

scanning

Matsuzaki 'maz' Yoshinobu

<maz@iij.ad.jp>

Stole slides from

Fakrul Alam

nmap (<https://nmap.org>)

- Nmap is a free and open source network exploration and security auditing tool
- Nmap was created by Gordon Lyon, a.k.a. Fyodor Vaskovich, and first published in 1997.
- Working cross-platform although best working on Linux-type environments
- It uses raw IP packets to determine
 - What hosts are available on the network
 - What services (application name and version)
 - Guesses the operational system, uptime and other characteristics

Ethical Issue

- Can be used for hacking-to discover vulnerable ports
- System admins ca use it to check that systems meet security standards
- Unauthorized use of Nmap on a system could be illegal.
- Make sure you have permission before using this tool.
- **There is no right way to do the wrong things**

Nmap : How it works

- DNS lookup-matches name with IP
- Nmap pings the remote target with 0 (zero) byte packets to each port
- If packets are not received back, port is open
- If packets are received, port is closed
- Firewall can interfere with this process

Nmap : Scanning Techniques

- Host Discovery and Target Specification
- Port Scanning Technique, Specification and order
- OS, Service and Version Detection
- nmap Scripting Engine
- Timing and Performance
- Firewall, IDS Evasion and Spoofing Technique
- Scan Report

Nmap: Scan

Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:

Can pass hostnames, IP addresses, networks, etc.

Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254

-iL <inputfilename>: Input from list of hosts/networks

-iR <num hosts>: Choose random targets

--exclude <host1[,host2][,host3],...>: Exclude hosts/networks

--excludefile <exclude_file>: Exclude list from file

OS DETECTION:

-O: Enable OS detection

--osscan-limit: Limit OS detection to promising targets

--osscan-guess: Guess OS more aggressively

Nmap: Scan

HOST DISCOVERY:

- sL: List Scan - simply list targets to scan
- sn: Ping Scan - disable port scan
- Pn: Treat all hosts as online -- skip host discovery
- PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
- PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
- PO[protocol list]: IP Protocol Ping
- n/-R: Never do DNS resolution/Always resolve [default: sometimes]
- dns-servers <serv1[,serv2],...>: Specify custom DNS servers
- system-dns: Use OS's DNS resolver
- traceroute: Trace hop path to each host

Nmap: Scan

SCAN TECHNIQUES:

- sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
- sU: UDP Scan
- sN/sF/sX: TCP Null, FIN, and Xmas scans
- scanflags <flags>: Customize TCP scan flags
- sI <zombie host[:probeport]>: Idle scan
- sY/sZ: SCTP INIT/COOKIE-ECHO scans
- s0: IP protocol scan
- b <FTP relay host>: FTP bounce scan

Exercise 1: Hostdiscovery

- ssh to workshop@nsXX.local
 - Note: XX is your group#
 - Note: password is iij/2497
- \$ `nmap -sP 10.0.1.0/24`

Exercise 2: Opening Ports

- Scan the host found in Exercise 1
- `$ nmap <$ip>`

Exercise 3: OS Fingerprint

- Guess the OS found in Exercise 1
- `$ nmap -O <ip>`

Exercise 4: Scan your client

- do not scan others'
- \$ nmap <your IP>
- What's kind of service running there?
- Let nmap guess your OS

Exercise 5: Version

- `$ nmap -sV 10.0.2.1`