The Hacking Dojo 4 - Sådan hacker du - Så går vi aktivt

Vi skal nu til at bygge videre på de ting du lærte i den sidste lektion og tage tingene et step videre og hvor den sidste lektion meget handlede om passive værktøjer og teknikker går vi nu aktivt ud, med de fordele og ulemper det har for en hacker. Det ov

Skrevet den **13. Nov 2010** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ⭐⭐⭐☆☆

Portscanning med nmap

Igen er der en naturlig årsag til at jeg vælger portscanningen som emne. Dels anvender og dermed forstærker vi det der er (Skal være) lært i sidste lektion og dels udbygger vi den forståelse som du forhåbentlig har opnået og endeligt løfter vi emnet yderligere nogle niveauer i forhold til OSI modellen, og kigge på sockets og socket forbindelser. Portscanning kan heller ikke betragtes som enkelthandlinger der hver især producerer et resultat. Ofte skal der foretages flere på hinanden følgende scanninger af samme host og en intelligent forholden sig til enkelt resultaterne for at kunne afgøre hvad det faktisk er man står overfor og skal man port scanne uden at larme og blive opdaget kan en enkelt scanning tage meget lang tid

[b]Portscanneren[b]

Der er også en god grund til at det værktøj jeg anbefaler er nmap. Dels er der her tale om "alle moders" portscanner, det er simpelthen den man bruger "i branchen" og du har måske allerede set den i action, hvis du har set filmen "Matrix Reloaded" hvor Trinity portscanner The Matrix med netop Nmap. En anden grund er at Nmap nok er den portscanner der kan mest. Den seneste udvikling har indført Nmap Scripting Engine der gør nmap til meget mere end en portscanner og der ligger her nogle muligheder for at automatiserer nogle ret hårde rutiner både til hacking og til overvågning. Det vil vi kikke på meget senere i denne lektions række.

[b]Advarsel[b]

Jeg vil på det kraftigste advare mod at ports canne rigtige levende host på internettet, selvom det kan færre fristende at gøre det og selvom der for det meste ikke sker det store ved det. Grunden til at der oftest ikke sker noget er ,at der ikke er ret mange der gider gøre noget ved en relativt simpel portscanning. Der skal dog ikke herske tvivl om at det er ulovligt og at du kan blive straffet for det, især hvis du scanner den samme host flere gange. Du kan også være ude for at det er din ISP der lukker din forbindelse hvis du laver den slags, så hold dig inden for dit lukkede miljø.

[b]Lab opsætning.[b]

Til portscanning bør du anvende flere hosts og gerne forskellige hosts med forskellige applikationer installeret idet en mail server ikke har de samme porte åbne som en ftp server. Hvis du har muligheden bør du også scanne hosts der står bag en firewall og hosts der har personlige firewalls installeret og kørende. Test gerne forskellige firewalls og forskellige settings for de enkelte firewalls. Du kan, på Microsofts hjemmeside donwloade 60 dages prøveversioner af Micrsofts servere og installerer disse i dit virtuelle miljø.

[b]Øvelser[b]

1. Som sædvanelig skal vi have fat i google til at starte med. Prøv denne gang også at kigge forbi youtube og http://vimeo.com og se om du ikke kan finde adskilledige videoer med instruktioner i brug af Nmap og port scanning, søg især på port scanning and firewall/IDS/IPS avoidance og defeating/circumventing firewalls/IDS/IPS og den slags søgninger

2. Når du er klar til at tage Nmap i brug (start med at give kommandoen man nmap på din Linux maskine) så skal vi i gang med noget basal host discovery. Husk først at læse om hvad switchen gør og husk hver gang at sniffe det du scanner og gem snifferesultatet så du kan sammenligne og se hvad den praktiske forskel på de enkelte kommandoer er. Husk også at tune hver snifning så du kun får de resultater det faktisk handler om med. Se på disse switche

-sL: List Scan -
-sP: Ping Scan - go no further than determining if host is online
-PN: Treat all hosts as online skip host discovery
-PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports
-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
-PO [protocol list]: IP Protocol Ping

Find også ud af hvilke porte Nmap som standard scanner og hvordan du sætter den til at scanne alle porte i ranget.

3. Så skal vi igang med decideret portscanning af hosts. kig på

-sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
-sU: UDP Scan
-sN/sF/sX: TCP Null, FIN, and Xmas scans
-scanflags <flags>: Customize TCP scan flags
-sO: IP protocol scan

4. Nmap kan også lave Layer 3 og 4 OS detection med -O og -A. Læs nmap man page, søg med google og kig på http://www.insecure.org for informationer. Husk at sniffe så du ser hvordan nmap laver sine OS detections og mindst lige så vigtigt hvordan de enkelte hosts svare tilbage. Lav OS detectcion mod så mange forskellige host som muligt også forskellige versioner af samme OS.

5. Næste trin at at kigge på teknikker til beskytte sig mod layer 3 og 4 OS fingerprinting. find, læs om og installer værktøjerne Security Cloak http://www.securiteam.com/tools/5MP052KI0A.html, Fingerprint Fucker og læs "A practical approach for defeating Nmap OS-Fingerprinting" http://www.zog.net/Docs/nmap.html samt IP Personality http://ippersonality.sourceforge.net/ og kør så øvelserne ovenfor igen. Husk at sniffe så du ser forskellen på hvordan de enkelte host svare på de forespørgsler der kommer.

6. Kig på timing og serviceces/version detection med switchene

-T[0-5]: Set timing template (higher is faster)

Og husk at paranoid scann (-T0) sagtens kan tage uger at afslutte og at det netop er den slags settings en hacker ville anvende for at undgå opdagelse af f.eks IDS mm.Det vil vi kigge på i en senere lektion.

7. Endelig bør du prøve nogle at de teknikker du læse om og så på video i øvelse 1 til at lave firewall circumventing, IDS avoidance og tilsvarende.

Formålet her er dels at lære at lave og tolke portscanninger, men også og måske endnu mere at give en endnu dybere protokolforståelse. Ved at kigge på Nmap med en sniffer vil du kunne se hvordan Nmap udnytter de enkelte protokoller og nogle gange udnytter protokollerne ved at gøre noget andet end protokollen normalt foreskriver. Denne viden er helt nødvendig for at kunne hacke

Igen er du meget velkommen til at spørge via min mail kim@bufferzone.dk hvis du får problemer med at forstå et eller andet.

Kommentar af walkie84 d. 25. Nov 2008 | 1

Rigtig god læsning!

Kommentar af dustie d. 20. Dec 2008 | 2

Kommentar af enza d. 24. Nov 2008 | 3

nu kan jeg se hvad du ville bruge en sniffer til udover at beskytte sig selv :)
har aldrig tænkt på at finde exploits på den måde :) godt med nytænkning :)
håber der vil komme nogle flere artikler fra dig =)