Linnéuniversitetet
Institutionen för datavetenskap, fysik och matematik

Laboration

Laboration 4

Rekognosering och nätverksattacker

Författare: Niclas Håkansson
Handledare: Niclas Håkansson
Termin: VT13
Kurskod: 1DV425

Innehåll

Instruktioner

Laborationens delar

Laborationen består av att förbereda miljön för laborationen, att läsa in sig på de delarna laborationen behandlar, genomförande och en skriftlig rapport.

Förberedelse

Läs igenom kapitel 5 och 6 i kurslitteraturen [1] med fokus på de delar som berör port scanning, ARP-spoofing, IP-spoofing, DNS cache poisoning och DNSSEC. Läs igenom hela laborationsdokumentet innan ni startar med uppgifterna för att säkerhetsställa att ni inte missar något.

Laborationsmiljö

För laborationen behövs tre maskiner, en klient av valfritt OS, en attackerare där ni med fördel kan välja Backtrack som kommer med många säkerhetsprogram förinstallerade och en server av valfri Linuxdistribution. Servern behöver ha en DNS-tjänst installerad som ni ska kunna göra uppslag emot och som använder sig av CSLab-nätverkets DNS-server som Authoritative server.

Redovisning

Laborationen redovisas genom en skriftlig rapport som skrivs enskilt av varje deltagare. Rapporten ska innehålla försättsblad med titel och författarens namn, en innehållsförteckning, beskrivning av genomförandet, en avslutande reflektion och en referenslista om ni använt er av referenser i rapporten.
Rapporten mailas till nh222aq@student.lnu.se som PDF eller delas på Google Docs. Deadline för rapporten är den 6 mars 2013.

Genomförande

Port Scanning

Beskriv hur en TCP scan, SYN scan, idle scan och UDP scan går till och vad för information du kan få ut av sökningarna. Beskriv även de problem som de olika sökningarna har och varför det inte alltid går att lita på den information som sökningen ger. Fundera även på vad du kan göra med den information som sökningarna ger och beskriv ett scenario där du som attackerare eller administratör kan använda den informationen till din fördel.

Traceroute

Gör en undersökning om hur er väg till adresserna www.uq.edu.au och www.google.se ser ut med hjälp av traceroute, kör traceroute från er fysiska maskin för att slippa få med konstiga resultat från VMWare. Försök även få fram lite mer information om adresserna genom att använda er av whois kommandot, för att få mer information om vad ni kan leta efter så rekommenderas det att läsa [2] där de går igenom hur informationsinsamling går till (observera att ni inte behöver samla in all den information de får ut i den artikeln utan läs de delar som handlar om whois

och vad ni får ut av det). Ni kan även slå upp adresserna på http://whatismyipaddress.com/ för att få fram lite mer information, till exempel den geografiska positionen.
I rapporten bör ni ta med den information som ni anser vara relevant om adresserna, kan till exempel vara vilken ISP de tillhör, hos vem domännamnet är registrerat, men även annan information ni tycker är relevant. Rapporten ska också innehålla en analys av den väg ni tar till domänen där ni resonerar kring de länkar som har högst fördröjning och varför just de länkarna har så hög fördröjning.

ARP Spoofing

Tanken här är att ni ska utföra en så kallad Man-in-the-Middle Attack (MitM) med hjälp av ARP spoofing. Upprätta en telnet-anslutning till en router på CSLab-nätverket från er klient och utför MitM attacken med hjälp av er attacker-maskin. Ettercap finns installerat i Backtrack och kan användas till denna attack, det finns även Wireshark på den så att ni kan försöka fånga upp lösenordet som används till routern.
Rapporten ska innehålla en beskrivning av attacken, hur lätt eller svår den var att utföra och om ni stötte på några problem. Försök även hitta några tekniker som ni skulle kunna implementera för att förhindra er ARP spoofing attack och beskriv de i er rapport.

IP Spoofing

Beskriv hur en IP spoofing attack går till och i vilka sammanhang de oftast används av attackerare. Beskriv även några tekniker som kan användas för att förhindra IP spoofing.

DNS cache poisoning

Ni ska med hjälp av attacker-maskinen utföra en DNS cache poisoning mot er egen DNS-server för att peka om er klient till en sida som ni sätter upp på attacker-maskinen. Ni behöver konfigurera er DNS-server till att använda er av en DNS-server på CSLab för att göra uppslag emot, de har IP-adress 192.168.228.4 och 192.168.231.4.
För att sätta upp en simpel sida som attacker-maskinen kan svara med kan ni använda er av kommandot

```
cat file | sudo nc -l 80
```

Filen file innehåller den text ni vill visa för klienten. Ni kan till exempel försöka sätta upp så att er attacker-maskin svarar på anrop till Wikisidan som ligger på CSLab-nätverket.
Tips för att lyckas är att använda en äldre version av DNS-programvaran som inte genererar slumpmässiga ID-nummer på paketen. Attacken går i kort ut på att ni skickar en DNS-request och utger er för att vara Authoritative DNS för er egen DNS-server och svarar med ett förfalskat DNS-reply som pekar

på er egen dator. I tråden [3] förklarar de lite hur det ska gå till och vad det finns för verktyg att lyckas med en DNS cache poisoning attack.
I rapporten ska det framgå om ni lyckades med attacken och hur ni gjorde, lyckades ni inte så förklarar ni varför och vad ni kunde gjort för att lyckats. Om ni lyckas med attacken och vill ha lite mer utmaning får ni gärna testa att göra attacken mot en helt uppdaterad DNS-programvara för att se om ni klarar det också, ta med i rapporten om ni lyckats eller misslyckats och varför.

DNSSEC

Beskriv hur DNSSEC fungerar rent teoretiskt och varför den DNS cache poisoning-attacken som gjordes i föregående uppgift inte hade fungerat om ni använt er av DNSSEC. Försöka även leta upp ett antal siter som använder sig utav DNSSEC och ta med dem i er rapport.

Referenser

[1] M. T. Goodrich and R. Tamassia, Introduction to computer security, Boston: Pearson, 2011.
[2] B. J. Nikkel, "Domain name forensics: a systematic approach to investigating an internet presence", Digital Investigation, vol. 1, no. 4, pp. 247-255, Dec. 2004.
[3] INTERN0T, “DNS Cache Poisoning Reviewed + Tools”, intern0t.org [Online] Available: https://forum.intern0t.org/hacking-tools-utilities/238-dns-cache-poisoning-reviewed-tools.html [Accessed: Feb. 19, 2013]