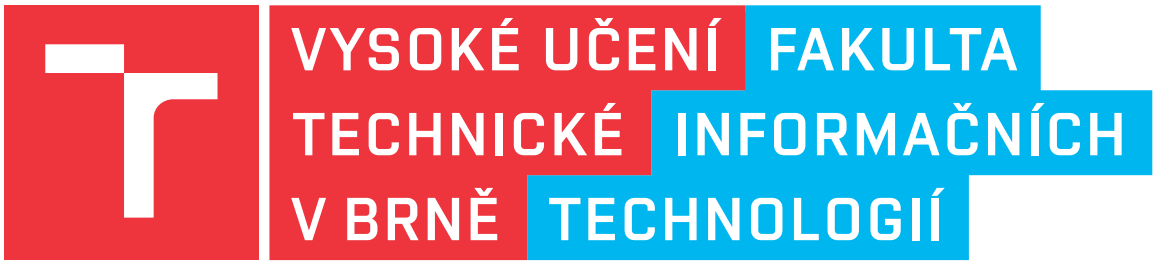


Dokumentace projektu do předmětu PDS

Man-in-the-Middle Attack

Jakub Stejskal (xstejs24@stud.fit.vutbr.cz)
23. dubna 2017

1 Úvod

Hlavním cílem projektu je implementace tří aplikací, které společně umožňují realizovat Man-in-the-Middle útok v lokální síti. K provedení útoku je nutné znát topologii sítě, respektivě IP a MAC adresy obětí,jejichž provoz chceme odposlouchávat. K tomu slouží program **pds-scanner**, která dokáže zmapovat lokální síť pomocí protokolů *ARP* pro IPv4 a *NDP* pro IPv6.

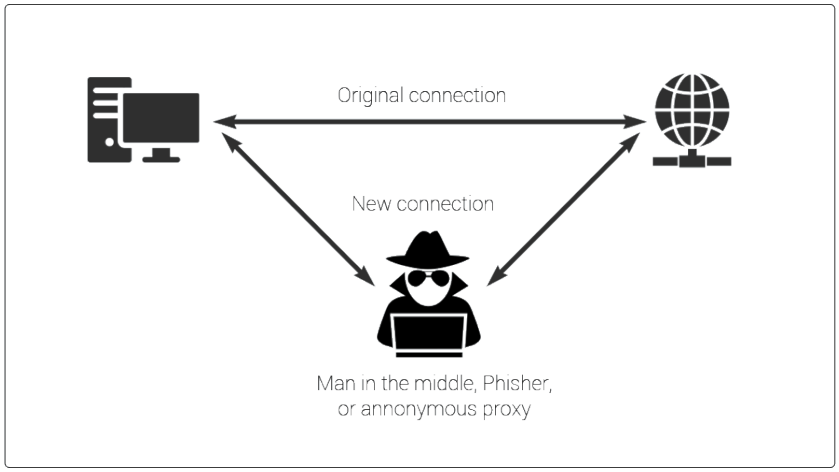
Aby bylo možné komunikaci odchytit, je nutné upravit ARP a NDP tabulky tak, aby si oběť myslela, že náš stroj je stanice, se kterou chce komunikovat. K tomu slouží program **prd-spoof**, která na základě adres vybraných obětí otráví obětem ARP/NDP cache.

Posledním střípkem skládačky je program**pds-intercept**, který odchytává komunikaci v síti a přeposílá provoz tak, aby vytvořil iluzi pro obě oběti, že se nic neděje. Oběti spolu mohou bez problému komunikovat aniž by tušili, že jejich komunikace je posílána přes prostředníka.

2 Rozbor MitM

Man in the Middle [1] je typ útoku, kdy na dva uživatele zaútočí třetí subjekt, který naruší jejich ARP/NDP tabulky a upraví je tak, aby si jeho oběti mysleli, že právě on je tím, s kým chtějí komunikovat. Komunikace pak není posílána v sítí přímo mezi stanicemi, ale všechno je směrováno přes útočníka, který následně provoz posílá druhé oběti.

Ukázku běhu komunikace před a během útoku můžeme vidět na obrázku číslo 1.



Obrázek 1: Obrázek demonstrující MitM.

3 Skenování sítě

Při skenování sítě je nutné si uvědomit, že naše oběti mohou být připojení pomocí více standardů protokolu IP. Je tedy nutné skenovat na přítomnost zařízení s adresou *verze 4* a také s adresou *verze 6*. Jelikož tyto standardy jsou od sebe odlišené, je nutné provádět skenování uzpůsobené danému protokolu.

3.1 IPv4 - ARP

Pro oskenování zařízení v síti, které mají přiřazenou adresu IPv4 je možné využít protokol *Address Resolution Protocol - ARP* [3]. Protokol ARP umožňuje získat link-layer adresu (MAC adresu) stanice pomocí její IP adresy. Dotaz pro získání MAC adresy jiné stanice je zaslán na multicastovou MAC adresu privátní sítě (ff:ff:ff:ff:ff:ff) a odesílatel je povinen (mimo jiné) vyplnit následující informace:

- IP adresu odesílatele
- MAC adresu odesílatele
- IP adresu příjemce

Tento dotaz pak dostanou všechny zařízení v síti, ale odpoví na něho pouze to, kterému patří zadaná IP adresa v podobě ARP-Reply paketu se svojí MAC adresou.

Implementovaný postup

Pds-scanner využívá *Brute-force* (hrubou sílu) pro získání IP a MAC adres všech zařízení připojených k síti. Jelikož je útočník sám připojen v síti je možné získat adresu sítě a masku, ze které je možné získat maximální počet připojených hostů. Například pro IP sítě *10.0.0.0* a masku *255.255.255.0* získáme počet hostů 254.

Po získání počtu hostů není těžké dopočítat všechny možné adresy v podsíti a rozeslat dotazy na všechny získané adresy. Pokud je adresa v síti přiřazena nějakému zařízení, toto zařízení útočníkovi rádo zašle svojí MAC adresu. Tento postup je možný pouze v sítích s IP verzí 4, kvůli relativně nízkému počtu připojených hostů.

3.2 IPv6 - NDP

Při vývoji IP verze 6 byl protokol v těchto sítích nahrazen protokolem *Neighbor Discovery Protocol - NDP*[2]. Stejně jako ARP slouží NDP k získávání linkové adresy zařízeních připojených v síti. Protokol NDP obsahuje dva základní druhy zpráv:

- solicitation - slouží k navázání komunikace s druhým zařízením v síti. Zasílá pro získání linkové adresy souseda nebo ke zjištění jeho dostupnosti.
- advertisement - odpověď na NDP solicitation obsahující požadované informace (linkovou adresu).

Implementovaný postup

Postup pro oskenování zařízení připojených pomocí IPv6 byl převzat z aplikace *THC-IPv6-Attack-Toolkit*, která obsahuje skenovací aplikaci *Alive6*. Princip spočívá v zaslání jednoho *ping* paketu a jednoho porušeného paketu na adresu ff02::1 (multicastová adresa lokální sítě).

Ty stanice, které mají povoleno odpovědět, na ping odpoví paketem,ze kterého je možné vyčíst MAC adresu stanice, která ping-reply odeslala. Problém nereagování na ping řeší, již zmíněný porušený paket (malformed). V tomto paketu jsou poškozeny nepovinné hlavičky *hop-by-hop*. Na tento paket stanice odpoví odesílateli, že je něco v nepořádku se zaslanou zprávou (unrecognized IPv6 option), čímž útočník získá zbylé adresy.

V IPv6 sítích není možné provést útok hrubou silou, protože zasílání paketů na všechny možné adresy v lokální síti by bylo časově nevyhovující.

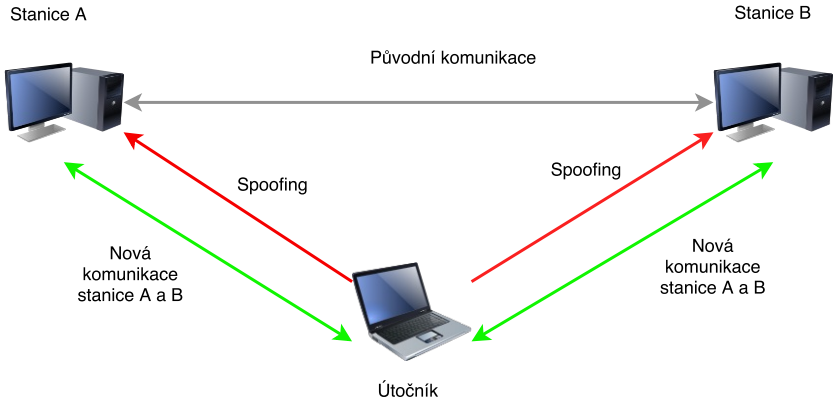
3.3 Výstup

Skenování sítě probíhá tak, že aplikace rozešle potřebné pakety do sítě a následně několik vteřin odposlouchává odpovědi, které zpracovává do stromu. Po uplynutí 10 vteřin je program sám ukončen a vyprodukuje závěrečný výstup.

Výstupem programu **pds-scanner** jsou tedy MAC adresy nalezených stanic, ke kterým jsou přiřazeny jejich IP adresy. Tento seznam zařízení je uložen do souboru formátu XML, který slouží jako vstup pro přesměrování komunikace.

4 Otrávení ARP a NDP cache

Otrávení ARP a NDP cache umožní útočníkovi dostávat komunikaci, která by normálně byla směrována přímo jejímu příjemci. Útočník kontinuálně zasílá upravené pakety svým obětem tak, že spojí svoji MAC adresu s IP adresou jedné z obětí a tuto informaci odešlé druhé oběti. Postup se opět lehce liší pro ARP a NDP protokoly. Obrázek 2 znázorňuje změnu v toku komunikace mezi dvěma obětmi.



Obrázek 2: Obrázek demonstrující změnu cesty pro komunikaci mezi dvěma obětmi.

4.1 ARP spoofing

Pro otrávení ARP cache se využívá takzvaný *gratuitous ARP*[4]. Jedná se o upravený ARP paket, kde obě IP adresy (zdrojová a cílová) jsou nastaveny na IP adresu zdrojové stanice, zdrojová MAC adresa je nastavena na MAC adresu útočníka a cílová MAC adresa obsahuje samé nuly. V ethernetové hlavičce je zdrojová MAC adresa útočníka a cílová MAC adresa oběti.

Oběť si po obdržení takového paketu upraví svou ARP tabulku, kde k IP adrese obsažené v obdrženém paketu přiřadí adresu útočníka.

Zrušení otrávení cache se provede zasláním ARP paketu, kde,jsou všechny údaje stejné jako před útokem.

4.2 NDP spoofing

Otrávení NDP cache[5] spočívá v zasílání *Neighbor advertisement* obětem. Neighbor advertisement je odpověď na paket typu solicitation. Tato odpověď v sobě nese informaci o IP adrese a MAC adrese odesílatele. Stanice, která tento paket obdrží si zapíše výsledky do své NDP tabulky, kde bude mít dvojici IPv6 adresa a MAC adresa.

Útočník v tomto paketu nahradí MAC adresu jedné z obětí za svoji, čímž řekne druhé oběti, že IP adresa, kterou ve skutečnosti vlastní první oběť je spojena s útočníkovou MAC adresou. Veškerá komunikace pro danou IP adresu tak bude směrována útočníkovi.

Zrušení se provede stejně jako u ARP.

5 Přesměrování provozu

Přesměrování provozu vytváří pro oběti iluzi, že jejich komunikace není nikým narušena. Tudíž všechny pakety odeslané obětí A se přes útočníka dostanou k oběti B a naopak. Útočník tak dostane přístup ke všem posílaným paketům obětmi.

Implementovaný **pds-intercept** odchytává veškerou přístupnou komunikaci v síti přeposílá dál ty pakety, které patří obětem. V okamžiku, kdy útočník obdrží paket zjistí z ethernetové hlavičky MAC adresu odesílatele, pomocí které vyhledá spřízněnou MAC adresu, které paket ve skutečnosti patří. Zda MAC adresy k sobě patří je zřejmé ze zadaného vstupního souboru, kde jsou dvojice obětí spojeny stejným atributem. Tento zadaní vstupní soubor je před odchytáváním komunikace zpracován na seznam dvojic k sobě patřících MAC adres.

Jakmile útočník nalezne potřebnou MAC adresu, odešle celý paket správnému vlastníkovi. Obě z obětí mají tedy pocit, že je vše v pořádku.

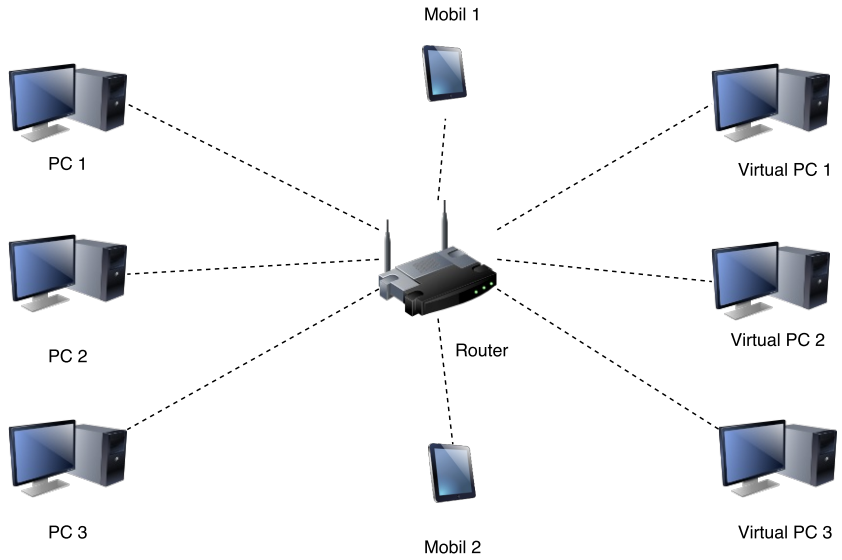
6 Experimenty s implementací

Po dovršení implementace bylo provedeno testování na vytvořené topologii domácí sítě s několika fyzickými zařízeními a několika virtuálními zařízeními. Většina zařízení podporovala IPv6 komunikaci, takže bylo možné otestovat obě části projektu. Obrázek 3 ukazuje schéma topologie.

6.1 Topologie

Bližší specifikace topologie:

- Router - bezdrátový router podporující IPv4 a IPv6
- PC 1 a 2 - fyzické počítače s operačním systémem Linux Mint, přiřazená IPv4 a Ipv6 adresa
- PC 3 - fyzické zařízení se systémem Windows 10, přiřazena IPv4 a IPv6
- Virtual PC 1-2 - virtuální zařízení s referenčním systémem Ubuntu, přiřazena Ipv4 a IPv6
- Virtual PC 3 - virtuální zařízení s referenčním systémem Ubuntu, přiřazena IPv6
- Mobil 1 - fyzické zařízení se systémem Windows, přiřazena IPv4
- Mobil 2 - fyzické zařízení se systémem Android, přiřazena IPv4 a IPv6



Obrázek 3: Obrázek referenční topologie, kde byl projekt testován.

6.2 Výsledky testování jednotlivých částí

6.2.1 Skenování

Skenování bylo provedeno nesčetněkrát během implementace a následného testování celku. Ve většině případů byla objevena všechna zařízení připojena pomocí IPv4 protokolu. Některá spuštění však nebylo možné zaměřit hlavní router na základě IPv4, ale povedlo se pomocí IPv6.

Zařízení, která měla spuštěný operační systém Linux Mint nebo Ubuntu byla detekována ve většině případů skenování. Problém se zaměřením stanice pomocí IPv6 přetrvává při spuštěném operačním systému Windows (podle RFC běžný jev v tomto zvoleném způsobu skenování). Mobilní telefon odpovídal pouze někdy.

Neúspěch při nalezení existující stanice byl zapříčiněn nejspíše ztrátou paketu nebo vypršením času pro skenování.

6.2.2 Otrávení cache

Otrávení cache bylo testování převážně na virtuálních strojích pro nenarušení plynulého chodu domácí sítě. Otrávení ARP i NDP cache je možné pro libovolná dvě zařízení v lokální síti bez sebemenších problémů. Po ukončení aplikace (ctrl-c nebo ctrl-z) jsou odeslány pakety, která obnoví ARP a NDP cache obětí na původní data.

Ověření, zda data v cachi jsou otrávena/správná bylo provedeno příkazem *ip neighb* v terminálech obětí, kde se přepisovaly jednotlivé MAC tak, jak útočník zasílal otrávené/opravné pakety.

6.2.3 Přesměrování provozu

Přesměrování provozu bylo testováno na jedné a dvou dvojcích obětí v síti. Kontinuální otrávení cache mělo za účinek, že útočící stanice odchytávala provoz mezi jednotlivými stanicemi dvojic. Všechny takto získané pakety následně přeposílala svým právoplatným majitelům bez známek problémů v komunikaci nebo síti.

Reference

[1] Man in the middle (mitm) attack. https://www.veracode.com/security/man-middle-attack, ©2017. [online]. [cit. 2017-23-04].

[2] H. S. E. Nordmark, W. Simpson. Neighbor Discovery for IP version 6 (IPv6). RFC 4861, RFC Editor, September 2007.

[3] D. C. Plummer. An Ethernet Address Resolution Protocol. RFC 826, RFC Editor, November 1982.

[4] E. G. S. Cheshire, B. Aboba. Dynamic Configuration of IPv4 Link-Local Addresse. RFC 3927, RFC Editor, May 2005.

[5] J. Stretch. Ipv6 neighbor spoofing. http://packetlife.net/blog/2009/feb/2/ipv6-neighbor-spoofing/, ©2017. [online]. [cit. 2017-23-04].