nyní myslí, že oběť je připojena na stejném portu jako útočník a přepíše si data v CAM tabulce. Pokud na switch dorazí paket adresovaný oběti, bude na základě CAM tabulky odeslán k útočníkovi. Ten nyní musí data dále poslat oběti, aby nebyl prozrazen a spojení přerušeno. Je proto potřeba opravit tabulku do pravdivé podoby. Je třeba přestat posílat pakety pro ukradení portu a odeslat ARP request paket. Oběť pošle ARP reply a switch si na základě příchozího paketu opraví svou tabulku. Po obdržení APR reply stačí poslat odposlechnutá data k jejich původnímu příjemci. Poté se celý proces opakuje. Pakety pro kradení portu je potřeba posílat rychle, protože pokaždé když oběť odešle nějaká data, CAM tabulka se obnoví do správné podoby.

Detekce

Detekce kradení portů je dost obtížná, zvláště pokud je útočník na stejném switchi jako počítač, na který útočí. Jediným vodítkem k odhalení jsou ARP request pakety, které se používají k obnovení CAM tabulky. Každý paket pro oběť znamená jeden request. Čím více bude request paketů na stejnou IP adresu, tím snazší je detekce útoku.

3.5.4 DNS Spoofing

Každý počítač v síti má svou vlastní IP adresu. Pro uživatele je však nemožné pamatovat si každou IP adresu serveru nebo počítače, který chce navštívit. Proto existuje systém DNS, který umožňuje přiřadit k číselné IP adrese určité jméno, tzv. doménové jméno, které poté uživatel může použít například ve webovém prohlížeči. (11) Tento systém se skládá ze soustavy serverů uchovávajících databázi IP adres a k nim přidělených doménových jmen.

DNS server funguje na formátu dotaz/odpověď. Uživatel se chce například připojit na adresu www.google.com. Počítač tedy vyšle dotaz na IP adresu doménového jména google.com. Pokud dotázaný DNS server nezná odpověď, vyšle dotaz na další DNS server. Takto se v hierarchické struktuře těchto serverů zjistí odpověď. Ta je odpovědními pakety postupně doručena zpět až k uživateli. Při opakování dotazů nedochází k opětovnému

rekurzivnímu hledání, ale odpovědi se ukládají do místní DNS Cache. Záznamy v ní mají omezenou životnost, po jejíž uplynutí jsou smazány.

Teorie útoku

Při DNS spoofingu je podvržena IP adresa, která se vrací jako odpověď na požadavek o překlad doménového jména na IP adresu. Útočník poté může oběť přesměrovat například na falešné webové stránky jeho banky nebo jakoukoliv kopii stránek, do kterých se zadávají citlivé informace. Ty útočník odposlechne a požadavek poté přepošle na skutečnou adresu, tak aby oběť nic nepoznala.

Je více způsobů, jak provést DNS spoofing, ale nejjednodušší je s využitím techniky ARP Cache poisoning. (viz 3.4.1) Útočník otráví ARP tabulku oběti a výchozí brány, čímž přesměruje všechny pakety včetně DNS paketů přes sebe. Každý DNS dotaz obsahuje své identifikační číslo. Stejné číslo musí obsahovat i odpovědní paket, aby počítač mohl jednoznačně k sobě přiřadit dotaz a odpověď. Útočníkovi tedy stačí vytvořit DNS odpověď se správným identifikačním číslem a podvrženou IP adresou. (12)

Detekce

Detekce tohoto útoku není vůbec lehká. Většinou jsou kopie stránek nerozpoznatelné od originálu, proto je lepší preventivní obrana. Záznamy navštěvovaných stránek s citlivými údaji lze uložit ručně bez potřeby dotazování DNS serveru. Dalším způsobem je zabezpečení pomocí DNSSEC. Tato služba používá asymetrickou kryptografii, tedy použití jednoho klíče na zašifrování a jiného klíče na dešifrování odkazu. (13)

3.6 Obrana proti odposlechu

Obranu proti odposlechu lze rozdělit na dva způsoby. Prvním z nich je detekce odposlechu. Pokud je v sítí detekováno zařízení v promiskuitním režimu nebo zařízení, které generuje podezřelý ARP provoz, je pravděpodobné, že se na síti vyskytuje útočník a je v zájmu správce sítě podniknout kroky k jeho odhalení. To platí ovšem jen pro místní síť. Když data odejdou z hraničního routeru, nevíme, jak je s nimi nakládáno. Zde přichází v úvahu druhý způsob obrany, a to šifrování dat. Útočník sice data může potencionálně zachytit, ale bez znalosti šifrovacích klíčů z nich nezíská užitečné informace. Pokud jsou například dvě geograficky oddělené pobočky firmy, lze s výhodou použít šifrovaných tunelů.

Mezi hraničními routery vytvoříme šifrovaný tunel, který se tváří jako přímé spojení sítí s tím, že data jsou šifrována.

Pokud bereme v úvahu jediného klienta připojeného k cizí síti, například na veřejném wifi hotspotu, obranou proti odposlechu je použití zašifrovaných protokolů. Většina poskytovatelů například poskytuje webový obsah s použitím podepsaného certifikátu. Ten je vystaven k dané doméně, takže lze detekovat útok i v případě man in the middle útoku, kdy by útočník podstrčil jinou IP adresu webového serveru za pomoci DNS spoofingu. I jiné protokoly, například pro komunikaci, mají vesměs šifrovanou verzi.

Pokud na veřejném hotspotu stejně chceme použít nezabezpečený protokol, je možné vytvořit šifrovaný tunel například do domácí sítě nebo využít služeb některého VPN providera (například ExpressVPN, SaferVPN, PureVPN). Příkladem softwaru pro tvorbu tunelů může být například openVPN, který je open source a podporuje jak šifrování statickým klíčem, tak i za použití certifikátů vydávaných pro jednotlivé klienty. Pokud tedy zaměstnanec ztratí notebook, lze zakázat jeho certifikát a ztráta neovlivní bezpečnost sítě. (14)

4 Vlastní zpracování

Tato kapitola je věnována praktickým ukázkám narušení síťové komunikace za účelem odposlechu. Veškeré pokusy a odposlechy probíhaly na vlastní síti s vědomím dotčených uživatelů. Pro propojení byl v následujících pokusech použit switch Repotec a routery Mikrotik RB2011 a TP-LINK TL-WR841N. Oba routery v sobě obsahují víceportový switch. Na obrázcích jsou záměrně zakryty části MAC adres pro zachování bezpečnosti vlastní sítě.

4.1 Použitý software

Pro odposlech síťové komunikace existuje celá řada programů. Tato práce se věnuje využití programů Wireshark a Ettercap. Oba nástroje byly vybrány pro jejich přehledné uživatelské rozhraní a multiplatformnost.

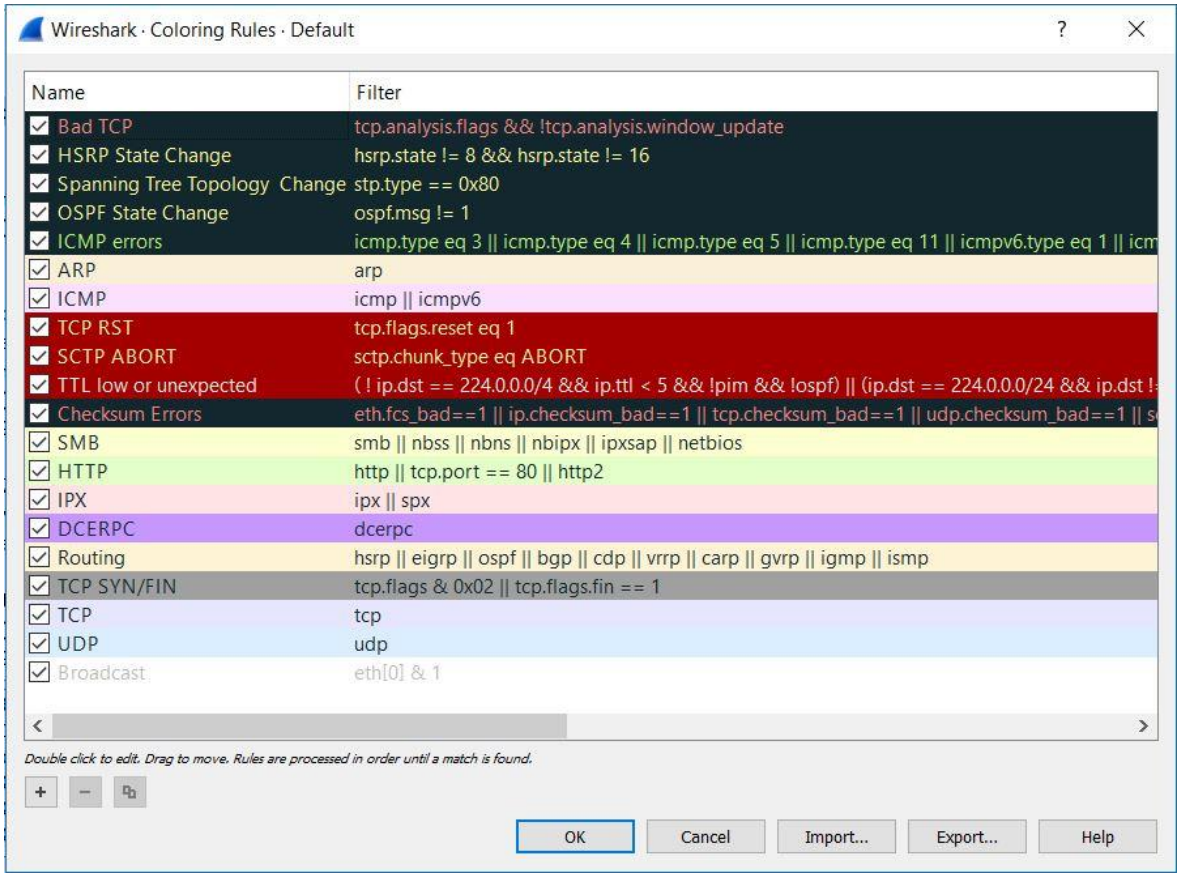
4.1.1 Wireshark

Wireshark je jedním z nejpopulárnějších paketových analyzátorů. Počátek jeho vývoje sahá až do roku 1998, kdy Gerald Combs vyvinul jeho první verzi, ještě pod názvem Ethereal. V roce 2006 Combs změnil zaměstnavatele, avšak neměl práva na značku Ethereal, proto pokračoval ve vývoji pod novým jménem Wireshark. Oblibě se těší hlavně díky tomu, že je open source, tudíž zdarma i pro komerční využití a protože funguje na mnoha platformách, a proto je nástrojem, po kterém sáhne řada profesionálů jako prvním. Aktuální verze byla vydána 26.2.2016 a nese označení 2.02.

Pro provoz Wiresharku je potřeba knihovna libpcap na unixových systémech nebo WinPcap pro Windows. Tyto knihovny se v programech starají o analýzu paketů. Knihovny tvoří rozhraní mezi síťovou kartou a programem, který chce zachytávat pakety. Když síťová karta zachytí rámec, předá jej ke zpracování knihovne libpcap nebo WinPcap. Ta jej podle požadavku prožene filtrem, zbývající data převede do vhodného formátu a předá aplikaci k dalšímu zpracování. (15 str. 131)

Wireshark je uživatelsky velmi přívětivý. Jeho grafické rozhraní je přehledné a vyznačuje se intuitivním rozložením a rozumně sestavenými nabídkami. Další pomocníkem pro lepší orientaci je barevné značení odchycených paketů dle protokolu zobrazené na obrázku níže. Aplikace podporuje kolem tisícovky protokolů a další podporované stále

přibývají. Patří k nim běžné protokoly jako IP, TCP, DHCP, ale i pokročilejší proprietární protokoly jako například AppleTalk.

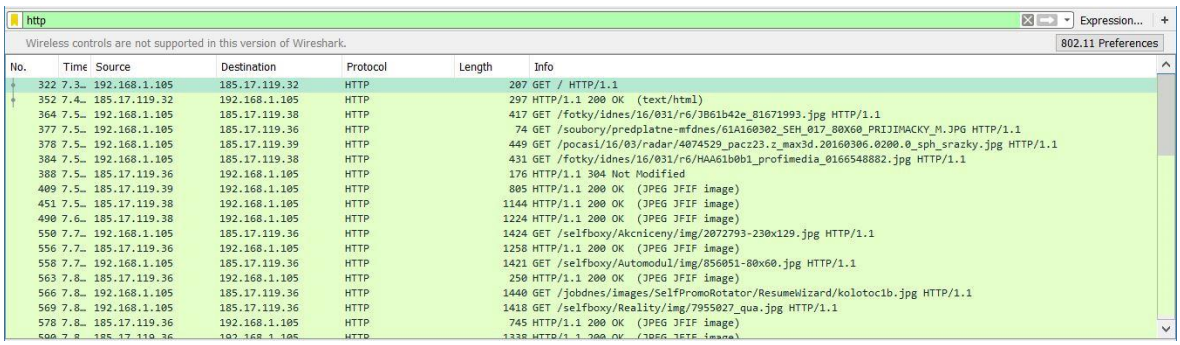


Obrázek 4 Wireshark- pravidla barvení záznamů

Po spuštění programu se zobrazí nabídka dostupných rozhraní pro odposlech i s malými grafy jejich využití. Po výběru rozhraní je automaticky spuštěna relace odposlechu. V ní je okno programu rozděleno na tři části. V první je seznam zachycených paketů včetně základních informací jako zdrojové a cílové IP adresy, použitého protokolu a dalších. V prostřední části jsou zobrazeny podrobné informace o vybraném paketu. Ty jsou hierarchicky děleny a lze je rozbalovat a sbalovat tak, aby bylo možné číst informace zjištěné o paketu. Spodní okno zobrazuje paket v původní nezpracované podobě. Zobrazuje tedy, jak vypadá paket při přenosu sítí. V seznamu zachycených paketů lze poté buď vyhledávat pomocí CTRL + F nebo filtrovat. Pokud není například kvůli ušetření výpočetního výkonu žádoucí zachytávat všechen síťový provoz, lze aplikovat filtry zachytávání. Díky nim lze zachytit provoz pouze na specifickém portu, s určitou IP nebo MAC adresou a mnoha

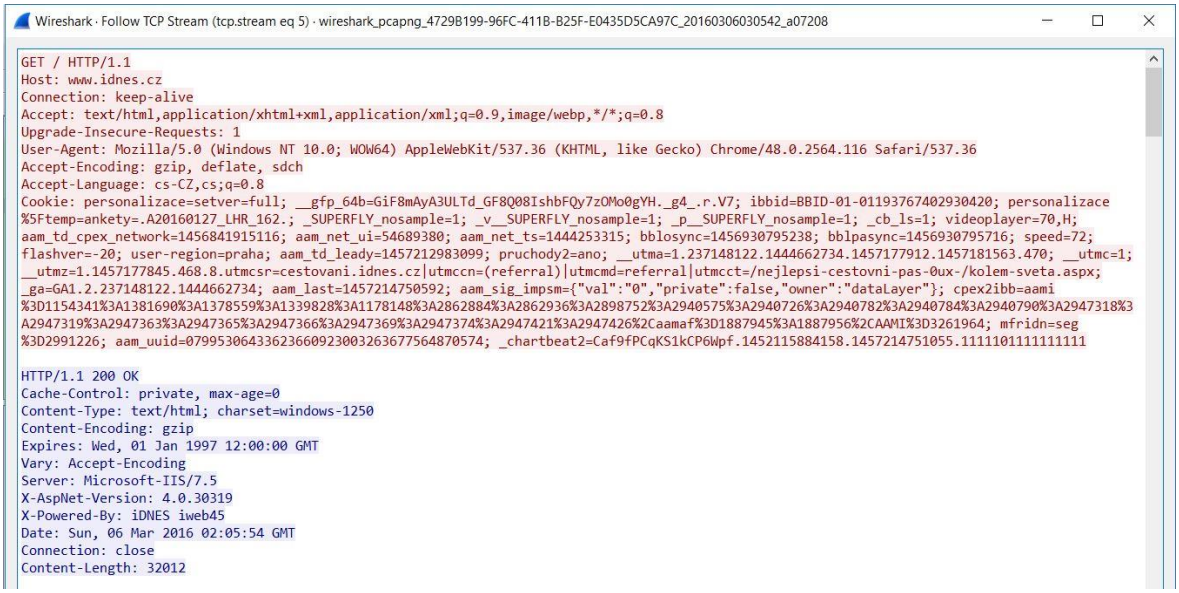
dalšími parametry. Na zachycený soubor paketů lze aplikovat filtr zobrazení, jehož pole je dostupné hned nad seznamem paketů.

Jednou z nejužitečnějších analytických funkcí programu Wireshark je sledování datových proudů TCP (Follow TCP Stream). Tato funkce umožňuje opakované sestavení datových proudů TCP do snadno čitelného formátu. Není nutné data sledovat paket po paketu, ale tato funkce data seřadí, seskupí a usnadní jejich zobrazení. Toto je užitečné například při prohlížení protokolů aplikační vrstvy, jako HTTP, FTP atd. Na obrázku níže je vidět seznam zachycených HTTP paketů.



Obrázek 5 Wireshark- ukázka zachycených HTPP paketů

Z tohoto seznamu není moc patrný celkový kontext a účel paketů. V okně Follow TCP Stream je již ale vidět, že uživatel přistupoval na adresu www.idnes.cz a spousta dalších informací. Červený text zobrazuje komunikaci od zdroje k cíli, modrý naopak. Uživatel jako první vyslal GET požadavek, proto je označen za zdroj. Server mu na jeho požadavek odpověděl zprávou HTTP/1.1 200 OK. (16 str. 100)



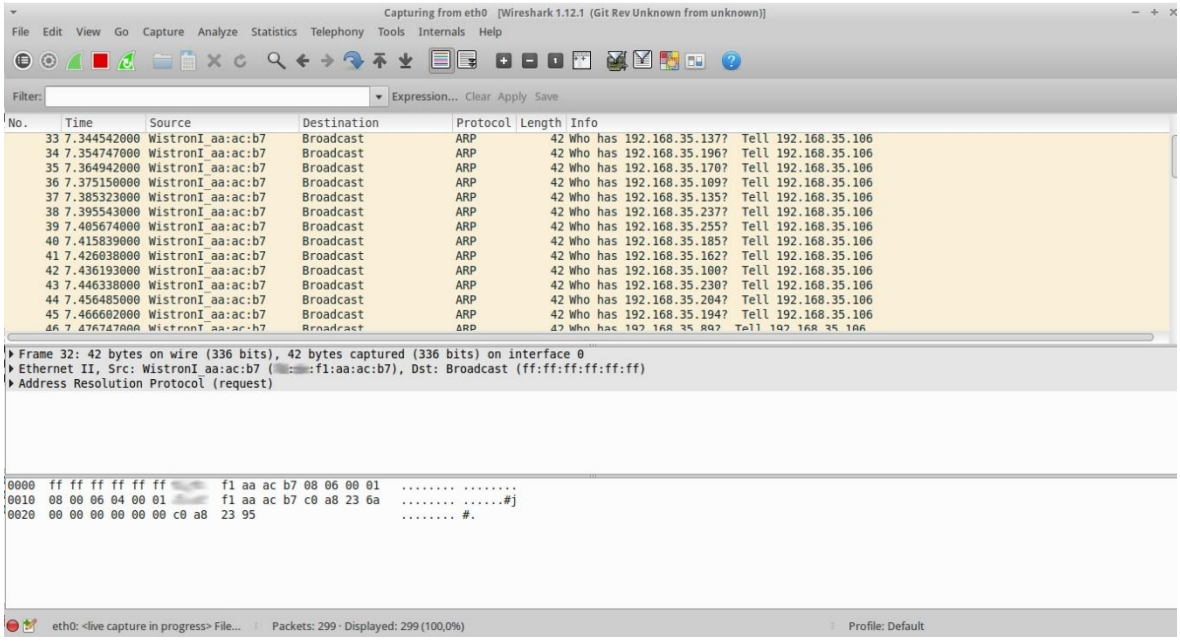
Obrázek 6 Wireshark- funkce Follow TCP Stream

4.1.2 Ettercap

Ettercap je nástrojem pro provádění man in the middle útoků na místních sítích. Jeho tvůrci jsou Alberto Ornaghi a Marco Valleri. Stejně jako Wireshark využívá ke svému provozu knihovny libpcap a WinPcap. Program pracuje na Unixu, Windows i OS X a lze jej provozovat v příkazovém řádku i v interaktivním grafickém režimu. Program podporuje jak pasivní, tak i aktivní odposlech, dekódování protokolů, zachytávání hesel a mnoho dalších funkcí. Navíc do něho existuje spousta zásuvných modulů, takže lze do programu dodat pluginy například pro zaplavování MAC adresami, DoS útoky, port skenery a další.

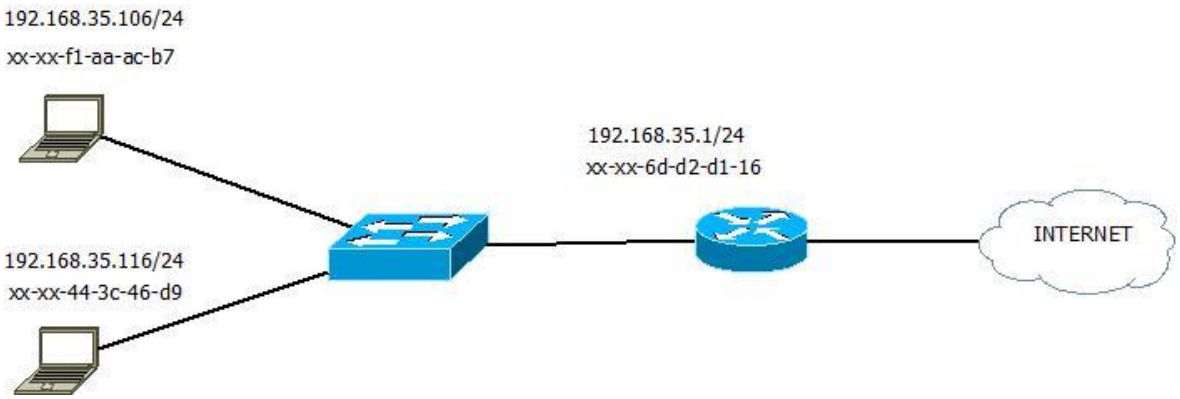
4.2 ARP Cache poisoning

Pro tuto techniku byl použit program Ettercap k samotné otravě ARP tabulky a program Wireshark pro analýzu procesu otravy. Nejdříve je potřeba v programu Ettercap nastavit cíle útoku. Abychom je bylo možné vybrat, je nutné provést skenování sítě volbou Hosts – Scan for Hosts. Program začne vysílat ARP request pakety na všechny adresy v rozsahu své podsítě. Z odpovědních paketů zjistí všechny aktivní zařízení a jejich adresy.



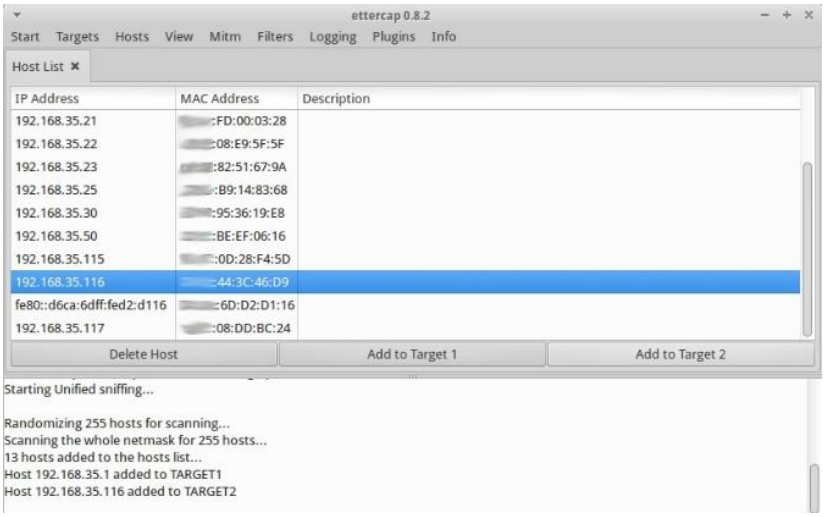
Obrázek 7 Skenování podsítě

Nyní má program všechny aktivní adresy. Dalším krokem je výběr cílů útoku. V tomto případě útočník s IP adresou 192.168.35.106 chce narušit komunikaci mezi obětí s IP adresou 192.168.35.116 a odchozí bránou s IP adresou 192.168.35.1. Zjednodušená topologie sítě je zobrazena na následujícím obrázku. V tomto případě byl použit switch Repotec a router Mikrotik.



Obrázek 8 Topologie ARP Cache poisoning

Pro otrávení ARP tabulek routeru a oběti stačí jen označit jejich IP adresy v Ettercapu jako cíle. Poté v nabídce Mitm vybrat ARP poisoning a potvrdit.

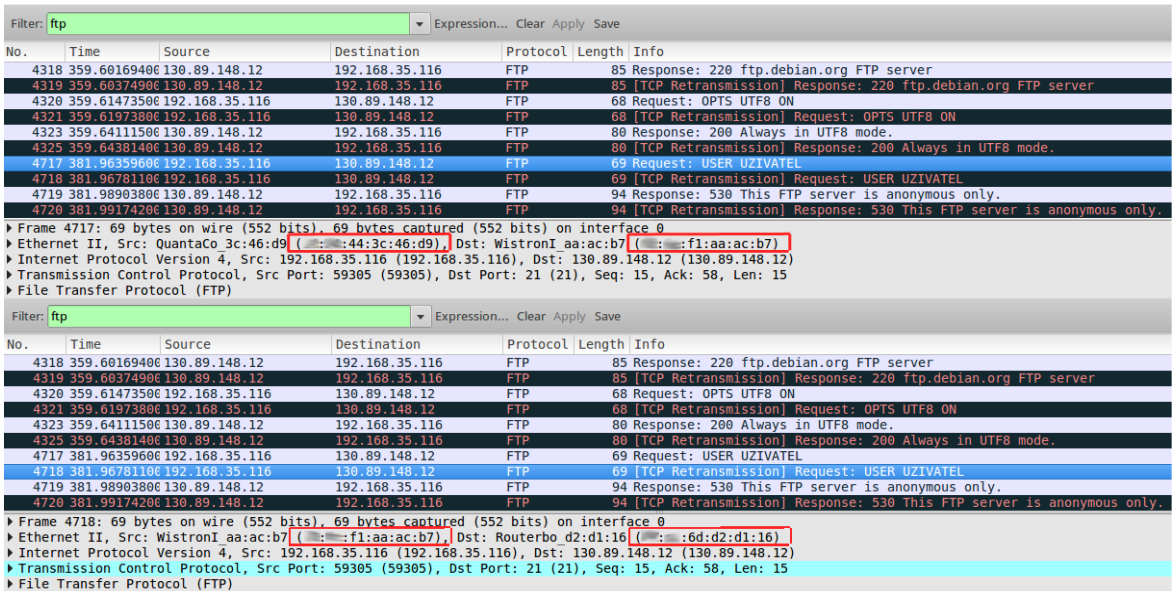


Obrázek 9 Ettercap- výběr cílů

Obrázek 10 Ettercap- spuštění otravy ARP tabulky

Tabulky jsou otráveny a útočník dostává celou konverzaci mezi výchozí bránou a obětí. Toto bylo ověřeno pokusem o přihlášení na ftp server. Na obrázku jsou vidět pakety procházející přes útočníkovu síťovou kartu v obou směrech. První paket na obrázku níže posílá oběť výchozí bráně, ale díky otrávené tabulce je cílová MAC adresa útočníka, viz

červené rámečky. Druhý paket je pouze přeposláním původní žádosti útočníkem k výchozí bráně.



Obrázek 11 ARP poisoning- přeposílání paketů útočníkem

Příkazem arp –a lze v příkazovém řádku systému Windows vypsat obsah ARP tabulky počítače. V ní je shodná MAC adresa u IP adres útočníka a výchozí brány.

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

Interface: 192.168.35.116 --- 0x12
  Internet Address      Physical Address      Type
  192.168.35.1          [illegible]-f1-aa-ac-b7     dynamic
  192.168.35.102        [illegible]-60-c7-ae-ec     dynamic
  192.168.35.106        [illegible]-f1-aa-ac-b7     dynamic
  192.168.35.213        [illegible]-1e-5b-06-fa     dynamic
  192.168.35.255        [illegible]-ff-ff-ff-ff     static
```

Obrázek 12 ARP poisoning- ARP tabulka oběti

4.3 MAC Flooding

K provedení zaplnění tabulek byl použit program macof z repozitáře linuxové distribuce. Ten generuje data s náhodnými MAC adresami a odesílá je do sítě v obrovském množství až přes 500 tisíc paketů za minutu, čímž přeplní CAM tabulku switche v naději, že se switch začne chovat jako hub a začne rozesílat příchozí data na všechny své porty.

Při spouštění macof lze nastavit parametry pomocí přepínačů.

-i	interface	Na kterém rozhraní odesílat data
-s	src	Nastavení zdrojové IP adresy
-d	dst	Nastavení cílové IP adresy
-e	tha	Nastavení cílové MAC adresy
-x	sport	Nastavení zdrojového TCP portu
-y	dport	Nastavení cílového TCP portu
-n	times	Počet paketů k odeslání

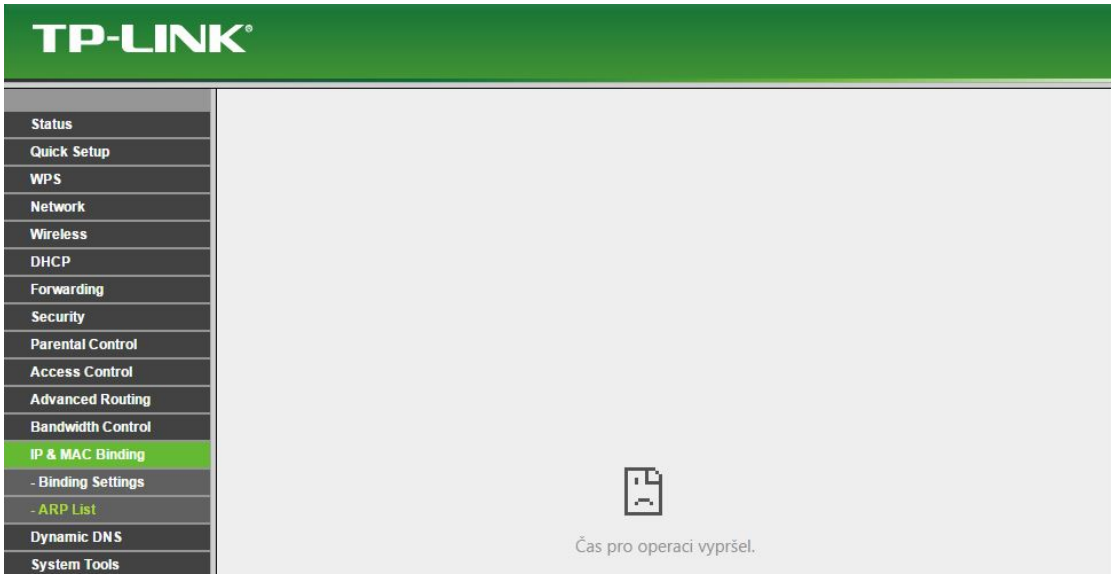
Tabulka 1 Dostupné parametry pro macof

Při pokusu byla použita topologie sítě jako v kapitole 4.2, s vynecháním switche Repotec. První pokus o zaplavení tabulky byl proveden na routeru TP-LINK. Po spuštění macof v terminálu příkazem **sudo macof –i eth0** začne být síť zahlcována pakety. Výstup programu je zachycen na obrázku níže.

```
b5:91:a8:3b:14:b5 67:e1:67:54:ee:b1 8.8.8.8.20953 > 0.0.0.0.58864: S 959813218:959813218(0) win 512
c2:fc:8b:79:3a:93 5f:9b:68:70:cd:1a 8.8.8.8.9263 > 0.0.0.0.37291: S 881594197:881594197(0) win 512
b9:6e:c3:2f:fa:9f 76:c3:1c:63:93:a9 8.8.8.8.26868 > 0.0.0.0.21828: S 846534512:846534512(0) win 512
19:bf:ab:76:9d:9d a6:bb:6c:68:2e:4d 8.8.8.8.28776 > 0.0.0.0.766: S 1358973929:1358973929(0) win 512
2b:e9:ab:6b:da:82 bd:e5:a6:28:10:db 8.8.8.8.41374 > 0.0.0.0.26321: S 1269286989:1269286989(0) win 512
b9:5f:47:2b:a0:25 3a:6f:f6:48:f2:34 8.8.8.8.22571 > 0.0.0.0.56197: S 826129523:826129523(0) win 512
e7:ad:72:13:f5:42 78:6c:c8:4b:ff:4b 8.8.8.8.54749 > 0.0.0.0.59410: S 1208253924:1208253924(0) win 512
41:df:f9:59:e6:48 77:da:4b:3:1b:ad 8.8.8.8.24733 > 0.0.0.0.48888: S 754437879:754437879(0) win 512
7f:7e:9f:5e:a0:5f db:d3:df:19:34:a 8.8.8.8.4956 > 0.0.0.0.16996: S 1588661281:1588661281(0) win 512
5a:6:36:14:18:fb f8:2e:31:16:eb:88 8.8.8.8.34847 > 0.0.0.0.16685: S 1745133677:1745133677(0) win 512
83:7c:87:1a:84:f8 b9:4a:9:7c:e4:57 8.8.8.8.36777 > 0.0.0.0.13735: S 439285838:439285838(0) win 512
29:da:1a:3c:5c:12 26:5d:f:49:9:f8 8.8.8.8.34261 > 0.0.0.0.56773: S 1656362748:1656362748(0) win 512
67:a5:ba:4b:13:3c 5b:39:af:56:9a:48 8.8.8.8.35619 > 0.0.0.0.36292: S 1698593368:1698593368(0) win 512
3f:65:a4:38:bb:a8 53:31:b4:1e:bd:96 8.8.8.8.49292 > 0.0.0.0.56783: S 1173814976:1173814976(0) win 512
3c:f6:ec:76:51:c5 d3:c0:54:0:98:9a 8.8.8.8.54147 > 0.0.0.0.16582: S 1551331113:1551331113(0) win 512
6:5d:96:69:66:29 67:62:46:5a:13:b7 8.8.8.8.63688 > 0.0.0.0.58973: S 2898398543:2898398543(0) win 512
c8:97:78:3a:e6:70 3a:14:b9:1a:d6:99 8.8.8.8.53166 > 0.0.0.0.27181: S 1497351239:1497351239(0) win 512
1d:5:4d:25:7:7b d4:de:4b:38:b7:14 8.8.8.8.56433 > 0.0.0.0.54758: S 1138999885:1138999885(0) win 512
fa:98:69:18:87:c3 b7:86:f1:7c:62:ec 8.8.8.8.11535 > 0.0.0.0.43288: S 1885425878:1885425878(0) win 512
d8:b9:1:68:55:8 a5:63:13:47:35:71 8.8.8.8.39839 > 0.0.0.0.41888: S 1501862631:1501862631(0) win 512
59:be:7e:31:49:5e 15:e7:db:58:4c:f7 8.8.8.8.15896 > 0.0.0.0.3694: S 438436681:438436681(0) win 512
```

Obrázek 13 MAC Flooding- zahlcování sítě pakety

Když byl router zahlcen adresami, namísto odesílání paketů na všechny porty se zhroutil a přestal reagovat.



Obrázek 14 MAC Flooding- zhroucení routeru

Z tohoto důvodu byl pokus proveden i s routerem Mikrotik. O provozu na síti svědčí i zaplněná ARP tabulka na straně oběti. Jelikož switch neměl cílové MAC adresy příchozích dat ve své CAM tabulce, rozeslal data na všechny ostatní porty. Z těchto dat si dotčená ARP tabulka vzala IP a MAC adresy adresáta. Na okamžik se dokonce příchozím datům podařilo z ARP tabulky oběti vytlačit záznam výchozí brány. Na obrázku níže je pouze část obsahu ARP tabulky.

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.35.116 --- 0x12
  Internet Address      Physical Address      Type
  192.168.35.255        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
  224.41.149.82         01-00-5e-29-95-52     static
  224.76.154.38         01-00-5e-4c-9a-26     static
  225.117.161.65        01-00-5e-75-a1-41     static
  226.47.214.122        01-00-5e-2f-d6-7a     static
  227.4.229.34          01-00-5e-04-e5-22     static
  227.40.8.68           01-00-5e-28-08-44     static
  227.88.138.1          01-00-5e-58-8a-01     static
```

Obrázek 15 MAC Flooding- zahlcená ARP tabulka PC

Switch v routeru Mikrotik se po zaplnění CAM tabulky začal pro příchozí data, jejichž cílovou MAC adresu v tabulce neměl, chovat jako hub a rozesílal je na všechny porty kromě příchozího. Toto bylo opět ověřeno pokusem o přihlášení na ftp server.

```
C:\WINDOWS\system32>ftp ftp.debian.org
Connected to ftp.debian.org.
220 ftp.debian.org FTP server
200 Always in UTF8 mode.
User (ftp.debian.org:(none)): edkhf
530 This FTP server is anonymous only.
Login failed.
ftp> quit
221 Goodbye.
```

Obrázek 16 MAC Flooding- přihlášení k FTP serveru

Na straně útočníka byla data po zahlcení tabulky odposlechnuta programem Wireshark. V tabulce ovšem ještě zůstal záznam o MAC adrese oběti, proto je zachycen pouze směr komunikace od oběti k serveru.

Filter: ftp — Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
307030	494.84092906	192.168.35.116	130.89.148.12	FTP	68	Request: OPTS UTF8 ON
317381	496.10945306	192.168.35.116	130.89.148.12	FTP	66	Request: USER edkhf
330137	498.15388706	192.168.35.116	130.89.148.12	FTP	60	Request: QUIT

Obrázek 17 MAC Flooding- odposlech přihlášení k FTP serveru

4.4 DNS Spoofing

Cílem tohoto útoku bylo přesměrování celého síťového provozu nebo jeho části na libovolnou adresu. K provedení útoku byl použit program Ettercap a ke sledování síťové komunikace program Wireshark.

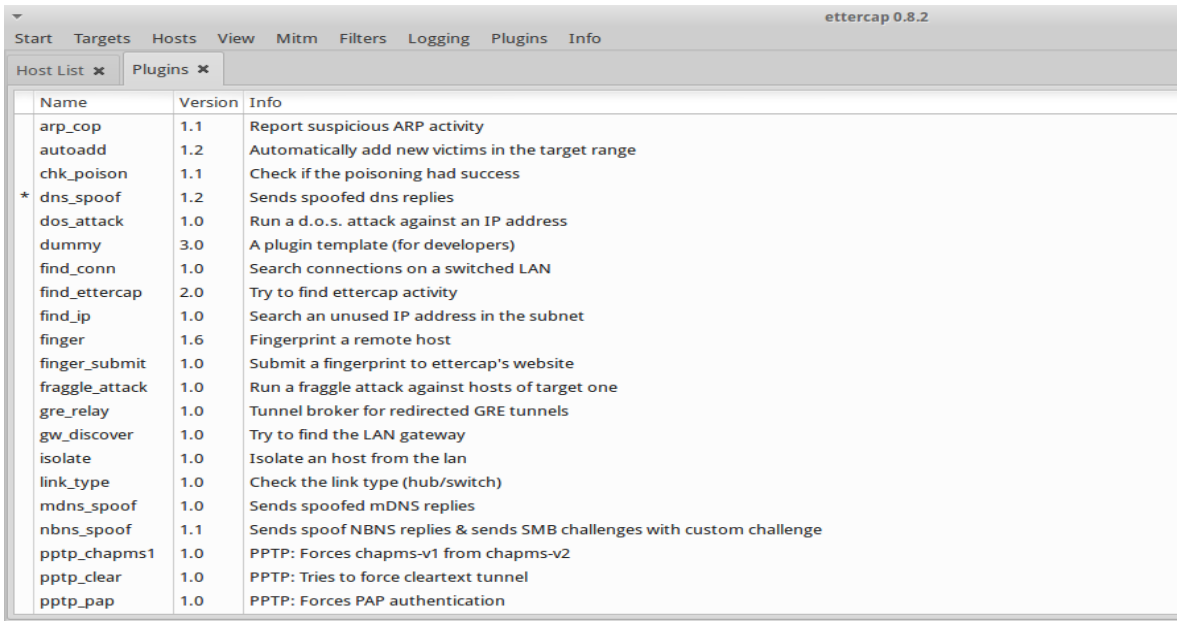
Prvním krokem je otrávení ARP tabulek oběti a výchozí brány. Tato technika byla vysvětlena v kapitole 4.2. Když je komunikace přesměrována k útočníkovi, lze začít s podvržením DNS response paketů. Nejprve je třeba upravit soubor etter.dns, ve kterém jsou uloženy seznamy přiřazení IP adres k doménovým jménům, která mají být podvržena. Tento soubor je k dispozici pro Windows ve složce s instalací programu, v podsložce Share. V linuxových systémech je dostupný v adresáři /usr/share/ettercap/ . Záznam v souboru říká pluginu dns_spoof v programu Ettercap, aby pokud přijde dotaz na IP adresu doménových

jmen microsoft.com nebo všech končících .microsoft.com, odeslal DNS odpověď s IP adresou 147.251.43.48.

```
microsoft.com      A   147.251.43.48
*.microsoft.com    A   147.251.43.48
www.microsoft.com  PTR 147.251.43.48
```

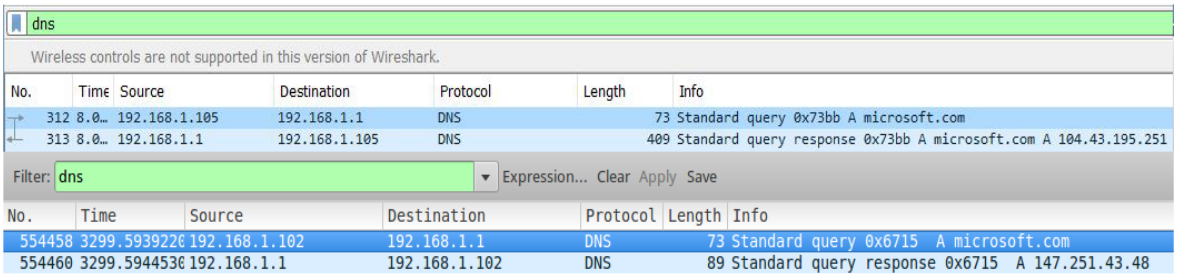
Obrázek 18 DNS Spoofing- podvržené domény

Po uložení upraveného souboru etter.dns je nutno ještě v záložce plugins spustit plugin dns_spoof.



Obrázek 19 Ettercap- pluginy

Na obrázku níže jsou vidět DNS query a response pakety na microsoft.com před a po DNS spoofingu.



Obrázek 20 DNS Spoofing- DNS pakety před a po

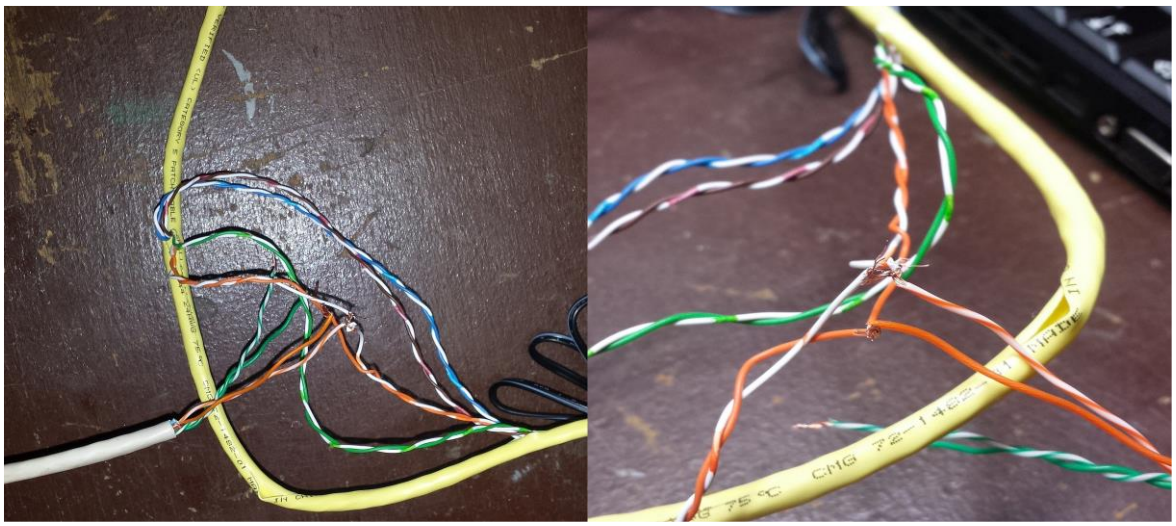
Uživateli, který by nyní chtěl otevřít webovou stránku www.microsoft.com, se tedy zobrazí toto:

Obrázek 21 DNS Spoofing- podvrh stránky www.microsoft.com

4.5 Paralelní připojení k lince

Pokud má útočník přístup k metalickému vedení od jeho oběti, je možné připojit se paralelně k síťovému kabelu a odposlouchávat pasivně bez nutnosti softwarového nabourání do sítě. Každá síťová karta nebo síťové zařízení připojující se pomocí kroucené dvoulinky má ve svém konektoru dva piny vysílající (Tx) a dva piny přijímací (Rx). (17) Tyto piny jsou na dvou sousedních zařízeních vzájemně propojeny, aby mohlo jedno zařízení přijímat, co druhé vysílá. A právě na tyto dva páry vedoucí mezi zařízeními lze paketový sniffer paralelně připojit. Jediným omezením je možnost sledovat na jedné síťové kartě pouze jeden směr konverzace, protože útočníkova karta má také pouze jeden přijímací pár. Pokud by se útočník pokusil připojit svůj přijímací pár na oba směry konverzace zároveň, došlo by ke zkratování vedení. Řešením je odposlech pomocí dvou síťových karet najednou, kdy každá zachytává jeden směr konverzace.

Prvním krokem je rozříznutí ochrany párů a oholení vodičů, ke kterým se chceme připojit. Poté stačí připojit svůj síťový kabel.



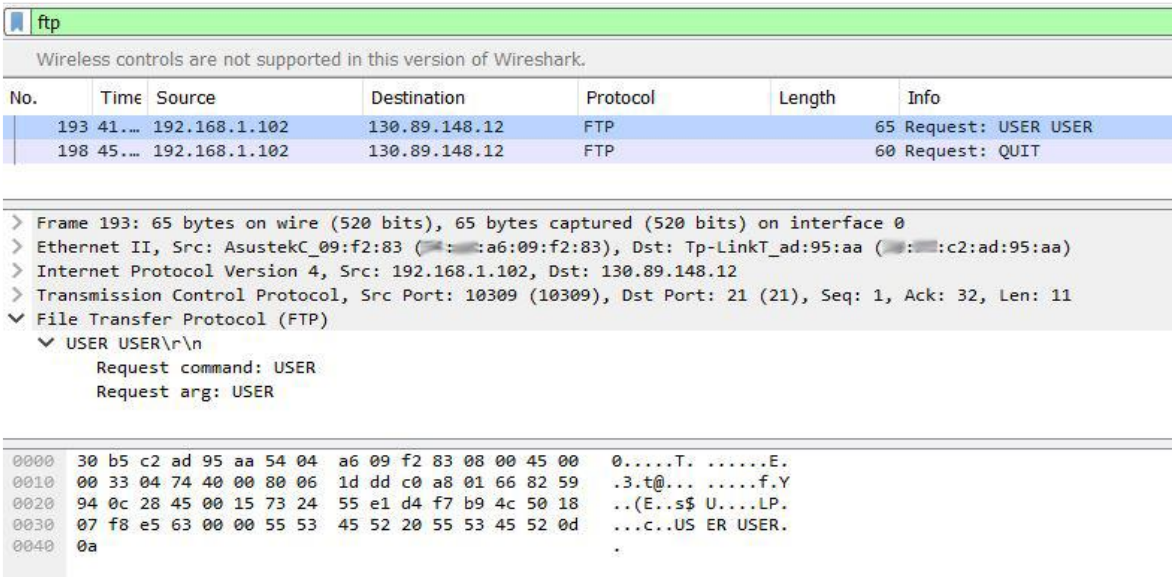
Obrázek 22 Paralelní připojení- detail připojení

Funkčnost připojení byla ověřena zkouškou připojení na ftp server Debian.

```
C:\Users\PC>ftp ftp.debian.org
Systém je připojen k ftp.debian.org.
220 ftp.debian.org FTP server
Uživatel (ftp.debian.org:(none)): USER
530 This FTP server is anonymous only.
Přihlášení se nezdařilo.
ftp> quit
221 Goodbye.
```

Obrázek 23 Paralelní připojení- přihlášení k FTP serveru

Programem Wireshark se podařilo odposlechnout tento neúspěšný pokus o přihlášení. V seznamu zachycených paketů je samozřejmě vidět pouze jedna strana konverzace, v tomto případě kdy je cílovým zařízením ftp server.



Obrázek 24 Paralelní připojení- odposlech přihlášení k FTP serveru

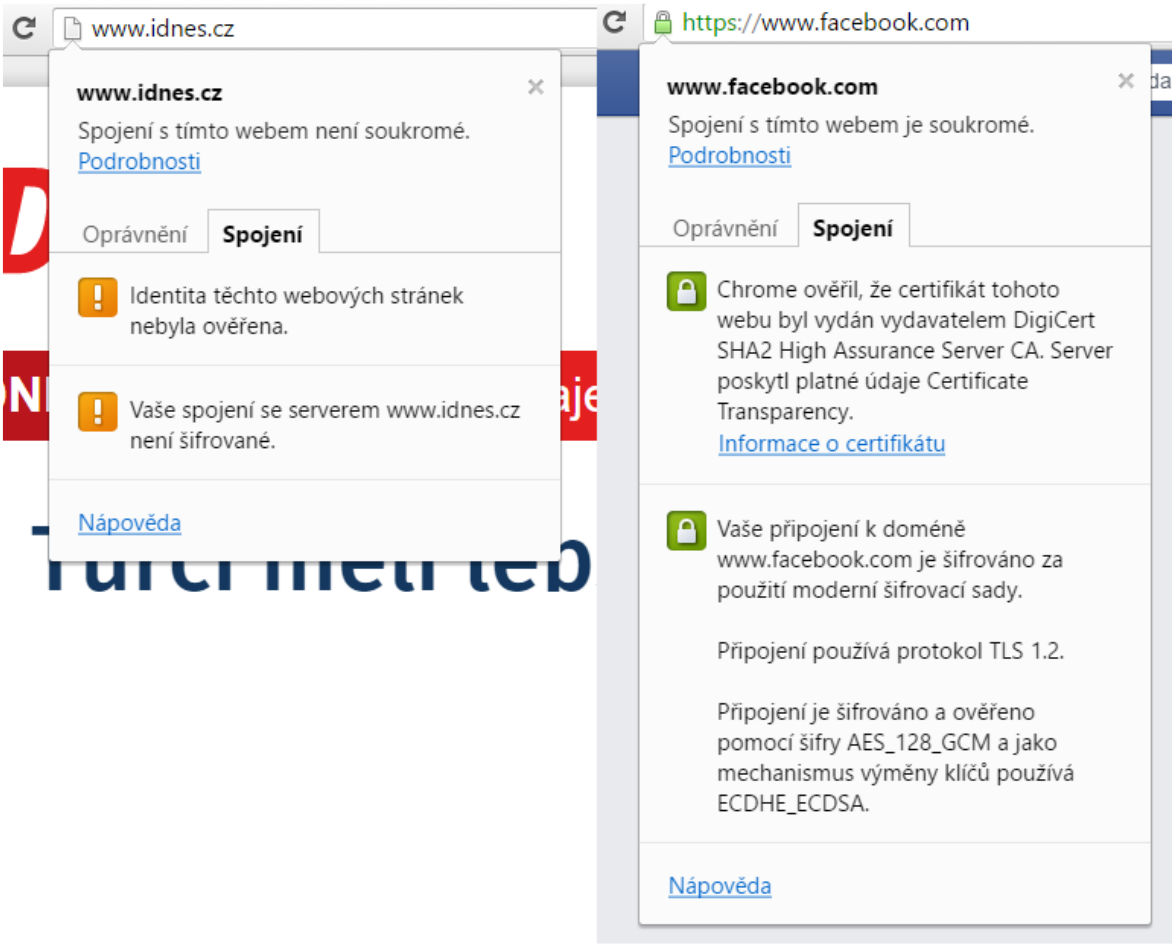
Tento způsob odposlechu síťové komunikace vyžaduje sice fyzický přístup k médiu mezi dvěma body sítě, ale je prakticky neodhalitelný, protože útočník nevysílá do sítě žádné pakety, tudíž je absolutně pasivní. Útočník sice dostane od systému automaticky přidělenou IP adresu po zapnutí rozhraní, ale pro ostatní klienty sítě není dostupný.

```
C:\Users\PC>ping 169.254.24.245

Příkaz PING na 169.254.24.245 – 32 bajtů dat:
PING: Odeslání se nezdařilo. General failure.
PING: Odeslání se nezdařilo. General failure.
PING: Odeslání se nezdařilo. General failure.
PING: Odeslání se nezdařilo. General failure.

Statistika ping pro 169.254.24.245:
Pakety: Odeslané = 4, Přijaté = 0, Ztracené = 4 (ztráta 100%),
```

Obrázek 25 Paralelní připojení- ping na útočníka

4.6 Protokoly HTTP a HTTPS

Protokol HTTPS je nadstavbou síťového protokolu HTTP, přičemž je jeho hlavním účelem zabezpečení komunikace. Přenášená data jsou šifrována pomocí protokolu SSL nebo TLS, které využívají asymetrické šifrování. K vybudování důvěrného spojení mezi klientem a serverem a zároveň k zašifrování přenášených dat slouží certifikát vydaný certifikační autoritou a veřejný klíč. Použití certifikátů také umožňuje ověření, zda stránky, ke kterým se prohlížeč připojil, jsou těmi, za které se vydává. Některé služby implicitně zabezpečené spojení nevyužívají. Je tedy dobré si u webových služeb pracujících s citlivými daty zkontrolovat, zda je použito HTTPS. Jako příklad lze uvést službu Facebook, kde je možné použití HTTPS vynutit. Že je provozované spojení zabezpečené lze poznat v adresním řádku prohlížeče.

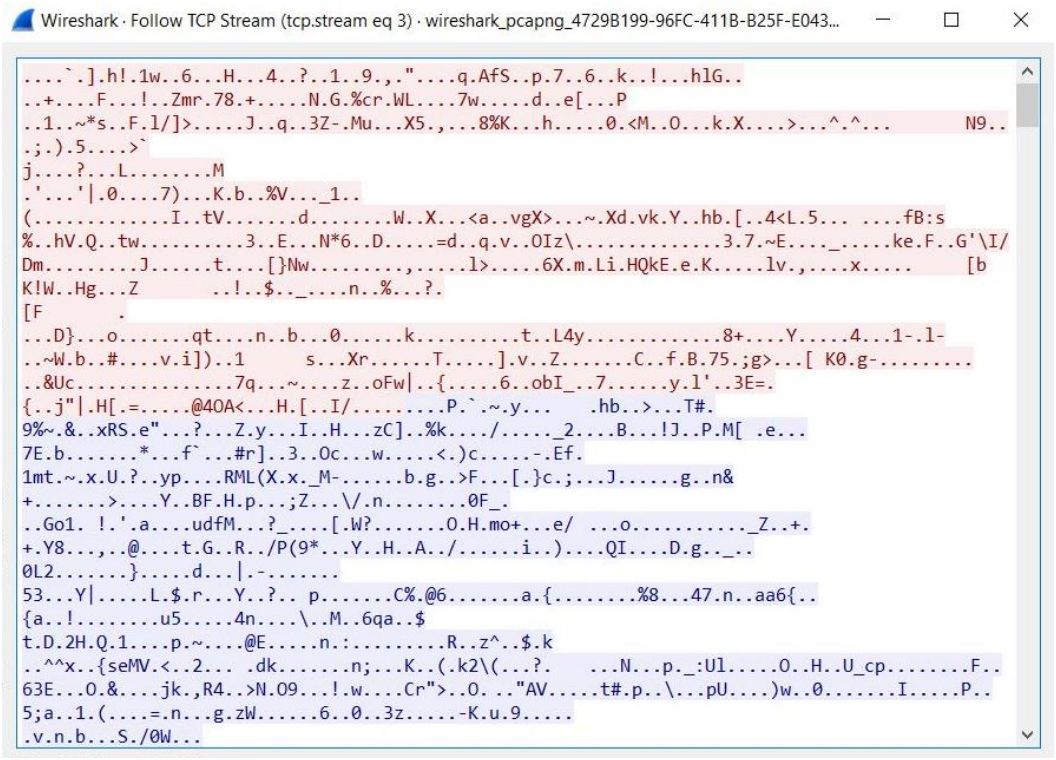


Obrázek 26 HTTP vs. HTTPS v prohlížeči

Zabezpečení šifrováním lze ukázat také analýzou paketů programem Wireshark. Na obrázku níže je zobrazen TCP stream připojení k nezabezpečenému serveru idnes.cz. Z těchto dat lze vyčíst cílový server a další podrobnosti o připojení.

Obrázek 27 HTTP- TCP stream

Naopak zachycená šifrovaná komunikace nedává jakékoliv informace o spojení. Zašifrovaná data nedávají žádný smysl a jsou bez šifrovacího klíče bezcenná.

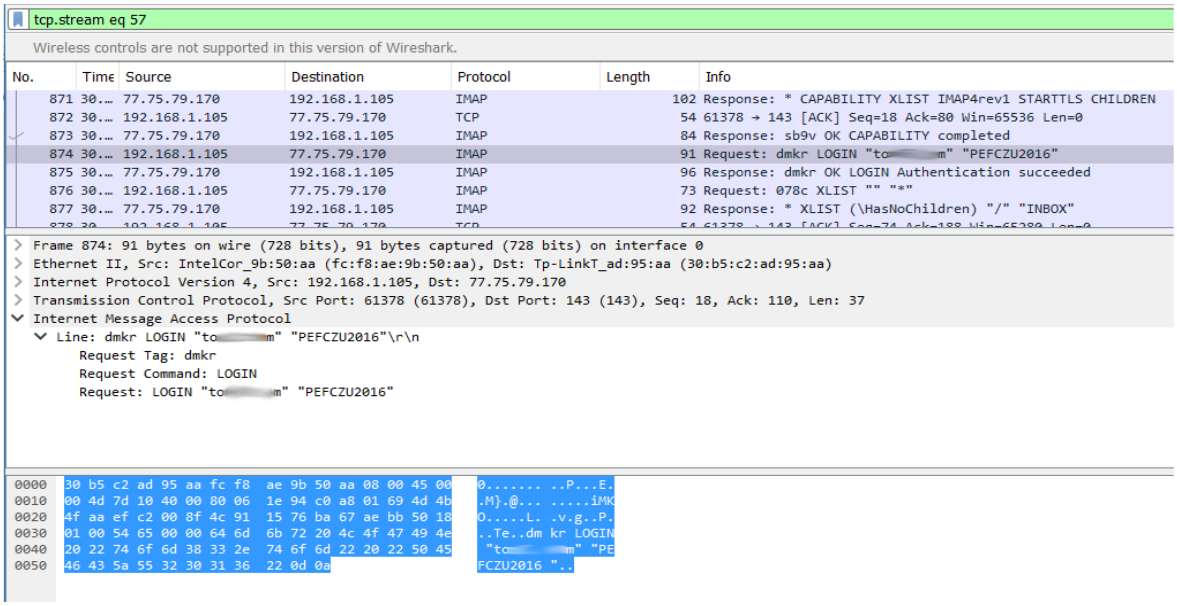


Obrázek 28 HTTPS- TCP stream

4.7 Odposlech IMAP

Poštovní schránka může obsahovat velmi citlivé uživatelské údaje. Proto je třeba používat při spojení emailového klienta se serverem zabezpečené připojení. Protokol IMAP slouží k práci se vzdálenou poštovní schránkou. Jelikož se o jeho konfiguraci stará uživatel, je třeba dát si pozor, aby byl použit šiforvaný IMAP pracující na portu 993. Například v prohlížeči pošty Outlook je jako výchozí nastaveno nešifrované spojení a aplikace uživatele na tuto možnost ani neupozorní.

V následujícím pokusu byly odposlechnuty přihlašovací údaje k emailové schránce za použití klienta pracujícího s nešifrovaným protokolem IMAP, pracujícím na portu 143. K emailové schránce umístěné na serveru seznam.cz bylo dočasně nastaveno heslo PEFCZU2016. Už z obsahu IMAP Request paketu jsou jasně vidět nezašifrované přihlašovací údaje.



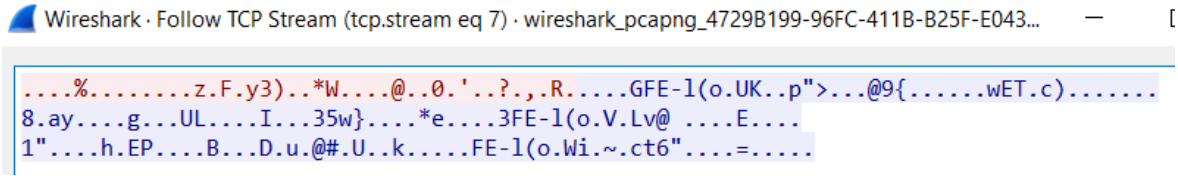
Obrázek 29 Odposlech IMAP- pakety bez šifrování

Navíc po rozkliknutí celého TCP streamu jsou jednoduše dostupné i samotné emailové zprávy.

```
Date: Fri, 11 Mar 2016 10:55:38 +0100
Message-ID: <CAD5OTFX3TNgA-COnO9zEysSNNv=K-HB9P8hppaRPgXDJV0V2EA@mail.gmail.com>
Subject: Fwd: Nesifrovany email
From: =?UTF-8?B?VG9tw6HFoSBGacWhZXI=?= <to @ ces.cz>
To: to m@seznam.cz
Content-Type: multipart/alternative; boundary=001a1141c87eecdc5a052dc2ee70

--001a1141c87eecdc5a052dc2ee70
Content-Type: text/plain; charset=UTF-8

Jsem nesifrovany email a kdokoliv me muze odposlechnout.

--001a1141c87eecdc5a052dc2ee70
Content-Type: text/html; charset=UTF-8

<div dir="ltr"><div class="gmail_quote"><div dir="ltr"><span style="font-size:12.8px">Jsem
nesifrovany email a kdokoliv me muze odposlechnout.</span><br></div>
</div><br></div>
```

Obrázek 30 Odposlech IMAP- obsah zprávy bez šifrování

Po změně spojení na šifrovaný protokol IMAP na portu 993 se stává komunikace pro útočníka nečitelnou.



Obrázek 31 Odposlech IMAP- obsah komunikace se šifrováním

4.8 Sledování manipulace s ARP Cache

Pro monitorování ARP tabulky byl použit program arpwatch. Tento jednoduchý nástroj sleduje změny IP a MAC adres v místní síti. Záznamy mají časové razítko, takže lze podle nich sledovat aktivitu na místní síti. Program umí zobrazovat data čtyřmi způsoby. Data mohou být vypisována přímo na systémovou konzoli, ukládána do souboru se systémovými logy nebo do uživatelem specifikovaného souboru nebo mohou být odesílána emailem. Program arpwatch je určen pouze pro linuxové distribuce a není obsažen v základních balících. Nainstalovat ho lze příkazem **$ sudo apt-get install arpwatch**. Jako jeho alternativa pro Windows může sloužit například program ArpCacheWatch.

Při pokusu o sledování změn ARP tabulky bylo využito odesílání hlášení o změně na email. Po spuštění programu stačí zadat příkaz, který nastaví odesílání emailů.

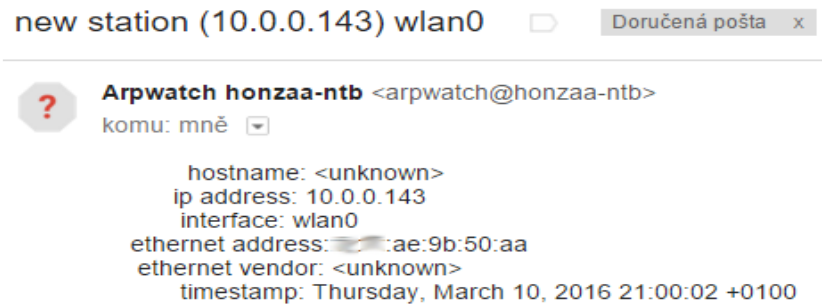
OPTIONS="-u arpwatch -e email@domena.com -s 'root (Arpwatch)'"

-u – uživatelské jméno

-e – email adresáta

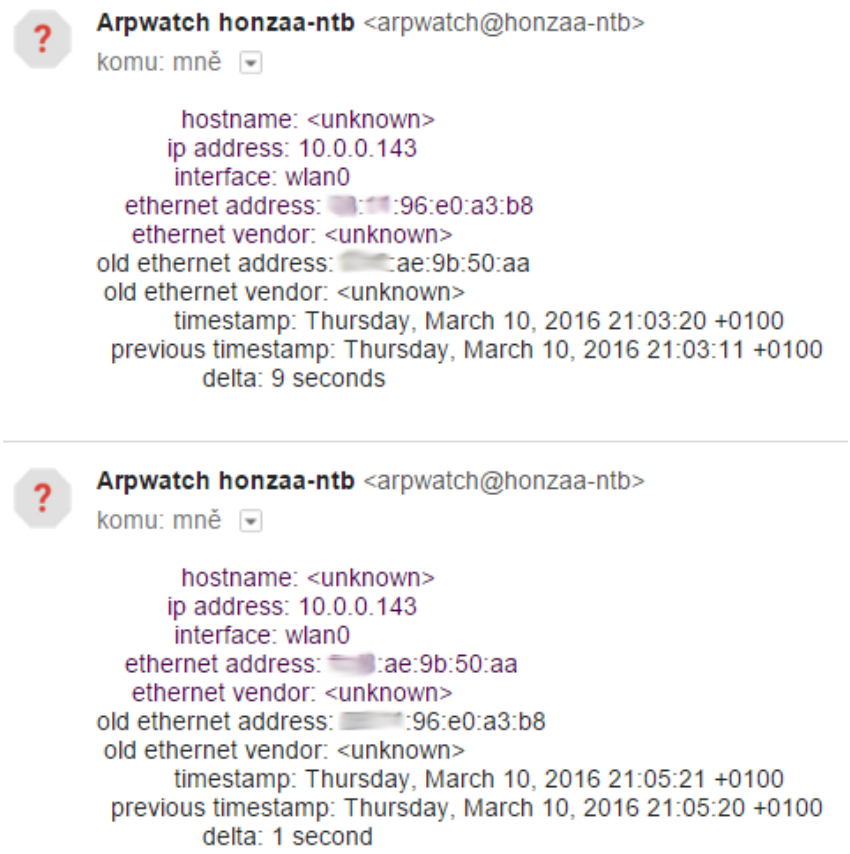
-s – email odesílatele

Pokud se nyní do sítě připojí nový účastník, čímž se jeho adresa dostane do sledované ARP tabulky, přijde administrátorovi následující email.



Obrázek 32 arpwatch- upozornění na nový záznam

Pokud dojde ke změně MAC adresy u již zapsané IP adresy, dostane o tom administrátor také zprávu, ve které je popsána i změna adres včetně časového úseku od poslední změny.



Obrázek 33 arpwatch- upozornění na změny záznamů

V případě takto rychlých změn se dá předpokládat, že na síti dochází k ARP poisoningu, což také v tomto případě došlo. Tento program by se dal využít i k detekci zahlcování MAC adresami. Pokud začne do sítě najednou přibývat velké množství nových záznamů, je jasné, že je síť pod útokem hackera.

5 Zhodnocení výsledků

V práci byly provedeny čtyři druhy útoků s cílem odposlechu komunikace procházející sítí. Kromě zahlcování MAC adresami routeru TP-LINK, který tak velký nápor nevydržel a zhroutil se, proběhly všechny útoky úspěšně. Každý z těchto čtyř útoků používá jiný princip dosažení dat

ARP Cache poisoning využívá absence zabezpečení ARP protokolu. Nevyžádanými reply pakety přesvědčí svou oběť o své falešné identitě, takže se stává prostředníkem komunikace, kterou přeposílá dále. Oběť tedy dostane data, o která si žádala a o jejich odposlechu nemá tušení. V praxi veškeré tyto úkony zastane program Ettercap, který v sobě obsahuje funkci ARP Cache poisoning. Router TP-LINK v sobě neobsahuje žádnou ochranu proti této technice. Router Mikrotik také ne, ale v jeho případě by nejspíš bylo možno ochranu doplnit úpravou softwaru.

V případě použití techniky MAC Flooding spoléhá útočník na změnu chování switche po zaplnění jeho CAM tabulky, což se praktickým pokusem potvrdilo jen zčásti. Útočník vysílá na switch velké množství paketů s náhodně generovanými MAC adresami. Switch si je ukládá do své tabulky, kde má ke každé MAC adrese přiřazený port na kterém je připojena. Útočník spoléhá, že po zaplnění tabulky a přepsání původních adres adresami falešnými začne switch všechny příchozí pakety, které nebude mít ve své tabulce, rozesílat na všechny porty kromě příchozího a chovat se jako HUB. Tento předpoklad se potvrdil u routeru Mikrotik. Ten po zaplnění své CAM tabulky skutečně rozesílal pakety oběti i k útočníkovi. Router TP-LINK tak velký nápor nevydržel a po zaplnění své tabulky se zhroutil. Tento způsob je poměrně zdlouhavější a s nejistým výsledkem. Předpokladem je vypršení životnosti záznamů zařízení v sítí a jejich nahrazení falešnými záznamy, což může trvat od minut i po hodiny.

Třetí vyzkoušenou technikou byl DNS Spoofing. Ten se od předchozích technik liší tím, že vlastně nejde o odposlech jako takový. Útočník přesměrovává DNS požadavky o překlad doménového jména nejčastěji technikou ARP poisoning a své oběti odesílá zfalšované odpovědi. Oběť se pak připojuje například na zfalšované webové stránky, do kterých zadává přihlašovací údaje, aniž by byly šifrovány a tyto údaje putují k útočníkovi. Tento druh útoku byl úspěšně vyzkoušen za pomoci programu Ettercap, který disponuje

rozšířením pro tento druh útoku. Podařilo se nastavit překlad doménového jména microsoft.com na IP adresu serveru linux.cz.

Posledním prakticky vyzkoušeným útokem bylo paralelní připojení k lince. Při tomto útoku není potřeba přístup do místní sítě, ale pouze fyzický přístup k síťovému kabelu mezi útočníkem a výchozí bránou. Poté stačí připojit na jeden z komunikačních párů (zelený- zelenobílý, oranžový- oranžovobílý) paralelně svůj přijímací pár vodičů. Tím je k útočníkovi doručován jeden směr komunikace. Pokud by chtěl odposlouchávat oba směry, musel by odposlouchávat pomocí dvou síťových karet, na každé jeden směr. Jelikož při tomto druhu připojení útočník nevysílá žádná data do sítě, je pro síť prakticky neviditelným.

Dále byla demonstrována efektivita šifrování komunikace, které je jedním z prvků obrany proti odposlechu. Prvním pokusem bylo ukázání rozdílů protokolů HTTP a HTTPS. Pomocí programu Wireshark byla odposlechnuta nešifrovaná komunikace se serverem idnes.cz a šifrovaná komunikace se serverem facebook.com, který používá šifrování pomocí protokolu TLS. Tato data byla porovnána a bylo poukázáno na nulový přínos odposlechu pro útočníka v případě šifrovaného spojení.

Druhou ukázkou využití šifrování byl odposlech emailové komunikace pomocí protokolu IMAP. Ten disponuje verzí bez šifrování pracující na portu 143 a se šifrováním využívající port 993. V aplikaci Wireshark byla úspěšně odposlechnuta komunikace mezi emailovým klientem Outlook 2013, který ve výchozím nastavení pracuje s nešifrovaným protokolem, a emailovým serverem seznam.cz. Na datech byly analýzou paketů a celého TCP toku ukázány přihlašovací údaje k emailové schránce a obsah emailové zprávy. Po nastavení šifrovaného protokolu IMAP byl odposlech proveden znovu a bylo poukázáno na bezcennost zachycených dat.

Monitorování změn ARP tabulky s cílem detekce její manipulace bylo provedeno v poslední kapitole praktické části práce. Použit k tomu byl program arpwatch, dostupný pro linuxové distribuce. Tento program sleduje příchozí ARP reply pakety a upozorňuje administrátora na nová zařízení v síti a veškeré změny adres v ARP tabulce. Při pokusu bylo využito funkce odesílání zpráv emailem. Na lince byl poté proveden ARP poisoning, což bylo demonstrováno příchozími emaily o změnách adres. Toto sledování ARP tabulky je účinnou detekcí proti otrávení ARP tabulky i zahlcení sítě falešnými MAC adresami.

6 Závěr

Programů a aplikací pro sledování nebo narušení síťového provozu je k dispozici už vcelku dost. Namátkou lze jmenovat programy dsniff, arpspoof, Cain and Abel, Kismet, tcpdump, ngrep a další. Většina z nich je ovšem omezena jen na určité druhy útoků a také jsou nejčastěji funkční pouze v Unixových systémech. Z tohoto důvodu byly v práci použity převážně programy Wireshark a Ettercap. Oba dva programy fungují jak na Unixu, tak i Windows a OS X. Také jsou oba stále ve vývoji a tedy pravidelně aktualizované a rozšiřované o podporu dalších protokolů nebo typů útoků.

Cílem práce bylo zmapovat metody odposlechu síťové komunikace a demonstrovat jejich použití. Ve třetí kapitole práce jsou popsány principy těchto metod a možnosti obrany proti nim. Na přepínaných sítích je hlavním cílem útočníka přimět switch, aby mu odeslal i komunikaci pro něho neurčenou. Nejčastějším způsobem jsou takzvané Man in the middle útoky, které spoléhají na záměnu identity útočníka za oběť, případně výchozí bránu.

Praktická část práce (kapitola „Vlastní zpracování“) je věnována ukázkám samotných postupů odposlechu a demonstraci jejich účinku na odposlouchávaná zařízení. Pomocí programu Wireshark byl pozorován průchod paketů sítí a změny v jejich směrování. Pokusy o odposlech probíhaly na zařízení TP-LINK TL-WR841N, jež je jedním z nejdostupnějších routerů na trhu a na routeru Mikrotik RB2011, vhodném pro použití v menších firmách. U routeru TP-LINK není obrana proti takovýmto útokům prakticky žádná. U routeru Mikrotik záleží na technické zdatnosti administrátora. Systémy pro detekci a obranu před tímto druhem útoků lze zlepšit změnou softwaru zařízení.

Je třeba upozornit na fakt, že neoprávněný odposlech síťové komunikace je trestnou činností dle Zákona č. 40/2009 Sb., trestního zákoníku, § 182 Porušení tajemství dopravovaných zpráv. Horní trestní sazba jsou dva roky odnětí svobody, vy výjimečném případě až 5 let. Proto probíhal veškerý odposlech a pokusy o narušení bezpečnosti sítě na vlastní místní síti, která byla zřízena pouze za účelem použití k této práci.

7 Seznam použitých zdrojů

1. **Zendulka, J.** Počet prodaných smartphonů loni poprvé překonal 1 miliardu, Samsung upevnil vedení. *KurzyCZ.* [Online] 1. 2 2014. [Citace: 8. 3 2016.] http://www.kurzy.cz/zpravy/361626-pocet-prodanych-smartphonu-loni-poprve-prekonal-1-miliardu-samsung-upevnil-vedeni/.

2. **Sosinsky, Barrie.** *Mistrovství- počítačové sítě.* 1. Brno : Computer Press, 2010. str. 840. 978-80-251-3363-7.

3. **Eisinger, Pavel.** Moderní bezdrátové sítě IEEE 802.11n, WiMAX. *ped.muni.cz.* [Online] [Citace: 10. 3 2016.] http://www.ped.muni.cz/wtech/03_studium/teps/stud/moderni_bezdratove_site.pdf.

4. **Rouse, Margaret.** routing table. *SearchNetworking.* [Online] 1. 4 2007. [Citace: 9. 3 2016.] http://searchnetworking.techtarget.com/definition/routing-table.

5. **Doyle, Jeff.** Dynamic Routing Protocols. *ciscopress.com.* [Online] 16. 11 2001. [Citace: 9. 3 2016.] http://www.ciscopress.com/articles/article.asp?p=24090.

6. Zákon č. 40/2009 Sb. [Online] 8. 1 2009. [Citace: 28. 2 2016.] www.mvcr.cz/soubor/sb011-09-pdf.aspx.

7. Sanai, Daiji. Detection od Promiscuous Nodes Using ARP Packets. [Online] 01 8 2001. https://www.ihatefeds.com/promiscious.pdf.

8. Himanshu, Arora. TCP/IP Attacks – ARP Cache Poisoning Fundamentals Explained. *The Geek Stuff.* [Online] 13. 1 2012. [Citace: 29. 1 2016.] http://www.thegeekstuff.com/2012/01/arp-cache-poisoning/.

9. Haller, Martin. Odposlouchávame data na přepínaném Ethernetu (2.). *Lupa.cz.* [Online] 20. 6 2006. [Citace: 29. 1 2016.] http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-2/#ic=serial-box&icc=text-title.

10. Popeskic, Valter. MAC Address Flooding – MAC address table overflow attacks. *How does internet work.* [Online] 14. 12 2011. [Citace: 14. 2 2016.] http://howdoesinternetwork.com/2011/mac-address-flooding.

11. CZ.NIC. O DOMÉNÁCH A DNS. *CZ.NIC Správce domény CZ.* [Online] 2016. https://www.nic.cz/page/312/o-domenach-a-dns/.

12. Sanders, Chris. Understanding Man-In-The-Middle Attacks – Part2: DNS Spoofing. *WindowSecurity.com.* [Online] 7. 4 2010. [Citace: 5. 3 2016.] http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part2.html.

13. CZ.NIC. JAK FUNGUJE DNSSEC. *CZ.NIC, Správce domény CZ.* [Online] 2016. [Citace: 6. 3 2016.] http://www.dnssec.cz/page/444/jak-funguje-dnssec/.

14. Šifrování. *Jak na internet.* [Online] 2014. [Citace: 10. 3 2016.] http://www.jaknainternet.cz/page/1251/sifrovani/.

15. Harper, Allen, a další. *Hacking - manuál hackera.* Praha : Grada, 2008. 978-80-247-1346-5.

16. Sanders, Chris. *Analýza sítí a řešení problémů v programu Wireshark.* Brno : Computer Press, 2012. 978-80-251-3718-5.

17. Ethernet crossover cable. *Wikipedia.* [Online] 25. 2 2016. [Citace: 5. 3 2016.] https://en.wikipedia.org/wiki/Ethernet_crossover_cable.

Seznam obrázků

Obrázek 1:Packet switching, zdroj: http://www.allsyllabus.com/aj/note/Computer_Science/Computer%20Networks%20-%20II/Unit1/Datagram%20or%20Connectionless%20Packet%20Switching1.PNG 11
Obrázek 2: Funkce ARP, zdroj: http://networkbasicknowhow.blogspot.cz/2013/05/ip-network-addresses-and-masks.html 21
Obrázek 3: ARP Cache poisoning, zdroj: http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-2/#ic=serial-box&icc=text-title 22
Obrázek 4 Wireshark- pravidla barvení záznamů, zdroj: vlastní 28
Obrázek 5 Wireshark- ukázka zachycených HTPP paketů, zdroj: vlastní 29
Obrázek 6 Wireshark- funkce Follow TCP Stream, zdroj: vlastní 30
Obrázek 7 Skenování podsítě, zdroj: vlastní 31
Obrázek 8 Topologie ARP Cache poisoning, zdroj: vlastní 31
Obrázek 9 Ettercap- výběr cílů, zdroj: vlastní 32
Obrázek 10 Ettercap- spuštění otravy ARP tabulky, zdroj: vlastní 32
Obrázek 11 ARP poisoning- přeposílání paketů útočníkem, zdroj: vlastní 33
Obrázek 12 ARP poisoning- ARP tabulka oběti, zdroj: vlastní 33
Obrázek 13 MAC Flooding- zahlcování sítě pakety, zdroj: vlastní 34
Obrázek 14 MAC Flooding- zhroucení routeru, zdroj: vlastní 35
Obrázek 15 MAC Flooding- zahlcená ARP tabulka PC, zdroj: vlastní 35
Obrázek 16 MAC Flooding- přihlášení k FTP serveru, zdroj: vlastní 36
Obrázek 17 MAC Flooding- odposlech přihlášení k FTP serveru, zdroj: vlastní 36
Obrázek 18 DNS Spoofing- podvržené domény, zdroj: vlastní 37
Obrázek 19 Ettercap- pluginy, zdroj: vlastní 37
Obrázek 20 DNS Spoofing- DNS pakety před a po, zdroj: vlastní 37
Obrázek 21 DNS Spoofing- podvrh stránky www.microsoft.com, zdroj: vlastní 38
Obrázek 22 Paralelní připojení- detail připojení, zdroj: vlastní 38
Obrázek 23 Paralelní připojení- přihlášení k FTP serveru, zdroj: vlastní 39
Obrázek 24 Paralelní připojení- odposlech přihlášení k FTP serveru, zdroj: vlastní 39
Obrázek 25 Paralelní připojení- ping na útočníka, zdroj: vlastní 39
Obrázek 26 HTTP vs. HTTPS v prohlížeči, zdroj: vlastní 40
Obrázek 27 HTTP- TCP stream, zdroj: vlastní 41

Obrázek 28 HTTPS- TCP stream, zdroj: vlastní 42
Obrázek 29 Odposlech IMAP- pakety bez šifrování, zdroj: vlastní 43
Obrázek 30 Odposlech IMAP- obsah zprávy bez šifrování, zdroj: vlastní..... 43
Obrázek 31 Odposlech IMAP- obsah komunikace se šifrováním, zdroj: vlastní 43
Obrázek 32 arpwatch- upozornění na nový záznam, zdroj: vlastní 44
Obrázek 33 arpwatch- upozornění na změny záznamů, zdroj: vlastní 45

Seznam tabulek

Tabulka 1 Dostupné parametry pro macof, Zdroj:
http://www.irongeek.com/i.php?page=backtrack-3-man/macof 34