LinuxFocus article number 245
http://linuxfocus.org

Een heterogeen netwerk beveiligen met Free Software gereedschappen

door Georges Tarbouriech
<georges.t(at)linuxfocus.org>

Over de auteur:

Georges gebruikt al heel lang Unix. Hij bedankt de Free Software gemeenschap voor de vele geweldige gereedschappen die ze ontwikkelen.

Vertaald naar het Nederlands door:
Hendrik-Jan Heins
<hjh/at/passys.nl>

Kort:

Dit artikel is eerder gepubliceerd in een Linux Magazine France speciale editie over beveiliging. De redacteur, de auteurs en de vertalers waren zo vriendelijk om LinuxFocus toestemming te geven alle artikelen van deze speciale editie te publiceren. Nu brengt LinuxFocus deze artikelen zodra ze in het Engels vertaald zijn. Dank an alle mensen die betrokken zijn bij dit werk. Deze samenvtting wordt voor ieder artikel uit deze bron geplaatst.

Inleiding

Veiligheid in computernetwerken is waarschijnlijk één van de grootste technische uitdagingen van de 21e eeuw.
Echter geldt, zoals voor zoveel probleemgebieden, dat iedereen erover praat, maar degenen die er het meeste mee te maken hebben schijnen nog niet op de hoogte te zijn van de schaal waarop het mogelijk fout kan gaan. De "direct betrokkenen" zijn natuurlijk de grote software- en systeemontwikkelaars. Het beste voorbeeld hiervan komt uit Redmond, waar het woord "beveiliging" door veel minder mensen begrepen wordt dan het woord "marketing".
Gelukkig is in de laatste twintig jaar van de 20e eeuw de "Vrije Software" geboren, met een opmerkelijke filosofie. Als je de beveiliging van je machines, je systemen, je netwerken "wil" verbeteren... dan moet je in deze richting kijken. De Free Software gemeenschap heeft meer gedaan aan

beveiliging dan alle grote software bedrijven tezamen.
Nu dit opgehelderd is; de juist gereedschappen hebben *op zich* is niet voldoende en het beveiligen van bijvoorbeeld een netwerk is een taak die continu om aandacht vraagt: er is altijd wel iets dat verandert! Dit betekent dat je nooit kunt zeggen dat een netwerk 100% veilig is. Je kan de risico's alleen verkleinen. Wat we hier laten zien is daar slechts een klein deel van. Na het lezen van deze speciale editie (opmerking van de auteur: denk er aan, dit artikel was onderdeel van een Linux Magazine France speciale editie over beveiliging), weet je een beetje meer over beveiliging, maar je kan absoluut nog niet zeggen dat je netwerk veilig is. Tot zover de waarschuwing.
Tenslotte: een artikel als dit kan niet compleet zijn. Er is veel leesvoer over dit onderwerp te vinden en dan nog is alles nog lang niet beschreven. Verwacht dan ook niet dat dit artikel alles noemt over besturingssystemen, gereedschappen, configuraties, gebruik... enz.
Aan het einde van deze inleiding, de opmerking dat sommige delen van dit artikel onteend zijn aan LinuxFocus, dit is gebeurd met instemming van de auteur: hij en ik zijn dezelfde...

Presentatie

Allereerst gaan we praten over de structuur ven een zeer gemengd (heterogeen) netwerk, dat veel verschillende soorten systemen bevat. Hoe meer besturingssystemen, hoe lastiger en complexer, aangezien niet alle systemen hetzelfde reageren op problemen. Bovendien hebben de machines die in het netwerk als server worden ingezet een andere functie: we hebben een 'gediversifieerd' netwerk.
Daarna bekijken we enkele gereedschappen die essentieel zijn, willen we de veiligheid verbeteren. De keuzes zijn arbitrair: er worden te veel keuzes gemaakt om ze allemaal expliciet te noemen. We gaan uitleggen hoe machines en netwerken met deze gereedschappen beveiligd kunnen worden. In het volgende hoofdstuk gaan we de beveiligingsmogelijkheden van verschillende systemen bekijken.
De conclusie wordt gebruikt om de "relativiteit" van de beveiligingsprocessen uit te leggen en om de reden achter de methodes te laten zien zonder in te gaan op toekomstige ontwikkelingen.

Voorbeeld van een heterogeen netwerk

Als eerste een voordeel: Het TCP/IP protocol wordt door alle bestande besturingssystemen "gesproken". Hierdoor kunnen totaal verschillende systemen toch met elkaar communiceren. Dus in het netwerk dat we voor dit voorbeeld gebruiken, zal TCP/IP altijd aanwezig zijn. We gaan dus niet in op de protocollen, niet de bekende en ook niet de minder bekende. We gaan ook niet in op de fysieke structuur, dus het type verbinding, de categorie enz..., van het netwerk.
In dit netwerk gaat dus van alles een beetje. Natuurlijk is er een Unix, gelicenseerd of gratis: bijvoorbeeld een drupje Solaris 2.6, of SunOS 5.6, als je dat liever hebt, een drupje Irix 6.5, Linux (RH 6.2), MacOS X. We hadden ook wat QNX of NeXTSTEP, of NetBSD of OpenBSD kunnen toevoegen. Aan de "conventionele" zijde voegen we de enige echte, eenzame en niet afgewerkte (*N*ot *T*erminated) 4.0 (nee, niets anders, die zijn erger). Ook hier hadden we OS2 kunnen toevoegen, dat minder erg is. En tenslotte voegen we nog een drupje "onconventioneel", laten we zeggen BeOS en AmigaOS (ja, het bestaat ... hoewel het niet veel voorkomt!) toe.
Natuurlijk klagen enkelen van jullie nu al: wat, geen AIX, geen HP-UX ? Nee! Als we alle soorten Unix zouden gaan opnoemen, zou het artikel tien volumes beslaan. De fundamentele beveiligingsregels

gelden voor alle systemen.

Wat zullen we ze nu eens vragen?
Laten we Solaris in dit geval eens een applicatie server maken. Irix beheert de backups. NT is een andere applicatie server. Linux is een gateway. Een andere Linux machine is een http server of een database server. Alle andere machines zijn clients. We gaan er vanuit dat dit netwerk ongeveer 30 machines bevat die gebruik maken van een autorisatie via een wachtwoord bestand. We hadden een geavanceerdere oplossing kunnen kiezen: NIS (Yellow Pages), of LDAP, of Kerberos... Laten we het eenvoudig houden. We maken ook geen gebruik van NFS. Hoewel het een handig systeem is, kan je het beter vergeten, omdat het, ondanks de verbeteringen, op beveiligingsgebied een probleem is. In Frankrijk zeiden oude mensen vroeger: "verzamel niet al je koeien in dezelfde stal". Zorg er dus voor dat "onveilige" maar noodzakelijke services en protocollen slechts één maal gebruikt worden, en dan speciaal op machines die nergens anders voor gebruikt worden. Dus bijvoorbeeld slechts een ftp server, een http server, en dan liefst op Unix machines. Enkele Unix machines worden SSH server en de anderen worden SSH clients. Hierover later meer. We gaan gebruik maken van statische IP adressen: geen DHCP. Het blijft dus eenvoudig! Dit kan natuurlijk ook worden toegepast op een netwerk met 50 machines; met nog meer machines kan het een nachtmerrie worden.

De gereedschappen en hoe ze gebruikt moeten worden

Zoals gewoonlijk is er meer dan een manier om dit voor elkaar te krijgen (TIMTOWDI). In het ideale geval start je zonder randvoorwaarden met lege machines en een nog op te zetten netwerk. Helaas gebeurt dit alleen in films! Laten we daaril eens kijken naar een netwerk dat door de tijd heen gegroeid is, met machines die van de ene plaats naar de andere verhuizen, nieuwe aanwinsten enz. Bijvoorbeeld door de Mhz "race", gaan de huidige Intel machines niet lang mee. Na ongeveer 3 jaar wordt het lastig om nog onderdelen te vinden. Dus de keuze is óf het recycleren van machines voor eenvoudige taken, óf ze weggooien. Helaas maar waar! Gelukkig gaan sommige machines langer mee en kunnen ze verder worden uitgebreid en verbeterd. Ga er niet vanuit dat dit niets met het onderwerp te maken heeft: een beheerder moet aan een hoge beschikbaarheid van machines werken.

De Basics

We kunnen "generaliseren" de eerste stap van de taak noemen. Het bestaat uit het verwijderen van alle waardeloze software van iedere machine - dat is geen "eenvoudige" taak! Ieder besturingssysteem, inclusief Unix, installeert een ongelofelijke hoeveelheid services en protocollen die je nooit zal gebruiken. Het credo is hier: gooi ze weg! Bij Unix is een eenvoudige en grove manier het "uitcommentariëren" van alles in/etc/xinetd.conf. Dat zijn een boel services minder. Dit is natuurlijk een beetje overdreven, maar op veel machines is dit absoluut mogelijk. Het is afhankelijk van wat je nodig hebt. Bij Linux en enkele andere besturingssystemen kan je ook het *chkconfig* commando gebruiken om enkele services uit te zetten.
Controleer ook de SUID/SGID bestanden en aarzel niet om de "foute" bit te veranderen, of zelfs het hele programma te deactiveren. Een commando als *find / -user root -a \(-perm -4000 -o -perm -2000 \) -print* geeft je een lijst van dit soort bestanden. Typ, om het "s" bit te verwijderen *chmod a-s programname* (opmerking: natuurlijk raak je wat functionaliteit kwijt door het verwijderen van de "s" bit. Het heeft immers een doel...).
Verwijder "gevaarlijke" programma’s en degenen die bekend staan als "risico gevallen": de

commando’s voor werk op afstand zoals rsh, rlogin, rcp... bijvoorbeeld. SSH is een zeer goede vervanger voor ze.
Controleer de rechten voor directories zoals /etc, /var... Hoe meer dichtgetimmerd hoe beter. Een commando als *chmod -R 700* op de directory met de opstartbestanden (/etc/rc.d/init.d bij veel Unixes) bijvoorbeeld, is geen slecht idee. Hetzelfde geldt voor alle systemen die deel uitmaken van het netwerk: verwijder dat wat je niet gebruikt, of deactiveer het op z’n minst. Stop bij NT bijvoorbeeld zoveel mogelijk services via het configuratiescherm. Er zijn veel eenvoudige "dingen" te doen en er is veel literatuur over het onderwerp te vinden.

De Gereedschappen

Laten we beginnen met Unix, aangezien dat de enige is die echt is gebouwd om rekening te houden met systeembeveiliging. Nu is er een grote hoeveelheid gratis gereedschappen te verkrijgen en de meeste daarvan werken op vrijwel iedere Unix variant.

Voor nu beperken we ons tot de individuele machines, aangezien het beveiligen van een netwerk betekent dat voor alles, de elementen beveiligd moeten zijn. Het installeren van deze gereedschappen is vrij eenvoudig, en daarom leggen we er niets over uit. De instellingen zijn ook afhankelijk van de systemen, de eisen... Het hangt van jou af hoe dit in jouw geval wordt toegepast. Het eerste benodigde gereedschap heet *shadow utils*. Het is een versleutelingsmethode voor wachtwoorden. Gelukkig is het onderdeel van veel Unix distributies. Het /etc/shadow bestand wordt nu "gemaakt" uit /etc/passwd.

Nog beter is *PAM* (Pluggable Authentication Modules) die het mogelijk maken om gebruikerstoegang te beperken per service. Alles wordt beheerd vanuit de directory die de configuratiebestanden van de betreffende service bevat, meestal /etc/pam.d. Veel services kunnen via PAM worden "aangestuurd", voorbeelden hiervan zijn ftp, login, xdm, enz, die de beheerder de de mogelijkheid geven in te stellen wie wat mag doen.

Het volgende gereedschap is een must: *TCPWrapper* . Ook dit werkt op vrijwel ieder Unix systeem. Kort gezegd maakt dit gereedschap het mogelijk om de toegang tot sommige services aan bepaalde hosts te beperken. Deze hosts krijgen wel of geen toegang, afhankelijk van twee bestanden: /etc/hosts.allow en /etc/hosts.deny. TCPWrapper kan op twee manieren worden ingesteld: ofwel door het verplaatsen van de daemons, of door het veranderen van het bestand /etc/inetd.conf. Verderop zullen we zien dat TCPWrapper goed werkt in samenwerking met andere gereedschappen. Je kunt TCPWrapper vinden op ftp://ftp.porcupine.org/pub/security

Een ander interessant gereedschap is xinetd. In het kort is xinetd een vervanger voor inetd met een boel toegevoegde mogelijkheden. Met wat we hierboven al hebben gezegd over inetd, zullen we er niet verder op ingaan. Wanneer je geïnteresseerd bent, kan je xinetd vinden op http://www.xinetd.org.

Er bestaat voor Linux een gereedschap waar je niet onderuit kan: het heet Bastille-Linux. Je kunt hem vinden op http://www.bastille-linux.org. Dit gereedschap, dat in Perl is geschreven, leert je niet alleen een boel, maar is ook zeer efficiënt. Na het draaien van een script beantwoord je vele vragen en Bastille-Linux gedraagt zich daar vervolgens naar. Iedere vraag wordt uitgelegd en de standaard antwoorden worden aangegeven. Je kan veranderingen ongedaan maken, een nieuwe configuratie opzetten, controleren wat er al gebeurd is... Alles zit erin! Het helpt ook bij het instellen van een firewall: maar daarover later meer. Toen dit geschreven werd, was Bastille-Linux beschikbaar als versie 1.1.1, en versie 1.2.0 was al beschikbaar als release candidate. Het is zeer sterk verbeterd en biedt nu een

grafische interface op basis van TK en zijn Perl module. (Opmerking van de auteur: dit artikel is maanden geleden al geschreven. Nu is versie 1.3.0 van Bastille-Linux al beschikbaar en 2.0 is bijna af).

Inbraak detectiesystemen zijn ook onmisbaar. De twee zwaargewichten op dit gebied heten "snort" en "portsentry". De eerste kan worden gedownload op http://www.snort.org en de tweede van de Abacus website, http://www.psionic.com. Deze gereedschappen moet je niet vergelijken: de eerste is een NIDS (Network Intrusion Detection System) dat vooral informatie doorgeeft, terwijl de tweede kan worden gezien als een actief reagerend programma. Snort heeft veel opties om netwerkverkeer te bekijken. Je kunt alles dat je wilt weten bekijken: inkomend verkeer, uitgaand, binnen de firewall, buiten de firewall. Het kan natuurlijk gigantische logbestanden aanleggen, maar je moet wel weten wat je wilt weten! Er is een win32 versie beschikbaar, een belangrijk gegeven wanneer we kijken hoeveel gratis gereedschappen er beschikbaar zijn voor dit type "systeem".

Portsentry heeft een heel interessante mogelijkheid: het kan, als je dat wilt, gescande poorten blokkeren. Of je stuurt de aanvaller door naar een ongebruikt adres, of je stuurt hem door naar de firewall. Je kunt natuurlijk ook instellen wie je wel en wie je niet wilt blokkeren. Nu kunnen we terug nar TCPWrapper: portsentry kan schrijven naar het /etc/hosts.deny bestand als je dat wilt. Zo wordt portsentry dus zeer effectief. We gaan nu niet in op het debat over de filosofie achter portsentry - het concept "port binding". Het hangt af van je wensen: jij moet beslissen nadat je je meer verdiept hebt in het onderwerp. Pas wel op dat portsentry een machine "onzichtbaar" kan maken, hoewel dat niet per definitie een slecht ding hoeft te zijn! En tenslotte kan portsentry worden gebruikt in verschillende operationele modi, waarvan de meest geavanceerde "gereserveerd" is voor Linux (tenminste tot op dit moment).

We kunnen niet praten over beveiliging zonder in te gaan op encryptie (versleuteling). Hoewel er wetten voor zijn, verschillen die van land tot land, en soms is het zelfs helemaal verboden om encryptie te gebruiken.
Opmerking van de auteur: het volgende deel is weggehaald uit de Engelse versie van dit artikel, aangezien het alleen van belang is onder de Franse wetgeving.
Conclusie: Als jou land encryptie toestaat, installeer dan ssh clients en servers op je Unix machines (tenminste, voor zover je dat nodig hebt!).

Om te eindigen met Unix gereedschappen, noemen we er nu die bij niet-gratis Unix versies meegeleverd worden, onder Solaris zijn er ndd en aset; onder Irix kan je ipfilterd gebruiken. MacOs X levert enkele gratis gereedschappen mee, zoals ssh, ipfwadm...
Hier later meer over.

Laten we nu eens praten over de enige echte (gelukkig !) Niet geTermineerde 4.0. Hier kunnen we niet spreken van gratis gereedschappen... de man uit Redmond levert echter wel "gratis" materiaal mee om de mogelijkheden van het systeem te verbeteren (dit heeft niets te maken met patches voor bugs, aangezien deze officieel niet bestaan in NT!). Wat betreft beveiligung is NT 4.0 een modelvoorbeeld... van absurditeiten. Het lijkt een beetje op een vergiet! Maar daar gaat het hier niet om. We gaan er vanuit dat je al een Service Pack hebt gedownload (nummer 6 ten tijde van dit schrijven). Daarna moet je nog wat hotfixes downloaden... het zijn dus veiligheidspatches. Nu kan je enkele gratis gereedschappen (vrijelijk beschikbaar maar zonder broncode) downloaden. Dat was het.

Voor andere systemen zal je wat meer moeten zoeken. De ontwikkeling van AmigaOS schijnt niet door veel mensen gedragen te worden en de TCP/IP laag is een beetje oud. Maar er is in het Public Domain nog voldoende te vinden. Bij BeOS is het al niet veel beter: dit geweldige besturingssysteem gaat een

twijfelachtige toekomst tegemoet en de netwerklaag, die "Bone" heet, is nog steeds niet uitontwikkeld. (Opmerking van de Auteur: helaas is BeOS nu dood. Enkele mensen proberen het nog in leven te houden als een free software product... en dat doen ze vrij goed!)
Maar oook hier kan je enkele gereedschappen uit de Unix wereld vinden die het werk vergemakkelijken.

De hosts beveiligen

Nu moet je dit alles instellen! Laten we er opnieuw van uitgaan dat alle Unix machines zijn uitgerust met shadow-utils, PAM, TCPWrapper, en dat alle nutteloze services zijn gestopt of verwijderd, de toegangsrechten zijn beperkt voor de "gevoelige" directories enz.

Voor de Linux machines is het nu tijd om Bastille-Linux te starten. (Dit gereedschap zou moeten werken op de meeste Linux distributies, maar het is in eerste instantie ontwikkeld voor RedHat en Mandrake). Beantwoord de vragen gerust zo dat de rechten zeer beperkt zijn.
Op het Linux systeem dat wordt gebruikt als gateway, moet een minimaal systeem geïnstalleerd worden. Je kunt de meeste servers verwijderen: http, ftp, enz. Verwijder X11: je hebt het toch niet nodig! Verwijder de software die je niet nodig hebt... je kunt dus bijna alles weggooien. Stop de nutteloze daemons. Je moet je systeem zo invullen dat wanneer je het commando *ps ax* geeft, het scherm niet eens volstaat. Als je gebruik maakt van IP Masquerading, moet het *lsof -i* commando een regel weergeven: die over de luisterende server (we gaan uit van een niet-permanente verbinding).
We kunnen ook portsentry installeren op de Linux machines en het laten opstarten tijdens de boot. We maken wel gebruik van de "geavanceerde" modus (alleen onder Linux, dit houdt in met -atcp en -audp opties). Hierbij wordt er dus vanuit gegaan dat TCPWrapper en een Firewall al zijn geïnstalleerd. Hier later meer over.

Voor Solaris zullen we gebruik maken van de *aset* en *ndd* commando's. Ook hierover later meer. Portsentry gebruiken we ook. We kunnen IP Filter toevoegen en de standaard versie van RPCbind vervangen door verie 2.1 die beschikbaar is op porcupine.org. Voor Irix kiezen we ipfilterd als pakketfilter. Het is onderdeel van de Irix distributie, maar het wordt standaard niet geïnstalleerd.

Wat betreft NT liggen de zaken iets lastiger...De "fascistische" oplossing is het blokkeren van de poorten 137 en 139, de NetBIOS poorten (of zelfs verwijdering van de complete NetBIOS)... maar dan kan er geen gebruik meer worden gemaakt van de netwerk mogelijkheden (Windows netwerk wel te verstaan) en dat kan een klein probleem zijn met betrekking tot de applicatie server! Je kunt ook snort installeren, maar daarmee voorkom en stop je de lekken in de machines niet. Bovendien is het verstandig om de partitie toegang zeer te beperken... dit kan natuurlijk pas wanneer je met NTFS partities werkt. Er is een gratis programmaatje beschikbaar om van de guest account af te komen, maar de broncode hiervan is niet beschikbaar. Daarna moet je alle beschikbare veiligheidspatches installeren! En tenslotte zal je handmatig het een en ander moeten veranderen in de darmen van het beest om hem minder kwetsbaar te maken. Het lijkt een beetje op rondrennen op een stormbaan, maar het is noodzakelijk.

Voor de meer "exotische" besturingssytemen, zul je zelf op zoek moeten. Maar ook hier gelden vooral de standaard regels: hoe minder actieve services, hoe beter.

Het netwerk beschermen

Als de machines goed zijn "voorbereid", ben je al halverwege. Maar je moet verder gaan. Aangezien we praten over Free Software, kiezen we voor een Free Software firewall voor de gateway: dat is dus de machine waarmee je toegang geeft tot het "wilde westen" van het web. Wij hebben hier gekozen (jawel!) voor een Linux machine: daardoor kunnen we gebruik maken van de Bastille-Linux firewall. Het werkt met ipchains of ipfwadm, afhankelijk van de gebruikte kernel versie. Wanneer je gebruik maakt van kernel 2.4, dan werkt het met iptables.

Een beetje uitwijding: het is niet handig om last te hebben van alle begin-problemen wanneer het om veiligheid gaat. De "wedstrijd" om de laatste kernel versie kan leiden tot een zeer negatieve situatie. Dit betekent echter niet dat gebruik maken van een nieuwe kernel niet goed is, maar het koppelen daarvan aan bestaande gereedschappen die daarvoor niet ontwikkeld zijn, kan een grote fout zijn! Een advies: heb geduld! De nieuwe firewall gereedschappen van kernel 2.4 zien er goed uit, maar ze zijn nog wel erg "nieuw". Na deze opmerking: de keuze is aan jou...

De Bastille-Linux firewall is zowel eenvoudig als effectief. Maar er bestaat een veel uitgebreider gereedschap, zo ongeveer zo groot als een compleet prehistorisch roofdier, T.REX geheten. Deze is beschikbaar op http://www.opensourcefirewall.com. Als je op zoek bent naar een zeer geavanceerd gereedschap, dit is het.

Er bestaan andere oplossingen zoals proxy’s, maar die zijn lang niet altijd beter. Opnieuw wat uitwijding: proxy’s worden vaak "firewalls" genoemd. Dit zijn echter twee verschillende dingen. De firewalls waar we het hier over hebben zijn pakketfilters en bieden geen authorisatie mogelijkheden. Er bestaan twee typen proxy server: applicaties en socks. In het kort, een applicatie-proxy is een beheersysteem voor de complete communicatie, inclusief gebruikers authorisatie. Dit is waarom het meer bronnen nodig heeft dan een firewall. Steeds weer is aangetoond dat dit soort gereedschap slechts korte tijd een barrière vormt. Een firewall kan worden "gekraakt" in ongeveer 15 minuten. Goed om te weten, niet? Vandaar dat je je machines goed moet beveiligen in je netwerk: de beslissing om een netwerk te beveiligen met alleen een firewall of een proxy is pure ketterij!

Een andere methode om de risico’s in een netwerk te verkleinen, is gebruik maken van encryptie. Gebruik maken van bijvoorbeeld telnet, is het uitrollen van een rode loper voor "crackers". Dit is DE manier om ze de sleutel van de voordeur te geven. Ze kunnen niet alleen zien dat er gegevens rondgaan, maar ze kunnen ook de wachtwoorden als gewone tekst langs zien komen: heel mooi, niet? Gebruik dus ssh over de "onveilige" protocollen (of in de plaats ervan). Als je echt telnet MOET (?) gebruiken, stuur de gegevens dan over een beveiligde verbinding. Met andere woorden, stuur de telnet poort door via een veilige poort. Je kunt hier meer over vinden in het artikel getiteld "Door de tunnel" (Gratis reclame!)

Goed, nu hebben we geprobeerd de beveiliging te verbeteren, maar we zouden ons werk ook moeten controleren. Om dit te doen, zullen we zelf "cracker" moeten worden, tenminste: we gaan hun gereedschap gebruiken. Gruwelijk, niet? Ook hier kunnen we een leuke collectie programma’s vinden. Maar ook hier kiezen we er twee uit: nmap en nessus. Ze overlappen elkaar niet, aangezien de tweede de eerste nodig heeft. Deze gereedschappen zijn portscanners, hoewel nessus nog iets meer is. Nessus vertelt je meer over kwetsbare plekken in een systeem, hij vergelijkt de scanresultaten met een database van zwakke plekken. Door deze gereedschappen te gebruiken kom je de zwakke plekken op alle machines tegen, het maakt niet uit welk besturingssysteem ze draaien. De resultaten zijn veelzeggend, dus deze gereedschappen zijn echt noodzakelijk. Je kunt nmap vinden op: http://www.insecure.org en nessus op: http://www.nessus.org.

Vanaf het begin van dit artikel hebben we gesproken over het beveiligen van een lokaal netwerk waarin enkele machines bereikbaar zijn vanuit de buitenwereld. Het geval van een Internet Service Provider (ISP) zou heel anders zijn. We zullen niet ingaan op de details hier. Laten we het houden bij de opmerking dat je nog steeds veel van de hier genoemde zaken kunt toepassen, maar je zult ook andere, veel uitgebreidere methoden moeten toepassen, zoals VPN (Virtul Privte Network), LDAP voor de authorisatie (bijvoorbeeld), enz. Het is bijna een ander onderwerp, aangezien er veel meer randvoorwaarden zijn in dat geval. Laten we niet ingaan op e-business sites, die vaak nogal roekeloos zijn. 'Beveiligde sites' roepen ze! Praat me er niet van.. Stuur jij je credt card nummer over internet? Als je antwoord ja is, ben je vrij dapper (of roekeloos?!) Suggestie: Als je Frans kunt lezen, kijk dan eens naar deze website http://www.kitetoa.com, hij is het waard.

Systeembijzonderheden

Zoals al gezegd, reageren de systemen niet op dezelfde manier op een aanval. Sommigen gaan er heel goed mee om terwijl anderen zo lek als een zeef zijn. Het is paradoxaal (hoewel, niet echt...), maar de gratis besturingssystemen zijn beter. De verschillende BSD's (OpenBSD, NetBSD, FreeBSD...), de verschillende Linux-en liggen behoorlijk voor op het gebied van veiligheid. Ook dit is het resultaat van het geweldige werk van de Free Software gemeenschap. De anderen, ook degenen die Unix heten, zijn wat minder geavanceerd. Maar wanneer ze geen Unix heten, is het nog veel erger!

Alle gereedschappen genoemd in dit artikel zijn ontwikkeld voor gratis besturingssystemen. De meeste betaalde Unix systemen kunnen er ook gebruik van maken. Maar deze betaalde besturingssystemen bevatten vaak hun eigen gereedschappen. Solaris bijvoorbeeld, bevat *ndd* en *aset*. Ondanks hun goede reputatie zijn Sun systemen geen voorbeelden van veiligheid. Een gereedschap als aset zorgt voor verbeteringen op het gebied van toegangsrechten. Aset biedt drie beveiligingsniveau's: low, medium en high. Je kunt het starten vanaf een commandoregel of via een cron taak. In een al draaiend netwerk ligt de situatie anders; wat waar is om 5 uur 's middags, hoeft nog niet waar te zijn om 6 uur 's middags. Daarom moeten de commando's periodiek gestart worden om wat eenheid te bewaren. Daarom kan aset via cron worden gedraaid, dan controleert het ieder uur, of welke periode je dan ook instelt, de toegangsrechten op bestanden, directories...
Ndd maakt veranderingen aan de IP-stack parameters mogelijk. Het kan bijvoorbeeld worden gebruikt om de afdrukken van een systeem te verbergen. Een bekend systeem is kwetsbaarder, aangezien de "crackers" dan beter weten waar ze zich op moeten richten. Met ndd kan je de TCP Maximum Segment size (MSS) veranderen. Standaard is het formaat 536 voor Solaris 2.6. Het commando *ndd -set /dev/tcp tcp_mss_def 546* verandert dit naar 546. Hoe hoger MSS, hoe beter (maar overdrijf het niet!). Nmap kan bijvoorbeeld deze zwakke plekken vinden. Door gebruik te maken van ndd, kan je het gras onder z'n voeten wegmaaien. Als je machines hebt die Solaris draaien, gebruik dan ndd. Er zijn veel opties: bekijk de man pagina's maar eens.
Je kunt ook IP Filter gebruiken, een pakketfilter. Deze is beschikbaar op: ftp://coombs.anu.edu/pub/net/ip-filter.

Wat betreft Irix is de situatie weer heel anders. SGI (ex-Silicon Graphics), heeft het systeem, zoals de naam al zegt, ontworpen voor grafische ontwikkelingen. Veiligheid was niet de belangrijkste zorg. Noodzaak kent geen regels, en het werd verplicht om manieren te verzinnen om de risico's te verkleinen. Daarna werd ipfilterd meegeleverd met de Irix distributie, maar het wordt niet standaard geïnstalleerd: je zult er naar moeten zoeken! ipfilterd wordt, natuurlijk, gebruikt voor pakket filteren, en

op die manier kan je de toegang weigeren aan iedereen die je wilt. Het vertrouwt op een configuratiebestand geheten ipfilterd.conf en dat is waar het wat lastig wordt. De syntax voor dit bestand is wat vreemd en houdt niet van onverwachtte witruimtes of lege regels. Dus, wanneer je een machine die "mars" heet wilt laten praten met een machine die "jupiter" heet (het SGI workstation), moet je een regel typen die er zo uitziet:
accept -i ec0 between jupiter mars
De machines die niet worden genoemd in dit script, kunnen geen toegang krijgen tot "jupiter". Het is nog erger: wanneer je de parameter *ipfilterd_inactive_behavior* niet wijzigt met behulp van systune, kan niemand toegang krijgen tot de machine! Zeer effectief, niet? Deze parmeter staat standaard op een waarde van 1, je moet deze veranderen in 0 met behulp van het commando: *systune -i ipfilterd_inactive_behavior 0.*
Iets anders wat je maar beter kunt onthouden, is dat Irix een "grote" achilleshiel heeft, geheten fam (File Alteration Monitor). Dit programma regelt de communicatie tussen de verschillende daemons. Bijvoorbeeld de daemon die de iconen voor het bestandsbeheer programma serveert. Er is helaas maar een ding wat je hieraan kunt doen: uitzetten! Helaas, maar het is niet anders.

En als laatste opmerking over Unix systemen, noemen we het feit dat QNX zeer kwetsbaar is, maar dat het met wat Free Software gereedschappen een heel eind verbeterd kan worden. Mac OS X wordt al geleverd met enkele van deze gereedschappen.

We moeten nu wat praten over de absolute referentie voor netwerk systemen: de enige echte NT 4.0. Het beveiligen hiervan is een utopische gedachte, ondanks wat de Koning van Redmond (en vele anderen) zegt. Het simuleren van een aanval met nessus bijvoorbeeld, levert een nachtmerrie op. Zolang NetBIOS draait, zal nessus de naam van alle machines in het netwerk geven, inclusief de bijbehorende gebruikers en beheerders. De oplossing hiervoor: gooi NetBIOS eruit! Goed, zoals al eerder gezegd, geen NetBIOS, geen netwerk... Je zult hier dus een keuze moeten maken.
Nessus zal je vertellen dat je kan inloggen als gast gebruiker met een NULL sessie (dat betekent met een NULL gebruikersnaam en een NULL wachtwoord). Verwijder deze dan! Ja, maar hoe...? En dat geldt ook voor de volgende problemen!
Dus, verklein de toegangsmogelijkheden tot de partities (NTFS) en directories. Voor FAT partities... is er geen oplossing. Maar, vanwege de software die je wilt gebruiken, heb je misschien wel FAT prtities nodig: er is software die niet werkt op NTFS. En tenslotte, vermijdt het geweldige IIS, vooral als ftp server. Installeer het NIET! Ook al zijn er vandaag de dag genoeg ISP’s zo gek dat ze het wel gebruiken, ze zouden beter apache kunnen gebruiken, maar... we gaan niet verder in op IIS, er is meer dan genoeg literatuur over dit onderwerp.
Het is echter wel mogelijk om van het vergiet een zeef te maken (de gaten zijn kleiner!). Het probleem is dat het nogal een lang verhaal is, een heel magazine vol zou nog niet voldoende zijn. We noemen alleen het belangrijkste. Hier is het duidelijk niet mogelijk om alles te beveiligen met Free Software: we hebben het over de Microsoft wereld! De eerste suggestie is het gebruik van MSCE (Microsoft Security Configuration Editor), deze is beschikbar vanaf ServicePack 4 met MMC (Microsoft Management Console). Maar wees heel voorzichtig! Als je een fout maakt, heb je een probleem. Deze software is natuurlijk alleen verkrijgbaar in het Engels, dus als je een niet-Engelse versie van het systeem gebruikt, houd er dan rekening mee dat taalfouten nooit goede resultaten hebben gegeven in de Redmond wereld (=vastlopers). Je bent gewaarschuwd! Nu enkele belangrijkere maatregelen: je moet de beheerder-account beveiligen, of zelfs desactiveren. Kijk eens naar *passprop*, beschikbaar vanaf SP 3. Je kunt ook de wachtwoorden verbeteren met behulp van de *passfilt* dll via het register (ik ben er altijd van uit gegaan dat de mensen die dit hebben uitgevonden onder invloed waren van LSD...). Deactiveer de beroemde gast account. Het is niet erg nuttig (zie hierboven), maar het maakt het wat minder erg. Je kan

z’n toegang tot de logs van het register beperken. Maak in "HKEY_LOCAL_MACHINE", de volgende ingangen: *System\CurrentControlSet\Services\EventLog\Application*, Security en System (deze laatste twee moeten in de plaats van ’Application’ staan). Hun naam is "RestrictGuestAccess", het type is REG_SZ en de waarde is 1. Je kunt de wachtwoorden coderen met *syskey*. Wees voorzichtig, het is een operatie die je niet ongedaan kan maken! En tenslotte wat goed nieuws: je kan de gast-toegang beperken. Opnieuw moet je wat spelen met het register, ook weer in "HKEY_LOCAL_MACHINE". Nu heet de ingang *System\CurrentControlSet\Control\Lsa*. De naam is "RestrictAnonymous", het type is "REG_DWORD" en de waarde is 1. Echter, Microsoft is een kwelgeest: ga ervanuit dat dit ook enkele netwerk services verandert... Behalve de belangrijke dingen, kan je ook de toegang tot enkele poorten beperken met behulp van de netwerk applicatie in het configuratie scherm. Kies TCP/IP eigenschappen, kies "Geavanceerd" en kruis het "Activeer beveiliging" vak aan (ik geloof dat het zo heet maar ik heb dit niet thuis om te controleren). Kies, in het "beveiliging" venster voor "Allow only" en kies de poorten die je wilt activeren. Wees ook hier weer voorzichtig. Je moet weten wat je doet, anders zullen enkele services niet meer werken.
Er kan nog veel meer worden gedaan, maar deze dingen zijn essentieel. Kijk om meer te weten te komen op sans.org: hier is heel veel documentatie beschikbaar.

Oh, de eenvoud!

Als je dit alles gedaan hebt, kan je nessus starten en het hele netwerk scannen en je zult nog steeds veiligheidsgaten krijgen. We zullen niet zeggen waar ze vandaan komen, we weten het al... Probeer dit toch een beetje te maskeren. Het zal niets doen aan de NetBIOS gaten, maar het zal de schade beperken. Maak subdomeinen aan. Log niet in als beheerder. Breng patches aan. En tenslotte: probeer dit alles te verbergen achter Unix machines die gebruikt worden als gateway. Helaas komt de relativiteit van beveiliging niet alleen van producten uit Redmond. Een netwerk leeft: er is altijd wel iets aan de hand. Een goede beheerder is een beheerder met ’paranoia’, die vaak controleert op fouten en fixes. Hij schrijft scripts om de checks te automatiseren. Bijvoorbeeld om regelmatig de SUID/SGID programma’s te controleren, evenals de kritische bestanden, de logs... Om nog wat meer vrienden te maken, blokkeer je de floppy en cdrom apparaten van gebruikers. Accepteer het niet langer dat gebruikers software downloaden zonder jou toestemming, vooral niet wanneer deze software gestart kan worden, zoals altijd in de Microsoft wereld. Zorg ervoor dat gebruikers geen meegestuurde documenten zoals Word en Excel bestanden meer kunnen openen. Dit is mogelijk met een mail filter systeem. Ja, ik weet dat dit fascistisch klinkt, maar wat kan je anders doen aan macro virussen? Gebruik geen producten zoals Outlook. Nogmaals: je moet weten wat je wil! Ik weet dat wat ik zeg geen waarde heeft, maar kan je nog van veiligheid spreken met zulke producten? Het beroemde "I love you" heeft kennelijk niemand iets geleerd.
Wat betreft Unix: downloads moeten ook worden gecontroleerd. De Checksums worden niet voor niets meegeleverd.

Leer jezelf de gewoonte aan dat je je netwerk regelmatig controleert met logs, scripts, scans... Je zal zien: dingen veranderen snel en niet alleen op de juiste manier.
Tenslotte, we hebben er tot nu toe niets van gezegd, maar vergeet niet om backups te maken. De strategie is altijd dezelfde: dagelijks, weekelijks en maandelijks. Een Unix machine kan ook problemen hebben, hoewel dat niet vaak voorkomt. En soms maken gebruikers fouten... maar niet vaak. Het is bekend dat de meeste problemen te danken zijn aan de machines of aan de afdeling die ervoor verantwoordelijk is :-(

Endelijk we zijn klaar!

Als je tot hier bent gekomen, ben je behoorlijk dapper. Het probleem is echter dat we het onderwerp slechts aangestipt hebben! Beveiliging eindigt nooit, en het is niet alleen van belang voor netwerken. Kwetsbare applicaties kunnen een netwerk compromitteren. Een slecht ingestelde firewall is veel gevaarlijker dan helemal geen firewall. Een Unix machine bevat duizenden bestanden. Wie kan er zeker van zijn dat geen van die bestanden kwetsbaar is? Wie gaat er vanuit dat een "cracker" probeert een 128 bits sleutel te kraken? Laat je niet voor de gek houden: hij gaat op zoek naar de achterdeur. En dat doet hij steeds weer, je kunt alle beschikbare beveiligingsgereedschappen installeren, maar als je een klein gaatje open laat, dan komt de "slechterik" hier doorheen.

Veiligheid is ook gedrag: volg op wat er gebeurt. Bekijk bijvoorbeeld de websites over beveiliging regelmatig, net als de websites over de besturingssystemen. Sun publiceert bijvoorbeeld iedere maand de patches die ze aanraden. SGI brengt iedere drie maanden een nieuwe versie van Irix uit. Microsoft brengt regelmatig hotfixes en ServicePacks uit. Linux distributeurs publiceren errata voor alle nieuw ontdekte kwetsbaarheden. Dit geldt ook voor de verschillende BSD’s. Als je niet het product gebruikt waar de patch voor geschreven is, verwijder deze dan van de harde schijf. En er zijn meer van dit soort dingen: de hoeveelheid taken die je hier kunt uitvoeren is zeer, zeer lang. Maar in het kort komt het er op neer dat je jezelf op dit gebied geen beperkingen moet opleggen.

Tenslotte, laten we nog eens zeggen dat dit alles alleen bijdraagt tot een iets veiliger en minder kwetsbaar netwerk. Verwacht nu niet dat je een 100% veilig netwerk krijgt, ook nu, op dit moment niet (hoewel, misschien wel, als alle computers uit staan). Je hoeft ook niet echt paranoïde zijn om dit goed te doen... maar het helpt wel. Zorg er echter wel voor dat je het in het dagelijks leven niét bent, dat is veel gezelliger voor de mensen om je heen...

Bronnen

- http://www.linuxsecurity.com
- http://www.sans.org
- http://www.infosyssec.org
- http://www.securityfocus.com
- http://www.cs.purdue.edu/coast/hotlist/

Het leven is deprimerend: laten we eens wat leuks doen!

Een andere manier om te werk te gaan ;-)

Site onderhouden door het LinuxFocus editors team © Georges Tarbouriech "some rights reserved" see linuxfocus.org/license/ http://www.LinuxFocus.org	Vertaling info: fr --> -- : Georges Tarbouriech <georges.t(at)linuxfocus.org> fr --> en: Georges Tarbouriech <georges.t%28at%29linuxfocus.org> en --> nl: Hendrik-Jan Heins <hjh/at/passys.nl>

2005-01-14, generated by lfparser_pdf version 2.51