Nmap in the Enterprise

By Paul Johnson
@bosconet

© 2019

All Enterprises are Snowflakes

This talk is based on my experience with 3 different enterprises over the past 10 years.

- Smallest enterprise “only” has ~340,000 live hosts
- Largest had over 800,00 live hosts
- All my enterprises spanned multiple physical location.

What’s nmap?

- A port scanner and more
- Free and Open Source since 1997
- Available at https://insecure.org

What else can nmap do?

- Discover Operating Systems
- Discover version of identified service on open ports
- Show network path from scanner to host
- Run scripts targeted at ports discovered

Why nmap?

- Free
- Scriptable
- Extendable
    - LUA
- Lots of Community Support

But I already have Nessus/Qualys/etc.

- Belt and suspenders
- Can compliment
- Can target ports/services not scanned by default
    - Default Qualys scan only scans 21-23, 25, 53, 80, 88, 110-111, 135, 139, 443, 445 and UDP Ports 53, 111, 135, 137, 161, 500 to determine if a host is alive
- Quality check

A word about OS discovery

- This should be considered a best effort service
- Uses tcp fingerprinting to make (reasonably) informed guess
- NOT always perfect
    - Most often printers will be misidentified as something else

Noise

- tcpfiltered ports
  - most of these are not really open
- Routing errors causing ‘random’ results
  - Errors?
    - Asymmetric routes
    - Routing loops
  - Results
    - Hosts that are live one scan but not another 2 minutes later
    - Ports open one scan and not another 2 minutes late
- Reduce noise by verifying traceroutes (i.e. add `--traceroute` switch to scans)

NSE Scripts

- Banner
- Ssl-cert
- http-title
- Smb-os-discovery
- ssh-brute/telnet-brute

NSE script: banner

- Connects to open port and dumps text returned from connection
    - Sometimes helpful
        - `banner: SSH-2.0-OpenSSH_5.9 FIPS`
        - `banner: 220 example.org FTP server (Version 4.2 Tue Feb 26 11:59:32 CST 2013) ready.`
        - `banner: 220 random.hostname.example.net Microsoft ESMTP MAIL Service ready at Sun, 9 Jun 2019 12:32:14 +0800`
    - Other times a correction to ‘identified’ service running on that port

```
902/tcp   open     nagios-nsca   Nagios NSCA
| banner: 220 VMware Authentication Daemon Version 1.10: SSL Required, ServerDaemonProtocol:SOAP,
MKSDisplayProtocol:VNC , , NFCSSL supported
```

-
    - Sometime not:
        - |_banner: \x80\x00\x00<\x00\x00\x00\x01\\xFB\x0F\xC0\x00\x00\x00\x00\x00\

NSE script: ssl-cert

- Captures the SSL certificate for the service
  - Can help ID expired certificates
  - Can help ID certificates expiring soon
  - Can also help ID what the service is (based on Subject: and/or Issuer: fields)
    - `Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser`

NSE script: smb-os-discovery

```
|    OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1 (Windows Server 2008 R2 Enterprise 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: userPC007
|   NetBIOS computer name: userPC007
|   Domain name: philadelphia.gov
|   Forest name: philadelphia.gov
|   FQDN: userPC007.philadelphia.gov
|_  System time: 2019-06-08T02:35:39+01:00
```

NSE script: ssh-brute / telnet-brute

- Does just what the name implies, brute force attack against ssh/telnet
- Can be leveraged to test for default credentials
  - Leverage SecLists on github
    - https://github.com/danielmiessler/SecLists/tree/master/Passwords/Default-Credentials
- **Warning**: you can easily lock accounts with this

Capture Entire Web Pages

- Http-fetch
  - Saves copy to locally defined directory
  - Lot of options to look for file extension/path/etc.
- Http-fetch-index
  - Personal fork of http-fetch
  - Grab’s default page (e.g. index.html)
  - Reports HTML text as output to console/XML

Other uses of NSE scripts

- Capture HTTP headers (http-headers)
    - Help identify operating systems
    - Show type and version of web server
- Discover 3rd party javascript used (http-referer-check)
- Display contents of robots.txt (http-robots)
- Enumerate users on your domain (smb-enum-users)
- Discover info about databases (ms-sql-info, mysql-info,mongodb-info)

Discover external data leaks

- Leveraging NSE can find internal IP data leakage in:
  - Ssl certs (ssl-cert)
  - BigIP cookies (bigip-cookie)
  - Error messages (http-fetch output)
  - HTTP get/ output (http-internal-ip-disclosure)
  - Via comments in pages (http-comments-displayer)
  - Mainframe terminals on network (tn3270-screen)

Leveraging the Data

- Discovering / confirming what is on your network
- Discovering what you didn't know
  - Devices out there being missed by other scannering
- Discovering services listening on well known ports but not that well know service
  - e.g. some internal agent listening on port 9898/tcp (monkeycom)
- Building a dataset of YOUR network.
  - What host mix do you expect to see
  - What port mix do you expect to see
- Dataset needs to be build over time

Saving Data

- Need to capture scan results to some data store to make useful
- By default nmap outputs to the console
- Can save data to 3 primary (useful) formats
  - -oN (.nmap) this is the same output you see on the console to a text file
  - -oG (.gnmap) this format is optimized for grepping
    - Not a full capture of data from scan especially if you use NSE scripts)
  - -oX (.xml) XML output containing all data for scan results.
    - Best format to use if you want to import data into something else
- For my needs I chose to feed the XML into a traditional RDBMS
  - ELK is also an option that I never tried

Something to Do with your Dataset

Idea 1: Build Top Ports for your organization

- Better know your network
- --top-ports scan switch
  - Can speed scanning
  - Most useful if you know what to expect
- Default data based on hundreds of scans conducted on public internet
  - Also not sure when it was last updated (most recent date in file from 2016)
- Public Internet != your internal network
  - Or even probably your public footprint

nmap’s top 5 ports

RANK	Service	Port/Proto	frequency
1	http	80/tcp	0.484143
2	telnet	23/tcp	0.221265
3	https	443/tcp	0.208669
4	ftp	21/tcp	0.197667
5	ssh	22/tcp	0.182286

Real World External top 5 ports

RANK	Service	Port/Proto	Default rank	frequency
1	http	80/tcp	1	0.480274
2	https	443/tcp	3	0.479685
3	ftp	21/tcp	4	0.002774
4	ssh	22/tcp	5	0.002245
5	domain	53/tcp	12	0.001717

Real World Internal top 5 ports

RANK	Service	Port/Proto	Default rank	frequency
1	https	443/tcp	3	0.065009
2	http	80/tcp	1	0.051483
3	ssh	22/tcp	5	0.050666
4	msrpc	135/tcp	13	0.045409
5	ms-wbt-server (RDP)	3389/tcp	7	0.044784

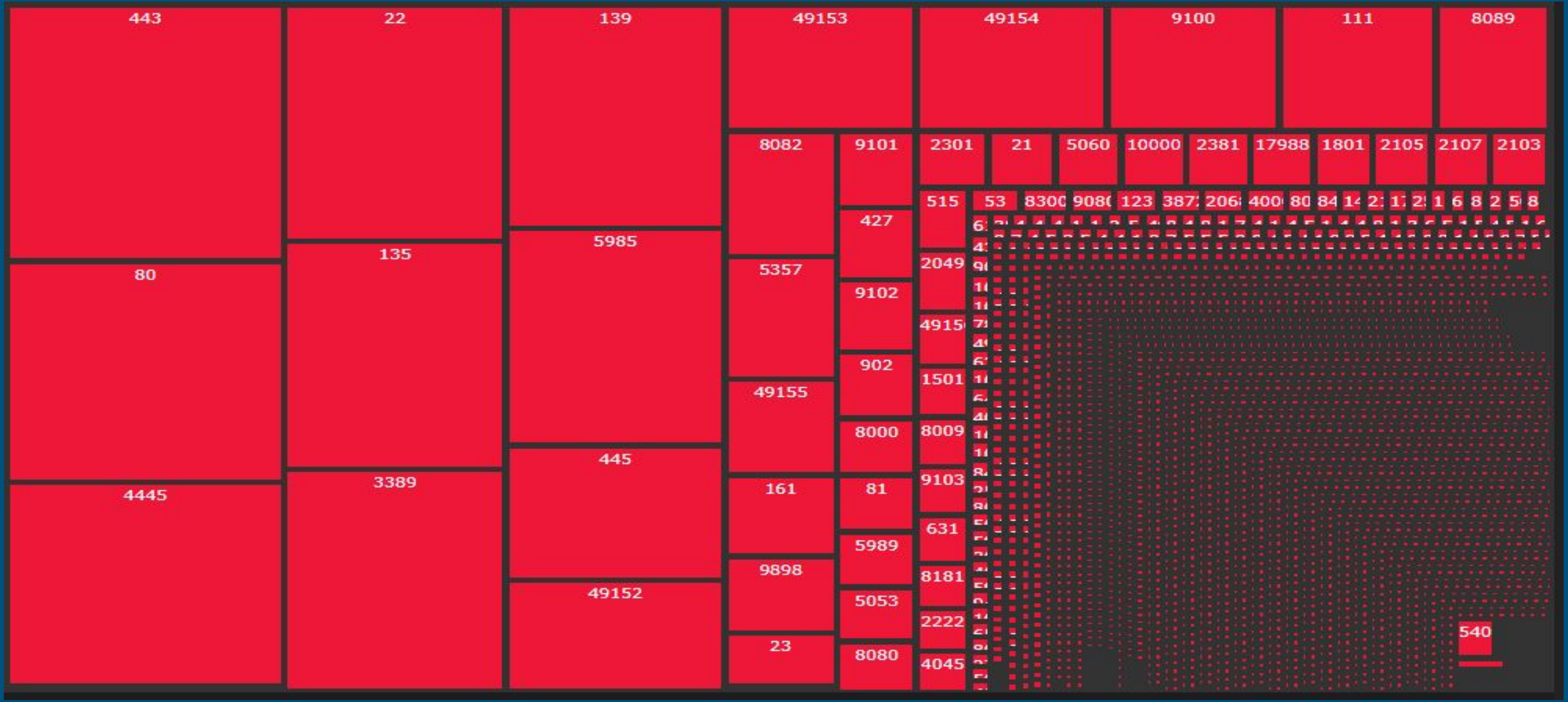
Idea 2: Audit software versions in use

- Using -sV switch capture version information
  - Use it to see if you have old vulnerable software in use
    - Qualys/Nessus might catch this but not always
  - Help track movement to standardize on versions of software
  - Find software you didn’t even know what in use on the network

Idea 3: Find Rogue Devices / Services

- That network printer isn’t one of our approved/standard models
- That windows hosts isn’t part of the domain
- Why does the domain server have VNC installed on port 1137/tcp
- Why is there a Raspberry Pi on the management network?
- Why do we have 3 open proxies that aren’t the official one?

Idea 4: Visualize Some Data (open ports)



What about massscan?

- Massscan
    - Able to scan VAST amounts of network space quickly
    - Comes at the cost of scanning limited amount of ports quickly
    - ‘Stateless’
        - Sends out ALL the tcp SYN packets at once and waits to see who answers…
    - DefCon 22 talk by authors (https://www.youtube.com/watch?v=UOWexFaRylM)

Questions?