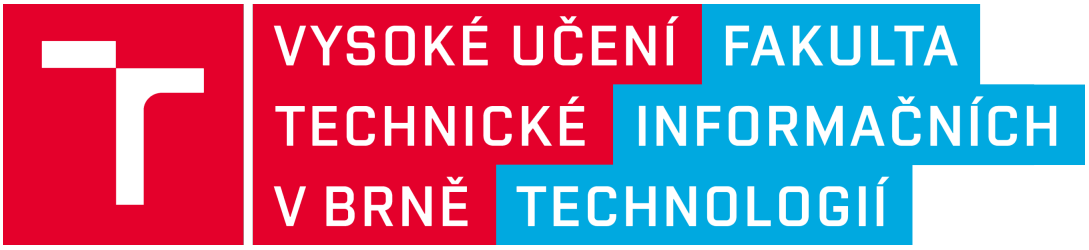
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií



L2 MitM (hromadný projekt)

Dokumetace k projektu do předmětu PDS

Autor: Jordán Jarolím, xjarol03
23. 4. 2017

Obsah

1 Úvod

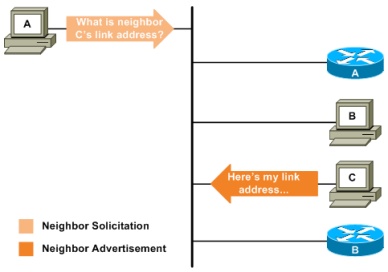
Cílem projektu L2 MitM (hromadný projekt) do projektu PDS bylo provést Man in the Middle útok na síťvou komunikaci. K útoku měla být využita ARP a NDP cache, respektive jejch otrávení a přeposílání komunikace. Tedy přeposílání ze zdrojového zařízení přímo na zařízení, na kterém je schopný útočník komunikaci odposlouchávat a dále ji přeposílat k cílovému zařízení tak, aby ani jeden z uzlů neměl ponětí o tom, že je odposloucháván.

1.1 ARP

ARP je protokol počítačových sítí využíván při IPv4 (Internet Protocol Version 4). ARP je jedním z klíčových funkcionalit protokolu této verze. Slouží k překladu (mapování) IP adresy s MAC adresou zařízení a funguje na principu dotazování-odpověď. Pokud budeme uvažovat striktní dodržování ISO/OSI modelu nebo TCP/IP, jedná se o propojení 2. a 3. vrstvy. Narozdíl o IP adresy by měla být MAC adresa v celém internetu unikátní a každé jedno zařízení by mělo mít svou MAC adresou odlišnou od všech ostatních. Toho se využívá při přeposílání datových rámců, paketů a všeobecně jakékoliv komunikace z jednoho zařízení na druhé, ať už v jedné síti, nebo v různých lokálních sítích. Pokud má být tedy paket poslán v síti na zařízení s IP adresou XY, odesílatel první musí přeložit tuto IP adresu na MAC a tuto MAC uvést do rámce. Podívá se nejprve na svou cache, kde má uložené známé překlady a pokud tam nenajde odpovídající IP adresu a MAC adresu, posílá ARP dotaz broadcastem ve znění: “Hledám MAC adresu zařízení s IP XY, dejte mi prosím vědět na adresu AB”. Zařízení, které má přiřazenou IP XY odpovídá unicastem zažízení AB. Po tomto kroku mají obě zařízení uloženy navzájem své adresy v ARP cache. Právě skutečnosti, že se odesílatel nejprve podívá do své ARP tabulky využívá implementovaný útok, viz níže.

1.2 NDP

NDP je oproti ARP protokol při Ipv6 a má daleko širší použití. Mimo překlad IP-MAC zaštiťuje také autokonfiguraci uzlů po připojení do sítě, nalezení routerů v lokální síti (router solicitation & advertisement), next-hop discovery, duplicate address detection a další... O překlad IP-MAC se starají zprávy Neighbour Solicitation a Neighbour Advertisement (u ARP je to ARP Request a Reply), viz obr. 1. Drobné rozdíly jsou také ve skupině příjemců těchto zpráv (broadcast vs multicast). NDP je součástí ICMPv6 a pokud říkáme, že je ARP klíčovým pro IPv4, tak NDP je ještě důležitější pro IPv6. Pro naše účely avšak stačí připomenout, že uzly si spravují svou NDP cache, do které si ukládájí mapování IP-MAC a otrávení cache funguje v podstatě na stejném principu.



Obrázek 1: Neighbour Solicitation

2 Man in the middle attack

Jak bylo zmíněno v úvodu, man in the middle attack má za cíl odposlouchávat komunikaci mezi dvěma uzly tak, aby se komunikace jevila jako normální bez známek jakéhokoliv útoku, obr 2. Útok pomocí otrávení cache má z pohledu útočníka několik fází:

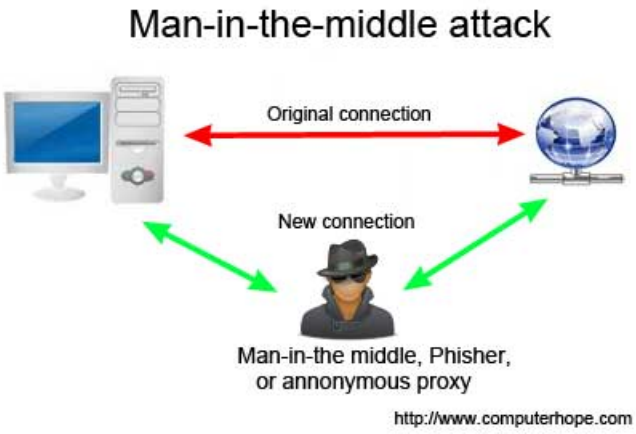
- Discovery sítě a zjištění možných obětí a zjištění relevantních informací (IP, MAC)
- Výběr obětí
- Otrávení ARP/NDP cache obětí útočníkem
- Odchytávání a přeposílání komunikace
- Zametení stop (vrácení cache do původního stavu)

Discovery sítě může být provedeno, dle IPv4 nebo IPv6 různými způsoby. Intuice říká, že by mohlo stačit poslat ping na broadcast (v případě IPv6 na multicastovou skupinu, kam jsou přihlášeny všechny uzly) a čekat na odpovědi. Problémem však je, že většina hostů blokuje a neodpovída na zprávy ping rozesíláné na broadcast. U IPv6 se tento problém (zatím) v takové míře nevyskytuje. Pro IPv4 je tedy jendou z možností zjistit rozsah sítě a poslat ARP dotaz na každou IP adresu v síti. Tím získáme kompletní seznam aktivních hostů připojených do sítě.

Otrávení cache oběti pak probíhá opakovaným zasíláním podvržených a custom vytvořených ARP odpovědí, nebo neighbour advertisement odpovědí. Klasicky by taková odpověď měl obsahovat mou IP a mou MAC adresu. Abych však trávil cache, je nutné zasílat na obě dvě oběti pakety s IP adresou druhé oběti a s MAC adresou útočníka.

Pakety jsou sice směřované na IP adresu oběti, ale díky otrávene cache je v rámci uložena MAC adresa útočníka. Tím pádem je mu doručena veškerá komunikace mezi dvěma uzly. Nyní je úkolem útočníka identifikovat pakety, které jsou si přes něj přeposílají oběti a přeposlat je správným směrem. Jednoduše poté, co si z paketů a přečte informace které potřebuje, nastaví do hlavičky ethernetového rámce správnou mac adresu oběti a paket přepošle do sítě. Obětipaket dorazí a komunikace se jeví jako naprosto normální bez známek odposlouchávání.

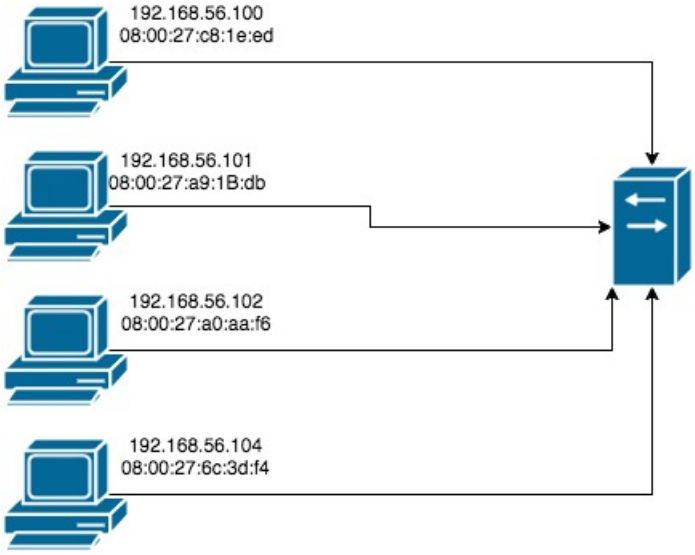
Po ukončení odchytávání komunikace je nutné po sobě také zamést stopy, tak aby se oběť nikdy nedozvěděla, že byla její komunikace odposloucávána. Stačí tedy uvést cache oběti 1 do původního stavu a k IP adrese oběti 2 přiřadit správnou MAC adresu.



Obrázek 2: Man in the middle

3 Implementace a demonstrace činnosti

Projekt byl dle zadání implementován v jazyce C/C++ pro unixové systémy. Pro implementaci IPv4 Man in the middle útoku byla použita knihovna libpcap (http://www.tcpdump.org/), pro verzi IPv6 nebyl implementován. Vásledný projekt se skládá ze třech samostatných programů, kde jeden provede discovery sítě (scanner), druhý má na starost otrávení cache (spoof) obětí a třetí se stará o přeposílání komunikace (intercept). Další externí použitou knihovnou je rapidxml (http://rapidxml.sourceforge.net/) pro manipulaci s xml dokumenty - konkrétně ukládání výsledků discovery sítě a načítání obětí pro spoof a intercept. Projekt byl testován v prostředí virtualbox na referenčních strojích ISA2015 a to v následující topologii:



Obrázek 3: Topologie

kde pod IP 192.168.56.101 se skrývá útočník a pod adresami 192.168.56.102 a 192.168.56.104 jsou oběti. Nejprve byla obětem otrávena ARP cache a poté 192.168.56.104 vyzkoušl ping na 192.168.56.102. Jako ICMP Request tak ICMP replies byly viditelné pro útočníka na 192.168.56.101 a ICMP komunikace probíhala normálně bez komplikací. Detailní testování je možno shlédnout zde: https://www.youtube.com/watch?v=g7R069Ho2Rw - jedná se o screen recording z testování útoku.

4 Závěr

Byl implementován Man in the middle attack pro IPv4 a všechny jeho dílčí části - discovery sítě, otrávení cache i přeposílání komunikace. Útok pro IPv6 implementován nebyl. Byly tedy alespoň částečně splněny všechny body zadání. Současně nebyl implementován žádný z bonusových příkladů.