Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Teze bakalářské práce

Odposlech síťové komunikace

Tomáš Fišer

Odposlech síťové komunikace

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.

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

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.

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.

Průběh řešení

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.

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.

Seznam použitých zdrojů

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

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

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

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

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.

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

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