CIS 700/002 : Special Topics : NMap

Kamenee Arumugam

Teng Zhang

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science

School of Engineering and Applied Science

University of Pennsylvania

Feb 24 2017

Introduction to NMap

- Nmap: A free and open source utility for network discovery and security auditing
- Nmap can check
  - what hosts are available on the network
  - what services are provided by the hosts
  - what OS are running on the hosts
  - what type of packet filters/firewalls are used
  - …
- Support scanning both single host or large scale network

Caution

- Scanning networks without permission to scan can get you in trouble
  - test on your internal network
  - test on machine provided by nmap.org
    - scanme.insecure.org
- Aggressively scanning may cause the network to crash
- Firewalls, routers, proxy servers, and other security devices can skew the results of an Nmap scan

Demo contents

- Basic scanning techniques
- Advanced options
- Port scanning options
- OS and service detection
- Timing options
- Evading firewalls
- Output options
- Troubleshooting and debugging
- Zenmap

Scan targets

- Single target
  - – nmap [target address]
- Multiple targets
  - – nmap [target1 target2 …]
- Subnet
  - – nmap [Network/CIDR]
- Random targets
  - – nmap -iR [number of targets]

Ping options

- No ping
  - nmap –P0 [target address]
- Ping only
  - nmap –sP [target address]
- TCP Syn ping
  - nmap –PS [target address]
- TCP Ack ping
  - nmap –PA [target address]
- Traceroute
  - nmap –traceroute [target address]
- UDP ping
  - nmap –PU [target address]

DNS resolution

- Disable dns reverse resolution
  - nmap –n [target address]
- Force reverse resolution
  - nmap –R [target address]
- Use dns servers in the system
  - nmap –system-dns [target address]
- Specify dns servers
  - nmap --dns-servers [server1,server2,etc] [target]

Scan options

- TCP connect scan
  - nmap –sT [target address]
- TCP syn scan
  - nmap -sS [target address]
- TCP ack scan
  - nmap –sA [target address]

Scan options(cont.)

- TCP Null scan
  - nmap –sN [target address]
- TCP Fin scan
  - nmap –sF [target address]
- TCP Xmas scan
  - nmap –sX [target address]
- UDP scan
  - nmap –sU [target address]
- IP scan
  - nmap –sO [target address]

Port scan options

- Fast scan
  - nmap –F [target address]
- Scan specific ports
  - nmap –p [port] [target address]
- Scan all ports
  - nmap –p “*” [target address]
- Scan top ports
  - nmap –top-ports [num] [target address]
- Scan sequential ports
  - nmap –r [target address]

OS & service detection

- OS detection
  - nmap –o [target address]
- OS guess
  - nmap –O –osscan-guess [target address]
- OS service version detection
  - nmap –sV [target address]

Timing options

- Timing templates
  - nmap –T[0-5] [target address]
- Parallelism
  - nmap –min-parallelism [number] [target address]
  - nmap –max-parallelism [number] [target address]
- Host timeout
  - nmap –host-timeout [time] [target address]
- Rate
  - nmap –min-rates [number] [target address]

Evading Firewalls

- Firewalls and intrusion prevention systems are designed to prevent tools like Nmap from getting an accurate picture of the systems they are protecting
- Nmap includes a number of features designed to circumvent these defenses.

Evading firewall - Features

Features	Feature Option
Fragment Packets	-f
Specify a Specific MTU	-mtu
Use a Decoy	-D
Idle Zombie Scan	-sI
Manually Specify a Source Port	--source-port
Append Random Data	--data-length
Randomize Target Scan Order	--randomize-hosts
Spoof MAC Address	--spoof-mac
Send Bad Checksums	--badsum

Demo – Evading Firewalls

- commands:
  - Fragment packets : nmap –f scanme.insecure.org
  - Using decoy addresses: nmap –D RND:10 scanme.insecure.org
  - Specific source port : nmap –source-port 53 scanme.insecure.org
  - Append random data: nmap –data-length 25 [target]
  - MAC spoofing addresses:nmap –sT –pN –spoof-mac 0

Output Options

- Feature Option
  - Save Output to a Text File -oN
  - Save Output to a XML File -oX
  - Grepable Output -oG
  - Output All Supported File Types -oA
  - Periodically Display Statistics --stats-every (-stats-every 5s instructs Nmap to display the status of the current scan every five seconds)
  - 133t Output -oS
- Demo

Troubleshooting and Debugging

- Feature Option
  - Help -h
  - Display Nmap Version -V
  - Verbose Output -v
  - Debugging –d
  - Display Port State Reason --reason
  - Only Display Open Ports --open
  - Trace Packets --packet-trace
  - Display Host Networking --iflist
  - Specify a Network Interface -e

Zenmap Overview

- a graphical frontend for Nmap
- cross-platform program - Windows, Mac OS X, and Unix/Linux systems
- Demo

Homework

- List all the open TCP and UDP ports of the host *scannme.insecure.org*
- Test if there are RPC services running on the *scannme.insecure.org*
- Get the public ssh-host key information from ssh service of the host *scannme.insecure.org*

Homework(Cont.)

- How to bypass and test firewall using the NMAP?
- Questions
  - Why ping scan is first done as an default option? If the icmp scan is blocked, what options can we use to scan the target?
  - When you scan the local network, what information can you get from Nmap that cannot be obtained when you scan the internet?

Solution

- nmap -p- -sU –sS scanme.insecure.org
- nmap –p- -sR scanme.insecure.org
- nmap –p- -A scanme.insecure.org
- https://www.hackingloops.com/nmap-scanning-tutorial-firewall-and-ids-evasion/
- ping can tell whether the target is up or down so that nmap will not waste time to scan targets that are not up. You can also use tcp syn or ack ping instead of icmp ping
- mac address information

Reference

- Nicholas Marsh, **Nmap® Cookbook** -*The fat-free guide to network scanning, 2010*