ARP Spoofing

Vložil/a 0xb1t [1], 1 Srpen, 2006 - 23:31

- Networks & Protocols [2]
- Security [3]

Teorie zneuziti Address Resolution Protocolu. Jde o to poslat pocitaci A tak sestavenej arp paket, aby si k IP adrese pocitace B priradil MAC pocitace X. Priklad vyuziti ARP Cache Poisoning je realizace utoku man-in-the-middle - utocnik vykonava funkci prostrednika => vidi veskerou komunikaci pocitacu A a B

Uvodem

Pocitac v siti typu Ethernet/TCP/IP ma dve adresy. Jedna patri sitove karte - MAC(Media Access Control) adresa. Teoriticky tato adresa je unikatni a nachazi se v pameti sitovky(v praxi je to ale ponekud jinak). MAC adresa je nedilnou soucasti prenosovy metody CSMA/CD, ktera se pouziva pro fyzicky prenos dat. Tato metoda deli data na 1.5KB dlouhy ramce (frame). Kazdy ramec ma ve svem zahlavi MAC adresu prijemece a odsilatele.
Druha adresa je IP adresa. IP se pouziva nezavisle na fyzicky realizaci site. IP adresa se prideluje softwarove. IP a Ethernet musi pracovat spolu. IP pouziva v komunikaci bloky dat - pakety, ovsem IP paket nemuze byt odeslan samostatne. V sitich Ethernet ja kazdy paket rozdelen na ramce, dostane prislusne zahlavi a teprv pak bude predan na sit. Ale ve chvili kdy pocitac generuje zahlavi, vetsinou nezna MAC adresu prijemce, kterou potrebuje pro prenos Ethernetem. Zna pouze IP. Pro vyhledani MAC adresy podle IP se pouziva ARP (Address Resolution Protocol).

ARP

ARP posila dotazy, ktere se v podstate ptaj: "Vase IP je x.x.x.x?Ano?Vyborne.Poslete mi pak vasi MAC." ARP pakety jsou vyslany vsem pocitacum v broadcast domene. Kazdej pocitac segmetu tak analyzuje prichozi ARP dotazy a odpovida v pripade shody IP adres. Pro zmenseni poctu ARP paketu, se prichozi odpovedi prubezne ukladaji do cache. Vzdycky kdyz pocitac prijme odpoved, ulozi si do cache novou kombinaci IP/MAC. Vetsina OS modifikuje cache tabulku bezohledu na to, zda se o to tazaly nebo ne. A o tom je ARP spoofing - poslat pocitaci A tak sestavenej arp paket, aby si k IP adrese pocitace B priradil MAC pocitace X. Pocitac A tak pochopitelne bude povazovat pocitac X za pocitac B. Bude komunikovat s X bez nejmensiho podezreni, ze nejde o B. Take se tomu rika otraveni (poisoning)...

Sniffing na switchi

Switch urcuje na jaky port pujde ktery ramec cestou porovnavani MAC adresy ramce se zaznamy ve sve tabulce. Jeho tabulka obsahuje seznam portu a MAC adres, ktere na nich zaslechl. Vetsinou se tabulka naplnuje po zapnuti switche automaticky - prvni zdrojova MAC se prirazuje portu z nehoz ramec pochazi. Sitova karta muze byt uvedena do rezimu odposlechu (promiscuous mode), pri kterem se budou prijmat vsechny ramce bez ohledu na cilovou MAC. V prepinanem Ethernetu to je celkem nuda, jelikoz aktivni prvky jako mosty a switche smerujou pakety podle svych tabulek. Ale pomoci ARP imitace lze prece jen neco poladit v prepinanych sitich... Jako priklad pouziti ARP muze poslouzit utok typu "man-in-the-middle". Utocnik v podstate stavi svuj pocitac mezi dva komunikujici a vykonava funkci jakehosi prostrednika, pres ktereho veskera komunikace proteka :). Pritom utocnik muze preposilat data, aniz by jejich tok prerusil. Priklad algoritmu muze byt nasledujici:
-X utocnik, A a B pocitace v siti
-X posila "jed" pro ARP cache A a B

-A si prirazuje IP adresu B k MAC adrese X
-B si prirazuje IP adresu A k MAC adrese X
-veskera kominukace 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 vsech 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, jejiz pouziti neni nijak vyjmecne.

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/