

ARP Spoofing

Vložil/a [0xb1t](#) [1], 1 Srpen, 2006 - 22:31

- [Networks & Protocols](#) [2]
- [Security](#) [3]

Teorie zneužití Address Resolution Protocolu. Jde o to poslat počítači A tak sestavený arp paket, aby si k IP adrese počítače B přiřadil MAC počítače X. Příklad využití ARP Cache Poisoning je realizace útoku man-in-the-middle - útočník vykonává funkci prostředníka => vidí veškerou komunikaci počítačů A a B

Uvodem

Počítač v síti typu Ethernet/TCP/IP má dvě adresy. Jedna patří síťové kartě - MAC(Media Access Control) adresa. Teoreticky tato adresa je unikátní a nachází se v paměti síťovky (v praxi je to ale poněkud jinak). MAC adresa je nedílnou součástí přenosové metody CSMA/CD, která se používá pro fyzický přenos dat. Tato metoda dělí data na 1.5KB dlouhé rámce (frame). Každý rámec má ve svém záhlaví MAC adresu příjemce a odesílatele.

Druhá adresa je IP adresa. IP se používá nezávisle na fyzické realizaci sítě. IP adresa se přiděluje softwarově. IP a Ethernet musí pracovat spolu. IP používá v komunikaci bloky dat - pakety, ovšem IP paket nemůže být odeslán samostatně. V síti Ethernet je každý paket rozdělen na rámce, dostane příslušné záhlaví a teprve pak bude předán na síť. Ale ve chvíli kdy počítač generuje záhlaví, většinou nezná MAC adresu příjemce, kterou potřebuje pro přenos Ethernetem. Zná pouze IP. Pro vyhledání MAC adresy podle IP se používá ARP (Address Resolution Protocol).

ARP

ARP posílá dotazy, které se v podstatě ptají: "Váš IP je x.x.x.x? Ano? Vyberte mi pak vaši MAC." ARP pakety jsou vyslány všem počítačům v broadcast doméně. Každý počítač segmentu tak analyzuje příchozí ARP dotazy a odpovídá v případě shody IP adres. Pro zmenšení počtu ARP paketů, se příchozí odpovědi průběžně ukládají do cache. Vždycky když počítač přijme odpověď, uloží si do cache novou kombinaci IP/MAC. Většina OS modifikuje cache tabulku bez ohledu na to, zda se o to tážely nebo ne. A o tom je ARP spoofing - poslat počítači A tak sestavený arp paket, aby si k IP adrese počítače B přiřadil MAC počítače X. Počítač A tak pochopitelně bude považovat počítač X za počítač B. Bude komunikovat s X bez nejmenšího podezření, že nejde o B. Take se tomu říká otrávení (poisoning)...

Sniffing na switchi

Switch určuje na jaký port půjde který rámec cestou porovnávání MAC adresy rámce se zaznamená ve své tabulce. Jeho tabulka obsahuje seznam portů a MAC adres, které na nich zaslechl. Většinou se tabulka naplňuje po zapnutí switche automaticky - první zdrojová MAC se přiřazuje portu z něhož rámec pochází. Síťová karta může být uvedena do režimu odposlechu (promiscuous mode), při kterém se budou přijímat všechny rámce bez ohledu na cílovou MAC. V prepínaném Ethernetu to je celkem nuda, jelikož aktivní prvky jako mosty a switche směřují pakety podle svých tabulek. Ale pomocí ARP imitace lze přece jen něco poladit v prepínaných sítích... Jako příklad použití ARP může posloužit útok typu "man-in-the-middle". Útočník v podstatě staví svůj počítač mezi dvě komunikující a vykonává funkci jakéhosi prostředníka, přes kterého veškerá komunikace protéká :). Přitom útočník může preposílat data, aniž by jejich tok přerušil. Příklad algoritmu může být následující:

-X útočník, A a B počítače v síti

-X posílá "jed" pro ARP cache A a B

ARP Spoofing

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

- A si prirazuje IP adresu B k MAC adrese X
- B si prirazuje IP adresu A k MAC adrese X
- veskera komunikace mezi A a B ted bude prbihat pres X

Mozne je "otravit" cache nejen pocitacu ale i routeru/gatewayu. Tim lze ziskat veskerou komunikaci s inetem (NE v pripade velke site - utocnik by riskoval byt zavalen pakety :)

Flood

Zapis neexistujici MAC adresy do ARP tabulky vyvola ztraceni ramce. Nepochopitelne komu vyslany ramec bude putovat siti, po vsehch jeji uzivatelech. To je mimochodem jeden z vedlejsich ucinku MiM utoku, kdy pocitac utocnika je nahle odpojen a "otravene" pocitace A a B nadale rozesilaji ramce s uz neexistujici MAC adresou. Proto je treba pred odpojenim vratit ARP cache obou pocitacu do puvodniho stavu.

Klonovani

Prakticky vsechny dnesni sitovky umoznuji zmenu MAC uzivatelem. Kdyz je znama MAC adresa obeti, utocnikovi nic nebrani v tom, aby jednoduse zamenil svou adresu adresou odeti. Tim muze napriklad zmast autorizaci zalozenou na MAC, jeziz pouziti neni nijak vyjmečne.

Kod pro ilustraci:

ARPoison

<http://www.arpoison.net/> [4]

Programek pro UNIX-like systemy, prikazovej radek. Umoznuje generovat ARP pakety.

Ettercap

<http://ettercap.sourceforge.net/> [5]

Vykonnej software pro UNIX s textovym GUI, specialne pro Script kiddies ;)). Veskere operace probihaji automaticky, seznam pocitacu vytvari na zaklade sitoveho provozu.

URL článku: <https://security-portal.cz/clanky/arp-spoofing>

Odkazy:

[1] <https://security-portal.cz/users/0xb1t>

[2] <https://security-portal.cz/category/tagy/networks-protocols>

[3] <https://security-portal.cz/category/tagy/security>

[4] <http://www.arpoison.net/>

[5] <http://ettercap.sourceforge.net/>