Hackerbesøg, hvordan opdages de, og hvad gør du.

Hvordan opdager man at en hacker er inde eller på vej ind,? hvad gør man når han er inde?. Denne artikel besvare nogle af disse spørgemål.
Denne artikel er Windows specefik. En linux artikel er under overvejelse.

Skrevet den **06. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Hackerbesøg, hvordan opdages de, og hvad gør du.

Hvordan opdager at en hacker er på færde.
Du bør faktisk gribe denne opgave an på samme måde som man laver efterretningstjeneste i forsvaret. Det drejer sig om at opbygge et normalbillede, altså et billede af hvordan tingene er når der ikke er noget galt eller ikke sker noget unormalt. På denne måde kan du, hvis du er vågen og ser de rigtige steder, opdage når noget afviger. Udover normalbilledet, er der også en række værktøjer, du kan anvende som i hjælper dig med at opdage de mistænkelige ting.

1. Normalbilledet.
Her er hvad du skal have styr på, og hvad du skal kontrollere når du har mistanke om at noget er galt. Jeg vil anbefale at du dokumentere dine ting, ved udskrifter, gemte filer og screen dumps. Denne diciplin kaldes også Baselining og er meget vigtig til mange ting.

- Start med dine logfiler. Disse logfiler bør du kontrollere jævnligt, idet der er her du vil finde de første tegn på at noget er i gang. Du skal helst fange hackeren mens han arbejder på at komme ind, hvis han er god, vil han, når han først er inde, kunne slette disse logfiler, overskrive dem, eller måske modificere dem, så du ikke kan se hvad der er sket. Hvis han installere et såkaldt rootkit, er du prisgivet, og vil ikke kunne opdage ham direkte. En lægmandsforklaring på hvad et rootkit gør, er at det gør hackeren til et spøgelse. Du kan ikke se hans filer, biblioteker eller de processer han starter. Du vil lige som med spøgelset kun opdage den kolde luft når han er på dit net. Du kan se pladsen på dine drev forsvinder, men ikke se hvorfor. Du kan se at din båndbredde og din processor kraft bruges, men ikke af hvad. Kontroller din "Event Viewer" for underlige logon aktiviteter, services, der er fejlet eller mærkelige genstarter, og gem dine logfiler, e.v.t brændt ud på CD. Der kan sagtens gå noget tid før du opdager at noget er galt, så skal du kunne gå tilbage og se hvornår hvad er sket. Dette er også meget vigtigt hvis du vil anmelde noget til politiet.

MEGET VIGTIGT!!!!!!!

Sørg for at urene på dine systemer går rigtigt alle sammen. Brug gerne netværkstid (NTP), så de alle går ens og rigtigt. Dette er vigtigt hvis du vil anmelde, dine logfiler kan ikke bruges i en retssag hvid de går blot lidt forkert. Dine logfiler skal kunne sammenholdes med udbyders logfiler, og hvis det skal holde i retten, skal tiderne være sammenlignelige.

- Kontroller dine drev for mærkelige filer, eller om størrelsen af den frie plads pludselig er blevet mindre. Dette kræver at du holder øje med dit pladsforbrug på dine diske, og det bør du. Det drejer sig i det heletaget om at danne et normalbillede, så du opdagere ændringerne. Du vil under normale omstændigheder kunne finde gemte filer og mapper i stifinderen. *vælg Vis, Mappeindstillinger, Vis alle filer* . I MS DOS promt ses de gemte filer med kommandoen dir /ah.
Ligesom dine almindelige filer, bør du også holde øje med dine systemfiler. Du bør have overblik over

versionsnumre, servicepackniveau, build nummer og den slags. Hvis hackeren er god, vil han ofte lukke huller og patche dit system, for at sikre at der ikke kommer andre ind og ødelægger det han har gang i. Du kan bruge programmer som Host Based Intrusion Detection, f.eks. Tripwire, MD5 eller andre kryptografiske checksum værktøjer.

C:/drever kan især være svært at holde øje med, da størrelsen ofte variere afhængig af størrelsen af dine mailfiler og dine Internet temp filer. Her er det vigtigt, at du over tid holder øje med hvordan diskforbruget udvikler sig i takt med at du modtager mail, og surfer på nettet, på den måde har du en chance for at opdage hvis der sker noget unormalt.

- kontroller om der er opretter nye brugere eller grupper, specielt Administrator gruppen og superbrugere. Se også efter om der er nogle af de kendte brugere eller grupper der pludselig har fået flere rettigheder end de bør have. Kontroller også dine policies og se om der er ændret noget. Hvia du skal kunne dette, bør du dokumentere dine indstillinger, så du kan følge med i hvad der sker

- kontroller også dine shares, herunder især dine skjulte shares/systemshares. Dette kan du gøre med de indbyggede Windows værktøjer, eller bruger netbios scanneren Leviathan, Brug helst begge. Du bør undersøge alle former for shares. Både fil, diske og print, da de alle kan udnyttes.

- Kontroller om der er ændret rettigheder på filer eller registry Keys. Hvis du har styr på din konfiguration kan du bruge de indbyggede værktøjer til at identificere ændringer, og du kan bruge XCACLS.EXE der er en del af NT Resource Kit. Denne kan kontrollere mange filer på en gang.

- Kontroller hvilke processor der køre på din maskine. Dette kan du gøre med taskmanageren (jobliste) eller med værktøjer som HijackThis. Læs Anette Overgaards udmærkede artikel "*Sådan bruger du HijackThis og Spybot*" *(http://www.eksperten.dk/artikler/127)* eller få hjælp til at tyde logfilen på eksperten. Du bør lave en HijackThis logfil af din rene maskine, og printe den ud, så har du et grundlag for sammenligning. Du kan også anvende "pulist.exe" og "tlist.exe" kommandoerne fra "NT resource kit" . Begge programmer startes fra en kommandopromt, Pulist.exe viser dig hvem, der har startet den enkelte proces, tlist.exe -t vise dig hvilke processer, der startede hvilke underprocesser. Services vil oftest være startet af SYSTEM kontoen.

- Kontroller hvilke programmer der startes op når din Windows startes. Du kan kikke i C:\winnt\Users\Menuen Start\Programmer\Start mappen (husk både at kontrollere den lokale brugers mappe og " alle brugere" mappen). Se også under Start - Programmer - start for genveje til programmer der startes op

- Du er også nødt til at kontrollere din system- og netværkskonfigurationen for uautoriserede adgange. Kik på WINS, DNS og IP forwarding, f.eks. med Windows indbyggede værktøjer eller med "ipconfig /all" fra en kommando promt. En "netstat -an" fra samme promt, vil fortælle dig om din maskine lytter på porte den ikke bør lytte på. (I DK-CERTs portliste, kan du se hvilke typer, af hændelser de enkelte portnumre oftest udsættes for.)

- Kontroller om der er Schedulerede opgaver på din maskine, f,eks, bagdøre der er sat til at åbne på bestemte tidspunkter om natten. Dette kan gøres fra en kommandopromt med "AT" kommandoen eller med programmer WINAT fra "NT resource kittet

2. Værktøjer.
Der findes forskellige værktøjer der kan hjælpe en administrator med at opdage at der er noget galt. Vi har allerede behandlet Host Based Intrusion Detection systemer ovenfor. Der findes også Network Based Intrusion Detection systemer, der kikker på netværkstrafikken og sammenligner denne med en signatur database og på den måde kan opdage meget af det der foregår. Det er klart at et sådant system ikke er bedre end den database der følger med, og at den kun kan opdage kendte metoder. Du kan derfor ikke stole blindt på dit IDS, men bør altid tillægge din egen intelligens og overvågenhed.

- Et godt og gratis eksempel på et Network Based Intrusion Detection systemer er Snort, der kan downloades på http://www.snort.org. Dette glimrende system, er fuldt på højde de fleste købesystemer og følger faktisk med en del linux firewalls, f.eks. Smoothwall (http://www.smoothwall.org). Husk at gemme logfilerne på et medie der ikke kan ændres af en hacker, f.eks en CD'rom eller på et offline system. Firewallen er også et værktøj du bør anvende til at opdage ting og sager. En firewall er et aktivt stykke værktøj. Du kan ikke bare tage den i drift, og så håbe på at den standser alt. Faktisk kan firewalls relativt let omgås/gennembrydes, hvis du har sårbarheder i dit system. Du skal derfor jævnligt kontrollere din firewall log, du skal gemme din firewall log på et sikkert medie, og så skal du reagere på de ting i loggen du ikke kan forklare.
Hvis du har en firewall funktionalitet i din router, bør den være slået til, så du på den måde skaber dybde i dit forsvar. Brug routerens firewall som første filter, der fanger alt skidtet, på den måde bliver det lettere at læse den rigtige firewalls logfil.

3. Angrebet er sket, hvad gør jeg.
Afhængig af hvad der er sket, drejer det sig i første omgang om at stoppe ulykken. I dette tilfælde vil det sige at afbryde Internetforbindelsen, hvis det overhoved kan lade sig gøre.

> Nogle virksomheder kan ikke gøre dette uden at konkurs. Disse virksomheder bør med det samme tilkalde eksperter og politiet.

Herefter bør du tage fat i damage control. Ikke alle, og slet ikke firmaer, vil finde dette naturligt, nogle vil oven i købet mene at det er en dårlig ide. Min holdning er dog, at du opnår mest ved ærligt at melde ud. Start med at kontakt din udbyder, og fortæl hvad du ved. Prøv derefter at identificere om hackeren har haft fat i andre fra din maskine, og kontakt dem med det samme. Nogle, især firmaer, vil forsøge at hemmeligholde, at der er sket noget sådant, bliver det opdaget, og det gør det normalt altid, vil de negative effekter ramme dig meget hårdere en hvis du ærligt har meldt ud

Næste trin er at finde ud af hvad der er sket. Alle logfiler skal gennemgås nøje, alle de ting der er nævnt i punkt 1, skal undersøges med en lup. Undersøg om der er kendte huller i dine systemer. Dette kan du f.eks. gøre på http://www.securityfocus.com/bid, ligesom du kan søge hjælp både til at tolke logfil entries som huller på Bugtraq, der er en mailingliste du finder på Securityfocus.com. Denne mailingliste er også stedet hvor nye sårbarheder og angrebs signaturer først meldes.

Beslut om du vil anmelde, Min anbefaling er at du som minimum kontakter politiet og lader dem afgøre om der er noget at komme efter. Hvis du anmelder, er der en chance for at han stoppes før andre skades. Undlader du at anmelde, risikere du dels at han går efter dig igen og dels at du kommer til at være medvirkende til tab hos andre, med mulig erstatning og sagsanlæg til følge.

Når du ved hvad der er sket, ved du også hvordan du skal stoppe hullet. Ofte vil en formatering og efterfølgende reinstallation være den eneste metode til at sikre at hackeren er helt ude af dit system. Hvis han har placeret et rootkit, er formatering og reinstallation ENESTE metode til at sikre at han er ude. Når du skal opdatere dit system over nettet, så bør du gøre det fra en anden IP adresse end den du plejer at bruge. Det tager ganske få minutter for en hacker at komme ind, og du kan ikke opdatere så hurtigt. Hvis han overvåger din IP adresse, vil han kunne generobre dit system før du får opdateret igen. Tag nye teknologier i brug efter angrebet. Efter et angreb, vil du altid være lidt paranoid. Spørgsmålet er om du er paranoid nok. Du bør selvfølgelig lukke alle huller, men også overveje at tage nogle at de teknologier der findes til hjælp. Jeg tænker her på. IDS (Host og network based), Firewalls, Kryptering, osv osv.

Du er naturligvis altid velkommen til at spørge her på eksperten, ligesom du kan kontakte mig på kim@bufferzone.dk med kommentarer, rettelser og spørgsmål. Undlad venligst at stille spørgsmål i dine kommentare, dem kan jeg jo ikke besvare

Kommentar af janbb d. 31. Jan 2004 | 1

Giver lidt 'indblik' for een som mig der ved meget lidt om emnet, men virker temmelig ustruktureret i opbygningen og jeg føler ikke det giver - overbik.

Kommentar af limemedia d. 28. Jan 2004 | 2

Titel er lettere misvisende - jeg søgte mere generel information hvor denne er mere minded mod Windows.

Kommentar af tahoo d. 20. Jan 2006 | 3

ok

Kommentar af iphase d. 21. Jan 2005 | 4

Kommentar af resten d. 03. Mar 2004 | 5

Ganske god artikel Kim har lavet der :)

Kommentar af cf560 d. 25. Nov 2006 | 6

Kommentar af lenk d. 10. Mar 2004 | 7

Der er mange ting at holde styr på. Gode teknikker og fornuftige råd

Kommentar af cronck d. 16. Jul 2004 | 8

Særdeles god artikel!

Kommentar af stoltenborg d. 05. Aug 2004 | 9

Kommentar af susanne_larsen d. 30. Jan 2004 | 10

Meget interessant, lærerig og uddybende.
Syntes dog du mangler link til flg. sider: http://www.ripe.net/ og http://www.politi.dk/itkrim/forside.htm samt hvad man kan bruge dem til.
I nogen tilfælde kan man "nøjes" med at anmelde direkte til udbyder - lidt info om dette kunne være godt.
Der er også stor forkel på hvordan de forskellige udbydere vil have mails skal se ud når man anmelder direkte til udbyder. Savner lidt en beskrivelse af dette. Ex. generelle retningslinier for hvilke info man skal kopiere ind. Ofte er de jo fx. ikke interesserede i vedhæftede filer ;)

Så lidt info om ovenstående og betragt min rating som opgraderet ;)

Kommentar af kbhadsten d. 27. Jun 2005 | 11

Gennemført!

Kommentar af babysus85 d. 02. Dec 2006 | 12

Forvirrende for newbies

Kommentar af dreamless d. 01. Dec 2005 | 13

God artikel, lidt for rodet og med små stavefejl, men kun et lille kosmetisk "hak" i den gode tekst :)

Kommentar af serverservice d. 16. Aug 2005 | 14

Godt arbejde og mange brugbare kommandoer er beskrevet- kun få steder kunne man ønske lidt mere om hvordan man gør i praksis - derfor fuld valuta herfra.

Kommentar af kalsmose d. 23. Jan 2005 | 15

Sådan :)

Kommentar af khalus d. 05. Dec 2005 | 16

Kommentar af countermads d. 05. Nov 2006 | 17

fin artikel

Kommentar af ird d. 12. Apr 2004 | 18

Meget oplysende og godt fortalt artikel.
Helt sikkert point og tid værd.

//Ird

Kommentar af themom d. 01. Dec 2005 | 19

Selv jeg fik noget ud af det ;) themom

Kommentar af mushkin d. 12. Jul 2004 | 20

God artikel, ikke relevant for mig personligt. Men fik alligevel en del ud af det.

Kommentar af nimb85 d. 17. Jul 2004 | 21

Kommentar af forevernewbie d. 09. Aug 2004 | 22

Bufferzone ved jo hvad han taler om, og man er klogere efter at have læst artiklen. Den "almindelige" bruger kan måske stå lidt af undervejs, men ellers super./forevernewbie.

Kommentar af knejt d. 15. Nov 2004 | 23

Ganske god artikel du har fået skrevet dig der..
mvh Knejt

Kommentar af joejjoej d. 03. Jul 2005 | 24

Kommentar af st3ff d. 04. Apr 2006 | 25

God artikel, en smule forvirrende men ellers udemærket