Introduction to Nmap/Zenmap

A LOOK AT A HIGHLY VERSATILE TOOL EVERY PENTESTER SHOULD KNOW
Table of Contents

• What is Nmap? Why use it?
• Basic functions/commands
• Using scripts to find weaknesses
• What is Nmap?
• What is Zenmap?
Gather Information → Plan the attack → Play the attack → Select Target → Results
Basic Commands/Switches

nmap <options> <host>

-sS, -sT, -Pn, -sU, -sn, -F, -p(0-65535),
-T5, -A(-O,-sC,-sV), -v, -n
Host Selection

- **192.168.0.1**
- **192.168.0.1-255**
- **192.168.240-255.1-254**
- **192.168.1-7.1**
- **192.168.0.1/24**
- **192.168.1.1/0**
- **dnsName**
- **dnsName/24**

- **-iL <inputfilename>** (Input from list)
- **-iR <num hosts>** (Choose random targets)
- **--exclude <host1>,<host2>[,...]]** (Exclude hosts/networks)
• Port Selection: 0-65535
• -p#  -p#,#_2,#_3...#n  -p#-#n
• -p http, *ftp*
• -p T:#,U:#
• 21,22,23,25,53,67,68,80,137,138,139,161,443,445,
Idle Scan

Step 1: Probe the zombie's IP ID.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

Step 2: Forge a SYN packet from the zombie.

The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by 2 since step 1, so the port is open!
Scripts

http://nmap.org/nsedoc/
Scripts Groups

- auth
- broadcast
- brute
- default
- discovery
- dos
- exploit
- external
- fuzzer
- intrusive
- malware
- safe
- version
- vuln

- --script <name>
- --script <name1>, <name2>
- --script <name> --script args param=value
- --script <category>
- --script “http-*”
Nbstat

Host script results:
  nbstat: NetBIOS name: WINDOWS2003, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:c6:da:f5 (VMware)

Host script results:
  nbstat: NetBIOS name: WINDOWS2003, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:c6:da:f5 (VMware)

  Names:
  - WINDOWS2003<00> Flags: <unique><active>
  - WINDOWS2003<20> Flags: <unique><active>
  - SKULLSECURITY<00> Flags: <group><active>
  - SKULLSECURITY<1e> Flags: <group><active>
  - SKULLSECURITY<1d> Flags: <unique><active>
  - \x01\x02__MSBROWSE__\x02\x01 Flags: <group><active>
Banner
21/tcp open ftp
|_ banner: 220 FTP version 1.0\x0D\x0A

http-headers
PORT STATE SERVICE
80/tcp open http
http-headers:
| Date: Fri, 25 Jan 2013 17:39:08 GMT
| Server: Apache/2.2.14 (Ubuntu)
| Accept-Ranges: bytes
| Vary: Accept-Encoding
| Connection: close
| Content-Type: text/html
| (Request type: HEAD)
smb-os-discovery

Host script results:
<table>
<thead>
<tr>
<th>smb-os-discovery:</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS: Windows Server (R) 2008 Standard 6001 Service Pack 1 (Windows Server (R) 2008 Standard 6.0)</td>
</tr>
<tr>
<td>OS CPE: cpe:/o:microsoft:windows_2008::sp1</td>
</tr>
<tr>
<td>Computer name: Sql2008</td>
</tr>
<tr>
<td>NetBIOS computer name: SQL2008</td>
</tr>
<tr>
<td>Domain name: lab.test.local</td>
</tr>
<tr>
<td>Forest name: test.local</td>
</tr>
<tr>
<td>FQDN: Sql2008.lab.test.local</td>
</tr>
<tr>
<td>NetBIOS domain name: LAB</td>
</tr>
<tr>
<td>System time: 2011-04-20T13:34:06-05:00</td>
</tr>
</tbody>
</table>
smb-ls

Host script results:
smb-ls:
  Directory of \192.168.56.101\c$
  2007-12-02 00:20:09 0  AUTOEXEC.BAT
  2007-12-02 00:20:09 0  CONFIG.SYS
  2007-12-02 00:53:39 <DIR> Documents and Settings
  2009-09-08 13:26:10 <DIR> e5a6b742d36facb19c5192852c43
  2008-12-01 02:06:29 <DIR> Inetpub
  2007-02-18 00:31:38 94720 msizap.exe
  2007-12-02 00:55:01 <DIR> Program Files
  2008-12-01 02:05:52 <DIR> temp
  2011-12-16 14:40:18 <DIR> usr
  2007-12-02 00:42:40 <DIR> WINDOWS
  2007-12-02 00:22:38 <DIR> wmpub
smb-enum-shares:

account_used: WORKGROUP\Administrator

ADMIN$
- Type: STYPE_DISKTREE_HIDDEN
- Comment: Remote Admin
- Users: 0
- Max Users: <unlimited>
- Path: C:\WINNT
- Anonymous access: <none>
- Current user access: READ/WRITE

C$
- Type: STYPE_DISKTREE_HIDDEN
- Comment: Default share
- Users: 0
- Max Users: <unlimited>
- Path: C:\
- Anonymous access: <none>
- Current user access: READ

IPC$
- Type: STYPE_IPC_HIDDEN
- Comment: Remote IPC
- Users: 1
- Max Users: <unlimited>
- Path:
- Anonymous access: READ
- Current user access: READ
### smb-enum-users

Host script results:

```
| smb-enum-users: |
| --- |--- |--- |
| _ _ Domain: RON-WIN2K-TEST; Users: Administrator, Guest, IUSR_RON-WIN2K-TEST, IWAM_RON-WIN2K-TEST, test1234, TsInternetUser |
```

Host script results:

```
| smb-enum-users: |
| --- |--- |--- |
| | RON-WIN2K-TEST\Administrator (RID: 500) |
| | | Description: Built-in account for administering the computer/domain |
| | | _ Flags: Password does not expire, Normal user account |
| | RON-WIN2K-TEST\Guest (RID: 501) |
| | | Description: Built-in account for guest access to the computer/domain |
| | | _ Flags: Password not required, Password does not expire, Normal user account |
| | RON-WIN2K-TEST\IUSR_RON-WIN2K-TEST (RID: 1001) |
| | | Full name: Internet Guest Account |
| | | Description: Built-in account for anonymous access to Internet Information Services |
| | | _ Flags: Password not required, Password does not expire, Normal user account |
| | RON-WIN2K-TEST\IWAM_RON-WIN2K-TEST (RID: 1002) |
| | | Full name: Launch IIS Process Account |
| | | Description: Built-in account for Internet Information Services to start out of process applications |
| | | _ Flags: Password not required, Password does not expire, Normal user account |
| | RON-WIN2K-TEST\test1234 (RID: 1005) |
| | | _ Flags: Normal user account |
| | RON-WIN2K-TEST\TsInternetUser (RID: 1000) |
| | | Full name: TsInternetUser |
| | | Description: This user account is used by Terminal Services. |
| _ _ _ Flags: Password not required, Password does not expire, Normal user account |
```
Clean machine (results printed only if extra verbosity ("-vv") is specified):
Host script results:
| p2p-conficker: Checking for Conficker.C or higher... |
| Check 1 (port 44329/tcp): CLEAN (Couldn't connect) |
| Check 2 (port 33824/tcp): CLEAN (Couldn't connect) |
| Check 3 (port 31380/udp): CLEAN (Failed to receive data) |
| Check 4 (port 52600/udp): CLEAN (Failed to receive data) |
| 0/4 checks: Host is CLEAN or ports are blocked |

Infected machine (results always printed):
Host script results:
| p2p-conficker: Checking for Conficker.C or higher... |
| Check 1 (port 18707/tcp): INFECTED (Received valid data) |
| Check 2 (port 65273/tcp): INFECTED (Received valid data) |
| Check 3 (port 11722/udp): INFECTED (Received valid data) |
| Check 4 (port 12690/udp): INFECTED (Received valid data) |
| 4/4 checks: Host is likely INFECTED |