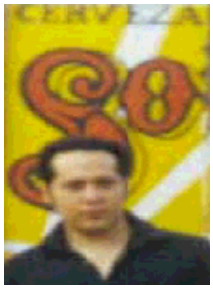
LinuxFocus article number 274
http://linuxfocus.org



door José Salvador González Rivera
<jsgr(at)tec.com.mx>

Over de auteur:

José Salvador González Rivera is een actief lid van de Linux Gebruikers groep van Puelba (Mexico). Hij is vaak betrokken bij evenementen om Free Software, en met name Linux, te promoten. Hij heeft zojuist een graad behaald in Computer Systems. Je kunt met hem in contact komen op jsgr(at)tec.com.mx of op jsgr(at)linuxpuebla.org.

Inbraakdetectie met Debian GNU/Linux

Kort:

Vandaag de dag is de meeste informatie digitaal opgeslagen, en daardoor eenvoudiger te benaderen met behulp van computernetwerken. Deze staan ons toe om 'remote' data te verkrijgen, of het nu financieel, administratief, militair, industrieel of commercieel is. Helaas vormt deze data een makkelijk doelwit voor mensen met slechte bedoelingen, die het willen inkijken of vernietigen, mensen die nog nooit van moreel gedrag hebben gehoord.

Aan het gebrek aan geweten kunnen we maar weinig doen. In dit korte artikel zal ik een techniek en de gereedschappen laten zien die we kunnen gebruiken onder Debian GNU/Linux om de aanvallers op te merken en te traceren. Ik zal niet de inhoud van de gebruikershandleidingen reproduceren, maar ik zal focussen op wat kan gebeuren in het 'echte' leven.

Vertaald naar het Nederlands door:
Guus Snijders
<ghs(at)linuxfocus.org>

Introductie

Bij het selecteren van een Linux besturingssysteem moeten we de vele beschikbare distributies bekijken. De meeste zijn gebaseerd op RedHat; bijvoorbeeld Connectiva (Brazilië), Hispa source (Spanje), Mandrake (Frankrijk), SuSe (Duitsland), Caldera en vele anderen gebruiken de RPM package manager. Ook is er Slackware, welke probeert dichter bij de traditionele Unixen te blijven met gebruik van .tgz

archieven. "Bijna" allemaal worden ze ontwikkeld door commerciële bedrijven, maar dit geldt niet voor Debian. Debian komt met een package manager (DPKG) welke zeer behulpzaam is bij het updaten en zo het systeembeheer vereenvoudigt, en een systeem toelaat up-to-date te blijven voor wat betreft de veiligheids patches.

Waarom Debian GNU/Linux ?

Debian heeft een aantal belangrijke features:

1) Het heeft geen commercieel oogmerk en volgt dus niet blindelings de grillen van markt.
2) Het heeft een goed systeem om bugs te volgen, en problemen worden opgelost in minder dan 48 uur.
3) Vanaf het begin heeft het ontwikkelen van een compleet en betrouwbaar besturingssyteem de hoogste prioriteit gehad.
4) Het wordt ontwikkeld door vrijwilligers van over de hele wereld.

Iedere nieuwe versie levert nieuwe hardware (architectuur) ondersteuning; op het moment is er ondersteuning voor: Alpha, ARM, HP PA-RISC, Intel x86, Intel IA-64, Motorola 680x0, MIPS, MIPS (DEC), Power PC, IBM S/390, Sun Sparc - aan Sun UltraSparc en Hitachi SuperH wordt gewerkt. Het is het Linux systeem met het grootste aantal ondersteunde platformen.

Onder de bestaande Debian packages zijn er aantal realtime inbraakdetectie tools die vijandelijk gedrag tijdens een connectie kunnen detecteren. Er bestaan twee types: degene die een pogingen tot aanvallen op een netwerk in de gaten houden en degene die specifiek host gedrag in de gaten houden.

Host tools

We gebruiken PortSentry om poortscans te detecteren, TripWire om systeemveranderingen te detecteren en LogSentry voor de analyse van de logs. De eerste en de laatse zijn onderdeel van de TriSentry suite van Psionic Technologies.

Poortscan detectie

PortSentry monitort de poorten van ons systeem en voert een actie uit (meestal een blokkade) als het een poging tot een connectie ziet naar een poort waarvan we niet willen dat er naar geluisterd wordt.

De homepage is op http://www.psionic.com/products/portsentry.html en PortSentry is beschikbaar voor Solaris, BSD, AIX, SCO, Digital Unix, HP-UX en Linux.

Onder Debian kan het geïnstalleerd worden met het volgende commando:

apt-get install portsentry

Er kunnen verschillende activiteitsniveaus worden geselecteerd, de stealth mode en de advanced (geavanceerde) mode. De configuratie gebeurt in het bestand /usr/local/psionic/portsentry/portsentry.conf .

De belangrijkste opties heb ik gevonden in een artikel van José Torres Luque in ES Linux Magazine en zijn als volgt:

TCP_PORTS, hier definieer je de poorten die gecontroleerd moeten worden in classic mode of in stealth mode. De auteur geeft drie poortlijsten, afhankelijk van het gevoeligheidsniveau dat je wilt toepassen. Het maximale aantal poorten is 64.

UDP_PORTS, net als de vorige, maar dan voor UDP poorten.

ADVANCED_PORTS_TCP, ADVANCED_PORTS_UDP, geeft het hoogste poortnummer aan om te gebruiken in de advanced mode. Iedere poort lager dan deze waarde zal worden gecheckt, behalve degenen die reeds waren uitgezonderd. Het maximum is 65535. Het wordt echter aangeraden om niet boven de 1024 te gaan om valse alarms tegen te gaan.

ADVANCED_EXCLUDE_TCP, ADVANCED_EXCLUDE_UDP, geeft een lijst van genegeerde poorten. De poorten die hier gevonden worden zullen niet gemonitord worden in de advanced mode. Hier geef je de lijst op van poorten die normaal gesproken worden toegewezen aan remote clients en degene die niet een echte service zijn, zoals bijvoorbeeld ident.

IGNORE_FILE, hier geven we het bestand op met de IP adressen die genegeerd moeten worden tijdens het monitoren. De locale interface, inclusief lo zou hier ook in moeten staan. Ook kun je hier de lokale IP adressen opgeven.

KILL_ROUTE, hier geef je het commando op dat moet worden uitgevoerd om de aanvallende host te blokkeren. Bijvoorbeeld: iptables -I INPUT -s $TARGET$ -j DROP waarbij $TARGET$ verwijst naar de host van de aanvaller.

KILL_RUN_CMD, duidt een commando aan dat uitgevoerd dient te worden alvorens de host te blokkeren.

SCAN_TRIGGER, definieert het aantal pogingen voordat het alarm wordt geactiveerd.

PORT_BANNER, geeft een bericht weer op de open poorten in connect mode.

Eenmaal geconfigureerd, moet het worden gestart in een van de drie modi met behulp van de volgende opties: voor TCP is er -tcp (basic mode), -stcp (stealth mode) en -atcp (advanced mode); voor UDP is er -udp, -sudp, -audp.

Integriteits analyse

Met TripWire kunnen we de intregriteit van het bestandssysteem controleren; de homepage is te vinden

op http://www.tripwire.org en het is vrijelijk beschikbaar voor Linux en commercieel voor Windows NT, Solaris, AIX en HP-UX.

Op Debian kan het geïnstalleerd worden met:

apt-get install tripwire

Om de informatie op te slaan zijn er twee sleutels nodig, de "site key" wordt gebruikt om het beleid en configuratie bestanden te versleutelen, de "local key" wordt gebruikt om de informatie met betrekking tot de gemonitorde bestanden te versleutelen.

De configuratie kan eenvoudig worden gedaan in het /etc/tripwrie/twpol.txt bestand en als het eenmaal is aangepast, kun je het "installeren" met:

twadmin -m P /etc/tripwire/twpol.txt

Om de initiële database te creëeren, welke de huidige status van de bestanden bevat, gebruiken we het commando:

tripwire -m i 2

Om de integriteit van het bestandssyteem te controleren, gebruiken we het commando:

tripwire -m c

Het configuratiebestand kan worden verwijderd om te voorkomen dat een inbreker weet welke bestanden gewijzigd zijn, met het commando:

rm /etc/tripwire/twcfg.txt /etc/tripwire/twpol.txt

Om ze opnieuw te creëeren indien nodig, gebruik je het volgende:

twadmin -m p > /etc/tripwire/twpol1.txt twadmin -m f > /etc/tripwire/twcfg.txt

Log analyse

LogCheck is onderdeel van LogSentry en staat toe om de logs op een zeer efficiënte manier te analyseren, daar het klassificeert en rapporteert over activiteiten en fouten die gelezen moeten worden. Er zijn 4 verschillende niveau’s van loggen: ignore (negerend), unusual activity (ongebruikelijke activiteit), violation of security (beveiligings doorbraken) en attack (aanval).

De home page is op http://www.psionic.com/products/logsentry.html. Het is beschikbaar voor Solaris, BSD, HP-UX en Linux.

De installatie onder Debian kan met:

apt-get install logcheck

Dit installeert het logtail programma in /usr/local/bin om een lijst bij te houden van reeds geanalyseerde logs. De volgende bestanden worden ook geïnstalleerd:

Logcheck.sh,
Een script met de basis configuratie.

Logcheck.hacking,
Bevat de regels die de activiteits regels definiëren.

Logcheck.ignore,
Bevat de expressies om te negeren.

Logcheck.violations,
Bevat expressies die worden gezien als doorbraken van de beveiliging.

Logcheck.violations.ignore,
De expressies in dit bestand zijn bedoeld om genegeerd te worden.

Je kunt gebruik maken van cron om logcheck ieder uur te draaien:

0 * * * * /bin/sh /usr/local/etc/logcheck.sh

Netwerk tools

We gebruiken Snort om pogingen tot aanvallen over het netwerk op te merken. De homepage kan hier gevonden worden: http://www.snort.org en Snort is beschikbaar voor BSD, Solaris, AIX, Irix, Windows, MacOs X en Linux.
De installatie onder Debian gaat met het volgende commando:

apt-get install snort

Het werkt in drie verschillende modi: sniffer, packet logger en intrusion detector.

Het kan gebruik maken van de volgende parameters:

-l directory
geeft aan in welke directory de bestanden moeten worden opgeslagen.

-h IP
geeft het IP adres aan dat we willen controleren.

-b
vangt ieder pakket op als binary.

-r file
bewerkt een binair bestand.

Snort Sniffer en Packet Logger modi

In de sniffer mode leest Snort het ieder pakket dat in het netwerk circuleert en geeft ze weer op de console terwijl in packet logger mode de data naar een bestand in een directory wordt gestuurd.

Snort -v

Geeft IP en headers weer.

Snort -dv

Geeft ook de circulerende data weer.

Snort -dev

Een meer gedetailleerde manier.

Snort Inbraak Detectie mode

In deze mode informeert Snort ons over portscans, DoS (Denial of Service) aanvallen, exploits, etc. Een en ander is afhankelijk van de regels in /usr/local/share/snort die je kunt downloaden vanaf de website - de server past ze ongeveer ieder uur aan.

De configuratie is heel eenvoudig daar deze bestaat uit het maken van veranderingen in het snort.conf bestand, waar we onze netwerkdetails en werkdirectories opgeven. Verander het IP:

var HOME_NET IP

Om snort te starten, typ:

snort -c snort.conf

De logbestanden worden opgeslagen in /var/log/snort waar we de IPs van de aanvallers kunnen zien. Dit is natuurlijk een heel korte bespreking van wat je kunt doen met met snort en ik raad aan om er meer over te lezen. De meeste organisaties, tijdschriften en beveiligingsgroepen zien Snort als het beste Intrusion Detection System (IDS, inbraak detectie systeem) voor de Unix en Windows platformen en raden het aan. Er is commerciële ondersteuning van bedrijfen zoals Silicon Defense en Source Fire en GUIs (Graphical User Interface, grafische gebruikers interface) beginnen te verschijnen om een aantrekkelijker presentatie van de resultaten te leveren.

Soms vereisen noodsituaties een diepere analyse omdat er onverwachte problemen zijn die onmiddelijk

opgelost dienen te worden.

Deze problemen worden meestal veroorzaakt door mensen met slechte bedoelingen of inbrekers die proberen onze servers te benaderen om wat voor reden dan ook, of het nu om het stelen of het aanpassen van je data gaat, om andere systemen van ons aan te vallen, of om een sniffer of een rootkit te installeren, welke tools zijn om meer privileges te krijgen op elk systeem.

Andere nuttige tools

Sniffer detectie

Een sniffer is een tool die de netwerk interface in promiscue mode zet met de bedoeling om het volledige netwerkverkeer af te luisteren. Het ifconfig commando levert ons de volledige informatie over de netwerk interface:

```
eth0 Link encap:Ethernet HWaddr 00:50:BF:1C:41:59
inet addr:10.45.202.145 Bcast:255.255.255.255 Mask:255.255.128.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:7180 errors:0 dropped:0 overruns:0 frame:0
TX packets:4774 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:8122437 (7.7 MiB) TX bytes:294607 (287.7 KiB)
Interrupt:10 Base address:0xc000
```

Echter, als het ifconfig commando omgewisseld is of als de sniffer op een andere machine in het netwerk draait, zul je de connecties van buitenaf moeten controleren, zoals het versturen van mail naar "vreemde" accounts of de logs van de sniffer detecteren.

Er bestaat een tool met de naam neped, ontwikkeld door een Spaanse hackers groep, welke ons informeert over interfaces in ons netwerk die in zich in de promiscuous mode bevinden. Het is geen onderdeel van Debian, maar kan gedownload worden van
ftp://apostols.org/AposTools/snapshots/neped/neped.c
Opmerking: deze server lijkt een paar weken plat te zijn geweest.

De uitvoering van het programma levert een resultaat op als het volgende:

```
neped eth0
-----------------------------------------------------
> My HW Addr: 00:80:F6:C2:0E:2A
> My IP Addr: 192.168.0.1
> My NETMASK: 255.255.255.0
> My BROADCAST: 192.168.1.255
-----------------------------------------------------
```

Scanning ....
* Host 192.168.0.2, 00:C2:0F:64:08:FF **** Promiscuous mode detected !!!
End.

Om een IP pakket van 191.168.0.1 naar 192.168.0.2 te sturen, moeten we zijn MAC adres weten. Dit doen we door een broadcast packet te sturen naar het netwerk, welke vraagt naar het MAC adres van het gespecificeerde IP: alle machines krijgen het verzoek, maar alleen de juiste host is degene die antwoord geeft.

In dit geval vraagt neped elk netwerk IP, echter, het stuurt geen broadcast maar gebruikt in plaats daarvan een niet-bestaand IP adres als doel. Alleen de hosts met hun interface in promiscuous mode zullen antwoorden, daar zij de enige zijn die in staat zijn om deze pakketten te lezen.

Ik ontdekte dit programma in een artikel over het detecteren van spionnen, welke ik op het net vond. Het gaf een vergelijkbaar voorbeeld. Als jij de URL weet van dit artikel, voel je vrij om het naar mij te sturen per mail, daar ik hem kwijt ben :-)

Rootkits detecteren

De rootkits leveren een manier om meer privileges te verkrijgen dan een normale gebruiker kan hebben. Meestal vervangen ze de systeem binaries met andere versies om later toegang tot het systeem te verkrijgen. Dit is waarom we moeten controleren of we nog steeds de originele versies hebben met behulp van chkrootkit. De installatie gaat zo:

apt-get install chkrootkit

De website is op www.chkrootkit.org en het controleert de volgende bestanden:

aliens, asp, bindshell, lkm, rexedcs, sniffer, wted, z2, amd, basename, biff, chfn, chsh, cron, date, du, dirname, echo, egrep, env, find, fingerd, gpm, grep, hdparm, su, ifconfig, inetd, inetdconf, identd, killall, ldsopreload, login, ls, lsof, mail, mingetty, netstat, named, passwd, pidof, pop2, pop3, ps, pstree, rpcinfo, rlogind, rshd, slogin, sendmail, sshd, syslogd, tar, tcpd, top, telnetd, timed, traceroute, w, write

Om het te gebruiken, typ:

chkrootkit

Het checkt de bestanden en zoekt naar bekende sniffers en rootkits. Er zijn andere tools om veranderingen aan logbestanden te controleren (chkwtmp en chklastlog) en ook ifpromisc om ons te vertellen of onze netwerk interface zich in promiscuous mode bevindt.

Referenties

Het wordt aangeraden om de man pagina's van deze programma's te lezen. Ik geef je een paar referenties die ik zelf heb gebruikt. Voel je alsjeblieft vrij om me suggesties en commentaar te sturen op mijn email adres.

- Alexander Reelsen, Securing Debian How To, versie 1.4, 18 February 2001
- Anónimo, Linux Máxima Seguridad, Pearson Educación, Madrid 2000
- Brian Hatch, Hackers in Linux, Mc Graw Hill 2001
- Jim Mellander, A Stealthy Sniffer Detector, Network Security
- Antonio Villalón Huerta, Seguridad en Unix y redes, Open Publication License, octubre 2000
- CSI FBI Computer Crime and Security Survey, CSI Issues&Trends, Vol.7
- Who's Sniffing Your Network?, www.linuxsecurity.com/articles/intrusion_detection_article-798.html
- Root-kits and integrity: Het November 2002 artikel van Linuxfocus

---

Site onderhouden door het LinuxFocus editors team © José Salvador González Rivera "some rights reserved" see linuxfocus.org/license/ http://www.LinuxFocus.org	Vertaling info: es --> -- : José Salvador González Rivera <jsgr(at)tec.com.mx> es --> en: Georges Tarbouriech <gt(at)linuxfocus.org> en --> nl: Guus Snijders <ghs(at)linuxfocus.org>

2005-01-14, generated by lfparser_pdf version 2.51