The Hacking Dojo 2 - Sådan hacker du - Byg dit Lab

I denne artikel beskriver jeg hvordan du bygger det lab der er nødvendig for at du kan lære det nødvendige. Husk at du ikke kan læse dig til viden og kunnen, du skal gøre og det foregår i et lab. Artiklen omfatter hardware, OS, systemer og programmer.

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

Computeren.

Du skal selvfølgelig bruge en computer, men grunden til at jeg specifikt nævner det, er naturligvis at der er et par pointer, der er værd at tage med. Du bør bruge en computer som du ikke rigtig bruger til andet, altså ikke den PC du eller familien er afhængig af til arbejde, lektier og daglig kommunikation. Dette skyldes to ting, dels at du med stor sikkerhed kommer til at om- og gen-installerer et antal gange og dels at en PC med hacker værktøjer og sårbare hosts (det forklarer jeg om lidt) er guf for alle andre hackere. Hackeren vil kunne bruge dine værktøjer og de huller du er nødt til at have når vi bliver mere avancerede til at hacke dig med, så for din egen sikkerheds skyld.

Hardware.

Det vigtigste er RAM, mindst 2 Gbyte og gerne 4Gbyte. Grunden til dette er, at du jo skal hacke en anden maskine og det bør du gøre på en sikker og kontrolleret måde, så du ikke ødelægger noget eller begår ulovligheder. Dette vil sige at du arbejder i et virtuelt miljø og det kræver RAM. Jo mere RAM jo hurtigere køre det og jo flere virtuelle maskiner kan du starte op

Harddiske er nr. to. Dels fylder alle de virtuelle maskiner du skal arbejde med jo en del og endelig giver hurtige diske i den rigtige konfiguration også hurtigere afvikling så du ikke skal sidde og vente på dit system. Jeg vil anbefale dig at have to diske i dit system, en til den fysiske maskinen operativsystem og en (eller flere) til de virtuelle maskiner. Med tingene fordelt på flere hurtige diske køre det samlede system noget hurtigere end hvis det hele ligger på en disk. En ekstern disk, til opbevaring af værktøjer, dokumenter, ISO'er og kopiere af dine virtuelle maskiner er også en stor fordel da tingene en gang i mellem går i stykker og skal indkopiere igen.

Grafikkort har de seneste år fået ny betydning. I gamle dage sagde jeg altid at grafikkort og lydkort var ligegyldige, men sådan behøver det ikke at være i dag. Grafikkort i dag har egne processore og ofte adgang til ram, hvis de ikke har onboard ram på kortet. Alle disse muskler kan bruges til andre ting end ligegyldige spil. De kan bruges til at cracke passwords og andre former for brute forcing. Dette er dog en lidt speciel diciplin, så du behøver ikke et muskel grafikkort til at starte med, men kan få brug for et senere hen i din læringsprocess

Operativsystemet.

Hvad du vælger som operativsystem til din fysiske maskine er i første omgang ikke så væsentligt. Da du til sidst alligevel ende på en Linux maskine så min anbefaling er naturligvis at du starter med at indlægge Linux på den. At have Linux i bunden har to fordele. Dels vil du skulle hacke fra en Linux maskine og har du Windows i bunden vil du skulle køre med to virtuelle maskiner åbne samtidig med dit bund OS. Med Linux i bunden skal du kun åbne en virtuel maskine og dermed bruger du mindre ressourcer. Den anden fordel er at du bliver bedre til at bruge Linux ved at skulle arbejde med dette operativsystem til alt på din maskine og det er meget nødvendigt hvis du vil være hacker.

Distribution

Jeg vil anbefale at du starter med en helt almindelig distribution, Fedora, Debian eller Ubuntu for at nævne nogle få. Med en almindelig distribution får du brug for at installerer programmer og konfigurere og den øvelse har du brug for til senere. Hvis du allerede er en erfaren Linux bruger kan du springe lige til BackTrack der er en decideret hacker distribution. Den finden pt. (sidst oktober 2008) i version 3 der kan være temmelig bøvlet at installerer som bund OS, da den er beregnet på at være en Live distribution. Den er på vej i version 4, der er bygget oven på en Debian distribution, og som bliver meget lettere at installerer, opdaterer og administrere

Virtuelt system.

Som virtuelt system bør du bruge VMWare, der kan downloades i en gratis version (VMWare server) Hvis du ikke har noget imod at betale, er VMWare workstation et lidt bedre valg da den kan mere. Du vil dog sagtens kunne klare dig med VMWare Server. Grunden til at vi bruger VMWare og ikke f.eks. Microsoft Virtuel server/Hyper-V er at alle de kurser og konferencer der findes bruger VMWare. Med Microsoft virtualisering vil du ikke kunne arbejde på kurser og konferencer og ikke kunne udveksle virtuelle maskiner og Virtual Appliances med andre hackere for de bruger alle VMWare.

Øvelser:

1. Start med google og slå alle de ord du ikke er helt sikker på op og læs. Forstå begreber som distribution og virtualisering. Læs om VMWare, fedora, ubuntu, debian og backtrack, forstå hvad forskellen er på de forskellige distributioner.

2. Installer en Linux distribution, enten som bund OS eller som en virtuel maskine. Lær at installerer applikationer som Nessus, Metasploit framework, Netwox og andre ting du måtte falde over som interessante. Lær dig at administrere din Linux maskine fra kommandolinien. Lær dig at bruge de mest almindelige kommandoer til at arbejde med fil systemet, netværk og andet nødvendige. Se f.eks. http://www.linuxbog.dk og kig på følgende kommandoer man applikationsnavn, grep, cp, chmod, ifconfig, dhcpd, mm. Kik også på editering af de forskellige conf filer som styre en Linux box.

3. Når du har dit bund OS klar, så installer VMWare Server eller workstation på maskinen og lær dig at oprette virtuelle maskiner, både som installerede operativ systemer og som startet fra ISO filer. Installer en typisk Linux som Fedora (ikke hvis du har den som bund OS allerede), installer en virtuel XP, installer Backtrack via ISO og senere på harddisken (kan faktisk downloades som # Virtual Appliances, Installer en Samurai (som ISO eller på HD) Installer en windows server, NT 4.0 eller en 2000 som du senere skal hacke.

4. Kig på dit (virtuelle) netværk, start flere maskiner op, kig på deres IP (ipconfig og ifconfig) oplysninger og se hvordan de er konfigureret. Forstå forskellen på når et virtuelt netkort er Bridged, NAT'ted eller Host only. Se om du kan pinge de forskellige maskiner fra hinanden.

5. Kig på at overføre filer mellem dine forskellige maskiner (ikke via cut and past som man faktisk kan hvis man installerer VMWare tools på sine virtuelle maskiner, for det kan du ikke når du hacker rigtigt) opsæt FTP servere på de forskellige maskiner (der findes masser af gratis versioner) og overfør filerne via kommandolinierne, du kan nemlig ikke bruge en FTP klient når du hacker. Opsæt SSH servere og tilgå via disse.

6. tag fat i google igen og se på de resterende af de begreber du ikke føler dig 100 % hjemme i.

Brug nu den tid der skal til, snyder du på vægtskålen vil det straffe dig senere når du skal hacke rigtigt. Hvis du ikke kan de mest almindelige ting, vil du ikke vide og dine problemer skyldes banale konfigurative og brugsrelaterede ting eller hackermæssige udfordringer. Den tid du investere her i starten vil du få tilbage med renters rente og investere du ikke nok vil du aldrig nå i mål nogen sinde. Du kan sagtens bruge år på disse øvelser, og heldigvis for dig vil de kommende lektioner også indeholde ting der rutinerer

dig i Linux Brug.

Kommentar af olebole d. 09. Nov 2008 | 1

Endnu en rigtig velskrevet artikel. Jeg må dog gentage mig selv fra kommentaren til den første artikel i serien: Jeg tror, nogen helt har misforstået noget. bufferzone har ganske klart defineret 'namespace' for denne artikelserie. Ovenikøbet så tydeligt, at selv de allertungeste burde evne at forstå, det for disse artiklers vedkommende ikke giver mening at diskutere 'cracker' kontra 'hacker' =)

Kommentar af psycosoft-funware d. 27. Oct 2008 | 2

fin atikkel. der er dog en væsentlig fejl i den;
her burde du ikke bruge ordet hacker. cracker ville være mere på sin plads, da der er himmels til forskel mellem disse to!
ordet hacker bliver i utroligt mange tilfælde brugt i forkerte sammenhænge.

Kommentar af shako d. 25. Oct 2008 | 3

God begynder-læsning. Jeg håber du kommer ind på den gigantisk store forskel mellem hackning og crackning på et tidspunkt.

Kommentar af gentlebug d. 26. Oct 2008 | 4

Kommentar af jape44 (nedlagt brugerprofil) d. 25. Oct 2008 | 5

Ok! Det var en fed læsning og rigtigt godt skrevet
Kommer der mere fra dig ?