

NMAP:

Je kunt vele details over de opzet van een netwerk ontzetselen met deze geavanceerde tool. Nmap gebruikt namelijk alle nu bekende technieken en het is vrijwel altijd mogelijk, gedetailleerd de netwerkopzet in kaart te brengen. En dan ook nog op een manier waarop de scans en probes moeilijk te detecteren zijn door vele security tools (IDS's en firewalls). Nmap is momenteel beschikbaar voor nagenoeg alle besturingssystemen, behalve windows. Nmap is zeer veelzijdig en flexibel.

VOORBEELDEN:

Het vinden van alle HTTP servers van een klasse C netwerk.

```
# nmap -sS -oN scan.log -p 90 chello.nl/24
```

Een aantal mogelijke chatboxes vinden.

```
# nmap -sF -v -p 6667 -iR
```

Welk OS draait er op machine x ?

```
# nmap -sS -O x
```

Welke besturingssystemen gebruiken ze bij UUNet ?

```
# nmap -O uunet.com/16
```

TCP WRAPPERS:

Draait onder de zgn. **tcpd daemon**. De tcpd fungeert als een soort veiligheidslaag. Voordat een service wordt gestart, wordt ie door de tcpd opgevangen. Die beoordeelt aan de hand van de bestanden host.allow en host.deny of de service uitgevoerd mag worden. Zie hoofdstuk 12.

/etc/host.allow, als hier services in vermeld staan mogen deze WEL worden uitgevoerd.

/etc/host.deny, als hier services in vermeld staan mogen deze NIET worden uitgevoerd.

De veiligste strategie is: ALLES DICHT, tenzij. Dus in host.deny moet een regel staan die alle verbindingen van alle systemen niet toestaat.

WACHTWOORDEN:

Wachtwoorden moet aan een aantal eisen voldoen om ze als veilig te beschouwen. Gebruik daarom niet de naam van je kat, je geboorte datum e.d. Een wachtwoord kan het beste bestaan uit letters (hoofd en kleine), cijfers en vreemde tekens. Stel een policy in die gebruikers verplicht om elke maand haar wachtwoord te laten veranderen. Ook kan er een lock komen op een user als er vaker dan x keer een onjuist wachtwoord is gebruikt.

SSH:

Ssh = secure shell

Ssh zorgt voor een veilige versleutelde verbinding naar bijv. Een linux system. Een bekende ssh cleitn is putty.

Extra veiligheid inbouwen is door de root gebruiker niet rechtstreeks in te kunnen laten loggen op een machine. Inloggen op een machine met een ander account moet als volgt.

Ssh job@10.0.0.1 gevolgd door wachtwoord. Daarna su – gevolgd door passwd om als root in te kunnen loggen.

Als je bijv, telnet gebruikt, dan kan de informatie die over de telnet sessie verzonden wordt, worden opgevangen met netwerk tracers. Denk hierbij aan gebruikersnamen en wachtwoorden.

SHADOW PASSWD:

/etc/passwd

Bij het (oude) /etc/passwd systeem worden de wachtwoorden versleuteld opgeslagen in de /etc/passwd . Deze moet leesbaar zijn voor het gehele systeem, er staat namelijk ook in wat de userID en groupID van een gebruiker is en wat zijn homedir is. Voor het verkrijgen van deze /etc/passwd is het hebben van een useraccount voldoende.

Shadow passwords

Bij het Shadow systeem is er weliswaar ook nog een /etc/passwd, maar deze bevat geen wachtwoorden. Die staan opgeslagen in de shadow, vaak /etc/shadow, die alleen leesbaar is voor de root en de shadow group. Om deze te bemachtigen is dus root access nodig of een useraccount in de shadow group. Of je kunt een van de volgende methoden proberen:

=====

Je kunt proberen de root account te hacken (maar waarom heb je dan nog de shadow nodig ?) met bijvoorbeeld een brute force via SSH: een script dat probeert in te loggen als root en gewoon net zo lang wachtwoorden probeert tot het het juiste wachtwoord gevonden heeft. Een beetje oplettende systeembeheerder ziet dit vrij snel in z'n logs. Of een ssh daemon kan zo geconfigureerd zijn dat hij na x foute pogingen een bepaalde tijd geen logins meer accepteert.

=====

ROOT ACCOUNT:

Gebruik altijd een normaal account. Mocht het nodig zijn om als root in te loggen doe dat dan door su – gevolgd door enter.

Als je de pc even verlaat, gebruik dan vlock je pc te locken.

FIREWALL

Via de Proxy

De drie rondjes staan voor de drie reeksen. Als een pakketje bij zo'n cirkel aankomt worden de regels nagelopen om het lot van het pakketje te bepalen. Als hieruit blijkt dat het pakketje moet worden genegeerd (DROP) dan wordt het pakketje gelijk daar gestopt. Als uit de reeks blijkt dat er niets mis is met het pakketje (ACCEPT) dan doorloopt het pakketje de rest van het schema.

Elke reeks bestaat uit een aantal regels en een beleid (policy). Elke regel heeft de vorm van: "Als het pakketje deze eigenschappen heeft, doe dan dit en dat met het pakketje.". Als deze regel niet van toepassing is op het pakketje (het pakketje heeft niet de eigenschappen voor deze regel), dan wordt de volgende regel gelezen. Als de laatste regel is gelezen en er is geen regel die van toepassing is op dit pakketje, dan wordt de actie uitgevoerd die het beleid is. Dit is dus een standaard actie die van toepassing is op alle pakketjes die niet door een regel gespecificeerd zijn. Het beleid is meestal het pakketje negeren (DROP) zodat onbekende pakketjes niet door kunnen dringen.

1. Als een pakketje binnenkomt (via een modem of ethernetkaart bijvoorbeeld), bepaalt de kernel eerst waar het pakketje heen moet. Dit heet routing.
2. Als het pakketje voor deze computer bedoeld is, wordt het pakketje doorgegeven aan de INPUT reeks. Als het hierdoor komt, wordt het doorgegeven aan de programma's op de computer.
3. Als het pakketje voor een andere computer bedoeld is, en de kernel kan niet forwarden of het weet niet hoe het geforward moet worden, wordt het pakketje genegeerd. Als er wel geforward kan worden, dan komt het pakketje in de FORWARD reeks. Komt het hierdoor, dan wordt het doorgestuurd naar een andere machine.
4. Als een programma op de computer een pakketje verstuurd, moet het eerst door de OUTPUT reeks om verzonden te kunnen worden.