**Verslag labo 2: Reconaissance**

**Opstelling**: 3 boxes in VirtualBox

Box1: Kali Linux, 192.168.137.10/24

Box2: Metasploitable2, 192.168.137.20/24

Box3: Web for pentesting, 192.168.137.30/24

**Stap 1**: Metasploitable vinden: lijst alle online hosts in een netwerk waarmee Kali verbonden is:   
nmap -sP 192.168.137.0/24 (Host discovery)

**Stap 2**: Alle poortscan technieken geven ongeveer dezelfde resultate. De meest agressieve is *nmap -sV 192.168.137.20 of .30* Hierbij worden alle open poorten getoond samen met de protocols die met deze poorten verbonden zijn, de services die achter deze poorten draaien en zelfs hun versies alsook hoe ver (hoeveel hops) de gekozen device zich bevindt.

Hierbij de resultaten van deze commando

|  |  |  |
| --- | --- | --- |
| Kali | Metasploitable2 | Web for pentesting |
| Nmap scan report for 192.168.137.10  Host is up (0.0000070s latency).  Not shown: 998 closed ports  PORT STATE SERVICE VERSION  22/tcp open ssh OpenSSH 6.7p1 Debian 5 (protocol 2.0)  111/tcp open rpcbind 2-4 (RPC #100000)  Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel | Nmap scan report for 192.168.137.20  Host is up (0.000091s latency).  Not shown: 977 closed ports  PORT STATE SERVICE VERSION  21/tcp open ftp vsftpd 2.3.4  22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  23/tcp open telnet Linux telnetd  25/tcp open smtp Postfix smtpd  53/tcp open domain ISC BIND 9.4.2  80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  111/tcp open rpcbind 2 (RPC #100000)  139/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)  445/tcp open netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)  512/tcp open exec netkit-rsh rexecd  513/tcp open login  514/tcp open tcpwrapped  1099/tcp open rmiregistry GNU Classpath grmiregistry  1524/tcp open shell Metasploitable root shell  2049/tcp open nfs 2-4 (RPC #100003)  2121/tcp open ftp ProFTPD 1.3.1  3306/tcp open mysql MySQL 5.0.51a-3ubuntu5  5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7  5900/tcp open vnc VNC (protocol 3.3)  6000/tcp open X11 (access denied)  6667/tcp open irc Unreal ircd  8009/tcp open ajp13 Apache Jserv (Protocol v1.3)  8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1  MAC Address: 08:00:27:B3:42:D7 (Cadmus Computer Systems)  Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel | Nmap scan report for 192.168.137.30  Host is up (0.00034s latency).  Not shown: 997 closed ports  PORT STATE SERVICE VERSION  22/tcp open ssh OpenSSH 5.5p1 Debian 6+squeeze3 (protocol 2.0)  80/tcp open http Apache httpd 2.2.16 ((Debian))  389/tcp open ldap OpenLDAP 2.2.X - 2.3.X  MAC Address: 08:00:27:8F:B1:B1 (Cadmus Computer Systems)  Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel |

Aan de hand van de versies op de server is het mogelijk om af te leiden hoe goed het system geupdate wordt en eventueel naar vurnerabilities van een bepaalde versie online zoeken.

Dezelfde scan op de host:

Nmap scan report for 192.168.0.155

Host is up (0.00041s latency).

Not shown: 995 filtered ports

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows 98 netbios-ssn

445/tcp open microsoft-ds (primary domain: WORKGROUP)

5357/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
5357/tcp open wsdapi  
6000/tcp open X11

**Stap 3:** smb-enum-users script als volgt uitgevoerd: *nmap -sU -sS --script smb-enum-users.nse -p U:139,T:139,U:445,T:445 192.168.137.20* (UDP en TCP protocols op poorten 139 en 445 van metasploitable2)

Resultaat:

Nmap scan report for 192.168.137.20 (Metasploitable)

Host is up (0.00024s latency).

PORT STATE SERVICE

139/tcp open netbios-ssn

445/tcp open microsoft-ds

139/udp closed netbios-ssn

445/udp closed microsoft-ds

MAC Address: 08:00:27:B3:42:D7 (Cadmus Computer Systems)

Host script results:

| smb-enum-users:

| METASPLOITABLE\backup (RID: 1068)

| Full name: backup

| Flags: Account disabled, Normal user account

| METASPLOITABLE\bin (RID: 1004)

| Full name: bin

| Flags: Account disabled, Normal user account

| METASPLOITABLE\bind (RID: 1210)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\daemon (RID: 1002)

| Full name: daemon

| Flags: Account disabled, Normal user account

| METASPLOITABLE\dhcp (RID: 1202)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\distccd (RID: 1222)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\ftp (RID: 1214)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\games (RID: 1010)

| Full name: games

| Flags: Account disabled, Normal user account

| METASPLOITABLE\gnats (RID: 1082)

| Full name: Gnats Bug-Reporting System (admin)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\irc (RID: 1078)

| Full name: ircd

| Flags: Account disabled, Normal user account

| METASPLOITABLE\klog (RID: 1206)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\libuuid (RID: 1200)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\list (RID: 1076)

| Full name: Mailing List Manager

| Flags: Account disabled, Normal user account

| METASPLOITABLE\lp (RID: 1014)

| Full name: lp

| Flags: Account disabled, Normal user account

| METASPLOITABLE\mail (RID: 1016)

| Full name: mail

| Flags: Account disabled, Normal user account

| METASPLOITABLE\man (RID: 1012)

| Full name: man

| Flags: Account disabled, Normal user account

| METASPLOITABLE\msfadmin (RID: 3000)

| Full name: msfadmin,,,

| Flags: Normal user account

| METASPLOITABLE\mysql (RID: 1218)

| Full name: MySQL Server,,,

| Flags: Account disabled, Normal user account

| METASPLOITABLE\news (RID: 1018)

| Full name: news

| Flags: Account disabled, Normal user account

| METASPLOITABLE\nobody (RID: 501)

| Full name: nobody

| Flags: Account disabled, Normal user account

| METASPLOITABLE\postfix (RID: 1212)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\postgres (RID: 1216)

| Full name: PostgreSQL administrator,,,

| Flags: Account disabled, Normal user account

| METASPLOITABLE\proftpd (RID: 1226)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\proxy (RID: 1026)

| Full name: proxy

| Flags: Account disabled, Normal user account

| METASPLOITABLE\root (RID: 1000)

| Full name: root

| Flags: Account disabled, Normal user account

| METASPLOITABLE\service (RID: 3004)

| Full name: ,,,

| Flags: Account disabled, Normal user account

| METASPLOITABLE\sshd (RID: 1208)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\sync (RID: 1008)

| Full name: sync

| Flags: Account disabled, Normal user account

| METASPLOITABLE\sys (RID: 1006)

| Full name: sys

| Flags: Account disabled, Normal user account

| METASPLOITABLE\syslog (RID: 1204)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\telnetd (RID: 1224)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\tomcat55 (RID: 1220)

| Flags: Account disabled, Normal user account

| METASPLOITABLE\user (RID: 3002)

| Full name: just a user,111,,

| Flags: Normal user account

| METASPLOITABLE\uucp (RID: 1020)

| Full name: uucp

| Flags: Account disabled, Normal user account

| METASPLOITABLE\www-data (RID: 1066)

| Full name: www-data

|\_ Flags: Account disabled, Normal user account

Zelfde commando op web for pentesting brengt geen resultaten op, aangezien daar geen samba service op draait.

**Stap 4**: Parallell verwerkt met stappen 1-3

**Reflectie Chingiz**

Als je het op een slimme manier aanpakt, kan je al heel veel leren over het systeem van je victim zonder opgemerkt te worden. Als je te weten kan komen welke services, met welke versies, op welke poorten en op welke machines draaien, kan je heel doelgericht je aanval beginnen voor te bereiden zonder dat de slachtoffer weet dat hij effectief aangevallen gaat worden. Zo heeft je aanval meer kansen op slagen.

Om het met de woorden van Sun Tzu te eindigen: “Rapidity is the essence of war: take advantage of the enemy's unreadiness, make your way by unexpected routes, and attack unguarded spots.”