TNE30019/TNE80014 – Unix for Telecommunications

Network and Traffic Analysis Tools – NMap

Dr. Jason But

Swinburne University

Outline

NMap – Network Mapper

- Tool to scan and probe network for vulnerabilities
  - `http://insecure.org/nmap`
- Occasionally used by hackers – black hats
  - Find vulnerabilities in networks
  - Exploit broken systems
- Also used by administrators – white hats
  - Check for potential vulnerabilities in configured systems
  - Check configuration of firewalls and access to networks
- Multiple scan types
  - Detect different aspects of system you are scanning
  - Can be public or more stealthy to bypass basic security
- Need to be **root** to run many scan types
- Needs **raw sockets** for advanced scans (fails in FreeBSD jails)

NMap – Network Mapper

FreeBSD Port

`/usr/ports/security/nmap`

Scanning Etiquette

- Rude to scan computers and networks that you do not manage/own
  - Some administrators run port scan detection software
  - Many administrators view scans as precursor to attacks
  - You could get in trouble
  - On your own boxes – can detect services you have left open and may want to disable

NMap – Scan Types

Discovery

Discover active hosts in network

Port scan

Identify open (service listening) ports on hosts

Service probing

Identify server/service running on ports
Identify versions of server software running

OS detection / fingerprinting

Identify/guess OS running on host
Identify OS version

NMap – Scan Techniques

Ping Scan (Discovery)

- Like broadcast ping
- But each machine is pinged individually – bypasses kernel broadcast ping configuration

UDP Scan (Port scan / OS detection)

Attempt to determine open UDP ports

Basic TCP Scan (Port scan / OS detection)

Attempt to determine open TCP ports using `connect()`

TCP SYN Scan (Port scan / OS detection)

- Do only part of TCP handshake (send SYN, don't send ACK)
- Bypasses some detection systems

NMap – Scan Types

Many other TCP-related scans (mainly OS detection)

ACK, Window, FIN, Xmas, ... scans

IP protocol scan (for later scans / OS detection)

- Send IP packet of each known protocol
- Responses indicate whether host supports that protocol

Decoy scan

Send some scan packets with spoofed source IP address

Idle scan

- Hides source (scanner's) IP address from scanned machine
- http://nmap.org/book/idlescan.html

NMap – Network Mapper

- Some scans can take a while to complete
  - By default nmap scans 1,000 most common ports
  - But you scan all 65,535 ports
  - Delays configured in target system
  - Verbose mode displays progress – have a coffee or get a life

Graphical frontends

- **zenmap**
- Unix, OSX and Windows versions available
- Where to find it – your research

More documentation

`http://insecure.org/nmap/docs.html`
`http://www.nmap-tutorial.com`

NMap – Example

```
> nmap rule21.caia.swin.edu.au

Starting Nmap 5.51 ( http://nmap.org ) at 2014-09-18 11:59 EST
Nmap scan report for rule21.caia.swin.edu.au (136.186.230.21)
Host is up (0.0026s latency).
Not shown: 992 closed ports
PORT     STATE    SERVICE
7/tcp    open     echo
13/tcp   open     daytime
21/tcp   open     ftp
22/tcp   open     ssh
79/tcp   open     finger
80/tcp   open     http
110/tcp  open     pop3
143/tcp  open     imap

Nmap done: 1 IP address (1 host up) scanned in 7.67 seconds
```