2018 KANSAS CITY BSIDES

Many thanks to our BSidesKC 2018 sponsors!!!

Platinum

Cerner

Gold

FORTINET

McAfee™ Together is power.

corelight

OPTIV

Carbon Black.

RSA

Silver

SIRIUS SECURITY

fishtech

netskope

CRITICALSTART

RAVENii MANAGE. GUARD. DELIVER.

ixia A Keysight Business

DEPTH SECURITY

PACKETSLED

Bronze

SANS

Brass

elastic

A la Carte, Workshops, Villages, & Gifts

AM Cyber Inc. Safe. Secure. Together. info@amcyber.org

netgate

Check Point SOFTWARE TECHNOLOGIES LTD.

burst iQ

KCP&L energizing life

SANS

no starch press

Westar Energy Taking energy to heart.

riskgenius

KANSAS CITY LEGAL HACKERS

I Am The Cavalry

HACKERBOXES

ForeScout

KUDELSKI SECURITY

pfsense

POLSINELLI INSURTECH

HAK5

Gigamon

paloalto NETWORKS

THOMSON REUTERS

From Port Scanning to Password Cracking

If you’re not using NMAP, you’re doing IT wrong

And want to do other stuff

Disclaimer

All views are my own. This presentation is purely informational and I’m not responsible for how you use it. I.e. breaking things, legal stuff, etc.

About Me

Security Analyst at a large data company.

Vulnerability management to cloud security.

GCIH Certified.

Live in Columbia, Mo.

10+ years in the IT Industry

Help_desk>sysadmin>133t

Twitter: @jeredbare


ARROW ROOT PHOTOGRAPHY


ARROW ROOT PHOTOGRAPHY

NMAP

Security scanner written by Gordon Lyon.

Port scanning.

Discovering hosts on the network.

Service and version discovery.

But….did you know….

NMAP can do the following...

Brute Force and crack passwords.

Check for weak ciphers on websites.

See if your host(s) is vulnerable to WannaCry.

Exploit vulnerable software.

How does it do that?

NSE Scripting Engine.

Custom scripts written by the community.

All the scripts are written in the embedded LUA Language.

Hundreds of scripts that have particular use.

FUN!

Library nmap

Interface with Nmap internals.

The nmap module is an interface with Nmap's internal functions and data structures. The API provides target host details such as port states and version detection results. It also offers an interface to the Nsock library for efficient network I/O.

Functions

address_family ()	Returns the address family Nmap is using.
bind (addr, port)	Sets the local address of a socket.
clock ()	Returns the current date and time in seconds.
clock_ms ()	Returns the current date and time in milliseconds.
close ()	Closes an open connection.
condvar (object)	Create a condition variable for an object.
connect (host, port, protocol)	Establishes a connection.
debugging ()	Returns the debugging level as a non-negative integer.
ethernet_close ()	Closes an ethernet interface.
ethernet_open (interface_name)	Opens an ethernet interface for raw packet sending.
ethernet_send (packet)	Sends a raw ethernet frame.
fetchfile (filename)	Searches for the specified file relative to Nmap's search paths and returns a string containing its path if it is found and readable (to the process). Absolute paths and paths relative to the current directory will not be searched.
get_info ()	Gets information about a socket.
get_interface ()	Returns the interface name (dnet-style) that Nmap is using.
get_interface_info (interface_name)	Gets the interface network information.
get_payload_length ()	Returns the payload data length selected with the --data-length option
get_port_state (host, port)	Gets a port table for a port on a given host.
get_ports (host, port, proto, state)	Iterates over port tables matching protocol and state for a given host
get_ssl_certificate ()	Retrieves the SSL certificate of the peer. The returned value can be accessed like a table and has the following members:
get_ttl ()	Returns the TTL (time to live) value selected by the --ttl option
have_ssl ()	Determines whether Nmap was compiled with SSL support.
ip_close ()	Closes a raw IPv4 socket.
ip_open ()	Opens a socket for raw IPv4 packet sending.
ip_send (packet, dst)	Sends a raw IPv4 or IPv6 packet.

How do I get started?

What You'll Need.

Permission

- ALWAYS ask for permission to run this tool on your network. If using the Cloud ***cough AWS*** you MUST fill out a Penetration test form and submit to the Cloud Gods.

A host: Windows, Linux, Mac OSX, Docker.

- I prefer a Mac OSX and/or a virtual Linux host.

NMAP Software

- https://nmap.org/download.html

What You'll Need Continued

Scripting Experience

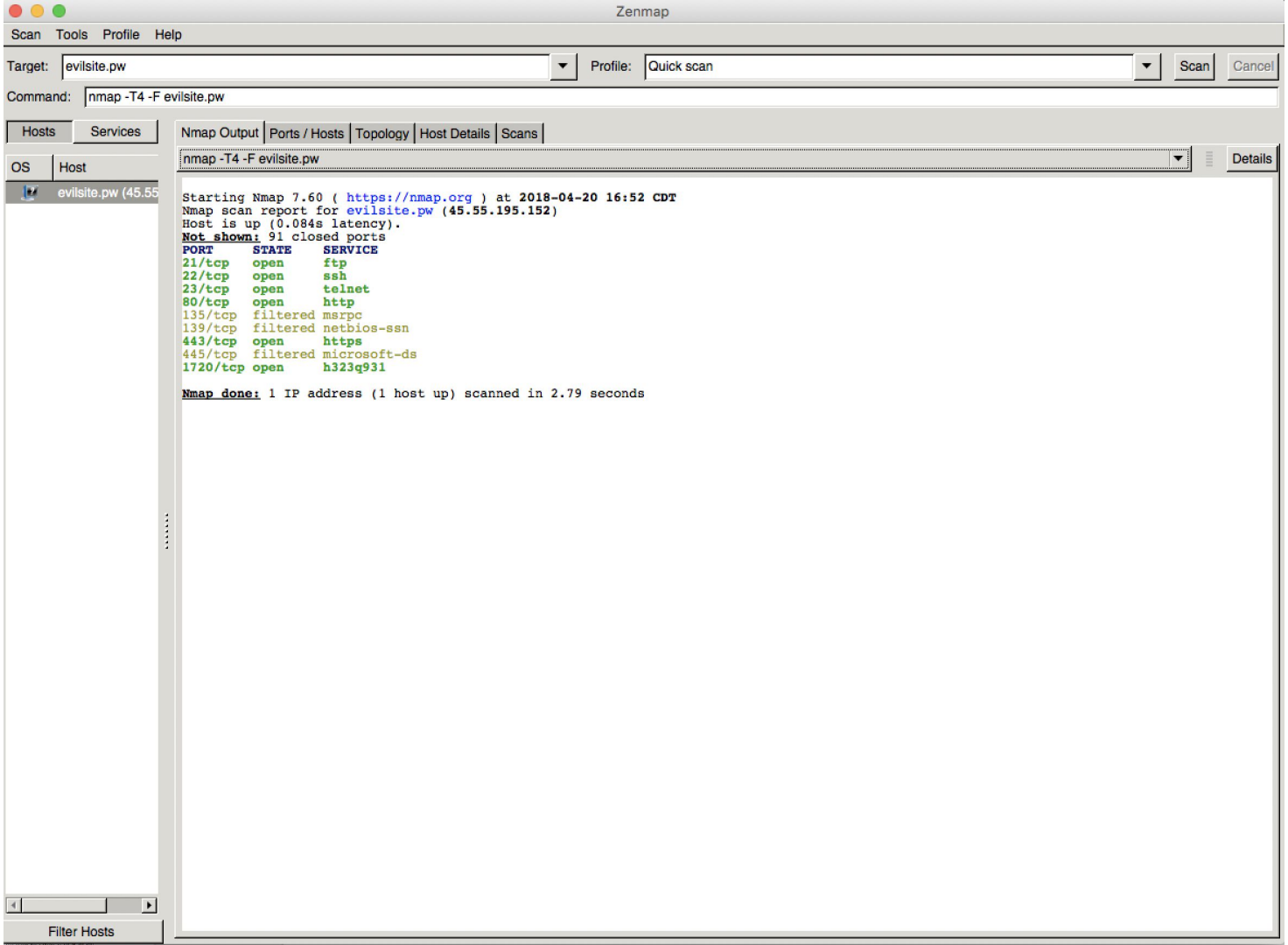
- Preferred, but not required.

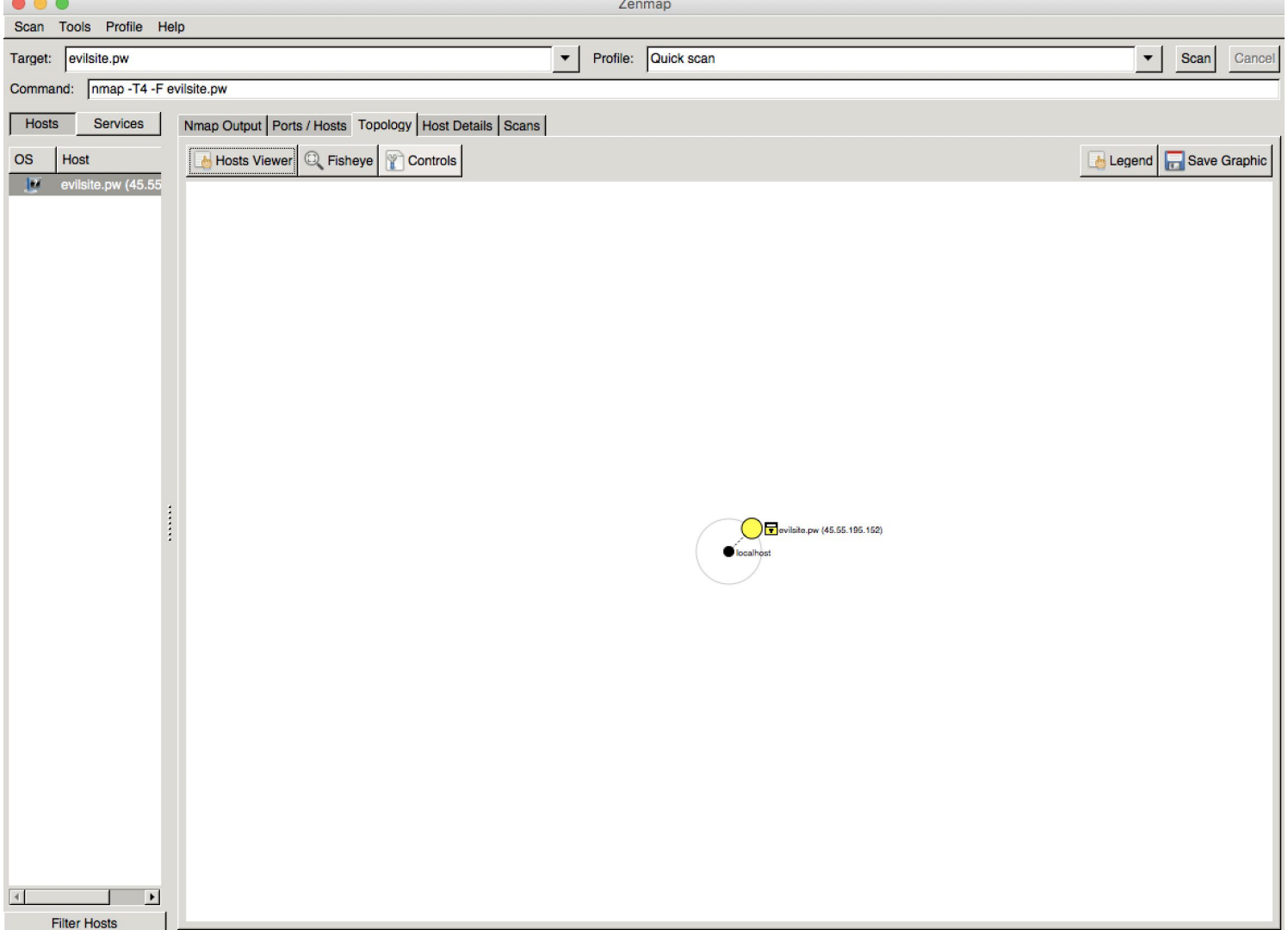
Familiarity with the command line

- Bash, Windows Command Prompt, Powershell, etc.

No command line experience?

- Use ZenMap -- a GUI interface for NMAP.


Zenmap
Scan Tools Profile Help
Target: evilsite.pw
Profile: Quick scan
Scan
Cancel
Command: nmap -T4 -F evilsite.pw
Hosts
Services
OS
Host
evilsite.pw (45.55
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -F evilsite.pw
Details
Starting Nmap 7.60 (https://nmap.org) at 2018-04-20 16:52 CDT
Nmap scan report for evilsite.pw (45.55.195.152)
Host is up (0.084s latency).
Not shown: 91 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
80/tcp open http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open https
445/tcp filtered microsoft-ds
1720/tcp open h323q931
Nmap done: 1 IP address (1 host up) scanned in 2.79 seconds


Zenmap
Scan Tools Profile Help
Target: evilsite.pw
Profile: Quick scan
Scan Cancel
Command: nmap -T4 -F evilsite.pw
Hosts Services
OS Host
evilsite.pw (45.55
Nmap Output Ports / Hosts Topology Host Details Scans
Hosts Viewer Fisheye Controls
Legend Save Graphic
evilsite.pw (45.55.195.152)
localhost
Filter Hosts

NMAP Commands

Basic NMAP Commands

nmap [host or ip_address or cidr_range]

- Basic scan.

nmap -T4 -A [host or ip_address or cidr_range]

- Runs a quicker scan with OS detection and checks a few other things, i.e. http headers, certs, ssh hostkey. etc.

nmap -sV [host or ip_address or cidr_range]

- My favorite starting command.

```
Jereds-MacBook-Pro:~ jeredbare$ nmap evilsite.pw

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-19 20:43 CDT
Nmap scan report for evilsite.pw (45.55.195.152)
Host is up (0.066s latency).
Not shown: 991 closed ports
PORT    STATE    SERVICE
21/tcp  open     ftp
22/tcp  open     ssh
23/tcp  open     telnet
80/tcp  open     http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
443/tcp open     https
445/tcp filtered microsoft-ds
593/tcp filtered http-rpc-epmap

Nmap done: 1 IP address (1 host up) scanned in 6.39 seconds
Jereds-MacBook-Pro:~ jeredbare$
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-20 17:02 CDT
Nmap scan report for evilsite.pw (45.55.195.152)
Host is up (0.066s latency).
Not shown: 988 closed ports
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 3.0.3
22/tcp   open     ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 e4:79:1c:9c:05:86:52:39:94:59:13:a3:ed:7a:16:84 (RSA)
|   256 16:24:32:88:bc:f7:72:25:26:50:22:bb:e0:29:98:3c (ECDSA)
|_  256 84:11:3c:52:7b:74:55:b3:f3:0d:5c:1f:72:12:d5:60 (EdDSA)
23/tcp   open     telnet       Linux telnetd
80/tcp   open     http         Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: EvilSite.pw | A non-malicious testing site
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     ssl/ssl      Apache httpd (SSL-only mode)
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: EvilSite.pw | A non-malicious testing site
| ssl-cert: Subject: commonName=Quit Checking/organizationName=Totally Not a Self-Signed Cert/stateOrProvinceName=Missouri/countryName=US
| Not valid before: 2017-06-13T04:00:41
|_Not valid after:  2018-06-13T04:00:41
|_ssl-date: ERROR: Script execution failed (use -d to debug)
445/tcp  filtered microsoft-ds
1023/tcp filtered netvenuechat
1720/tcp open     h323q931?
2967/tcp filtered symantec-av
9898/tcp filtered monkeycom
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.31 seconds
```

```
Jereds-MacBook-Pro:~ jeredbare$ nmap -sV evilsite.pw

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-20 16:58 CDT
Nmap scan report for evilsite.pw (45.55.195.152)
Host is up (0.068s latency).
Not shown: 988 closed ports
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 3.0.3
22/tcp   open     ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
23/tcp   open     telnet       Linux telnetd
80/tcp   open     http         Apache httpd 2.4.18 ((Ubuntu))
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     ssl/ssl      Apache httpd (SSL-only mode)
445/tcp  filtered microsoft-ds
1023/tcp filtered netvenuechat
1720/tcp open     h323q931?
2967/tcp filtered symantec-av
9898/tcp filtered monkeycom
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.03 seconds
```

Useful NMAP Commands

nmap -T4 -A [host or ip_address or cidr_range] -oN [file.txt]

- Outputs the information into a file. You can use the flags -oX for xml, -oS for script kiddie and -oG for a grepable format. -oA will output the format in all three.

nmap -sV -iL [target_list.txt]

- Using a combination of IP addresses, CIDR ranges and hostnames to feed nmap a target list.

Nmap -sV -6 [host or ip_address or cidr_range]

- Scans for IPV6 Hosts

Before moving on….

REMEMBER THE DISCLAIMER


I'M NOT JUST SERIOUS,
I'M DEAD SERIOUS.
imgflip.com

K. Let’s have some fun.

Brute Forcing a Server

1. Going to run this command to start to see what services are listening.
    a. nmap -sV evilsite.pw
2.

```
Jereds-MacBook-Pro:~ jeredbare$ nmap -sV evilsite.pw

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-20 17:32 CDT
Nmap scan report for evilsite.pw (45.55.195.152)
Host is up (0.068s latency).
Not shown: 988 closed ports
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 3.0.3
22/tcp   open     ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
23/tcp   open     telnet       Linux telnetd
80/tcp   open     http         Apache httpd 2.4.18 ((Ubuntu))
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     ssl/ssl      Apache httpd (SSL-only mode)
445/tcp  filtered microsoft-ds
1023/tcp filtered netvenuechat
1720/tcp open     h323q931?
2967/tcp filtered symantec-av
9898/tcp filtered monkeycom
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Brute Forcing a Server

1. Going to run this command to start to see what services are listening.
   a. nmap -sV evilsite.pw
2. Let’s use the telnet-brute NSE Script to brute force port 23.
   a. Create list of users and common passwords.

```
Jereds-MacBook-Pro:~ jeredbare$ vi users.txt
Jereds-MacBook-Pro:~ jeredbare$
```

```
admin
tadmin
administrator
bill
root
```

```
Jereds-MacBook-Pro:~ jeredbare$ vi pws.txt
```

```
password
password1234
admin
hamsandwich
Spring2018!
toor
```

Brute Forcing a Server

1. Going to run this command to start to see what services are listening.
   a. nmap -sV evilsite.pw
2. Let’s use the telnet-brute NSE Script to brute force port 23.
   a. Create list of users and common passwords.
3. EXECUTE.
   a. nmap --script telnet-brute --script-args userdb=users.txt,passdb=pws.txt [host]

```
Jereds-MacBook-Pro:~ jeredbare$ nmap --script telnet-brute  --script-args userdb=users.txt,passdb=pws.txt evilsite.pw

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-20 17:48 CDT
Nmap scan report for evilsite.pw (45.55.195.152)
Host is up (0.063s latency).
Not shown: 988 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
22/tcp   open     ssh
23/tcp   open     telnet
| telnet-brute:
|   Accounts:
|     tadmin:password1234 - Valid credentials
|_  Statistics: Performed 27 guesses in 10 seconds, average tps: 2.7
80/tcp   open     http
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     https
445/tcp  filtered microsoft-ds
1023/tcp filtered netvenuechat
1720/tcp open     h323q931
2967/tcp filtered symantec-av
9898/tcp filtered monkeycom
```

Some More Brute Forcing Scripts

1. SSH
   a. nmap --script ssh-brute [host]
2. MySQL.
   a. nmap --script mysql-brute [host]
3. LDAP and SMB.
   a. nmap -p 389 --script ldap-brute --script-args ldap.base='"cn=users,dc=cqure,dc=net"' <host>
   b. nmap --script smb-brute.nse -p445 <host>
4. And Many more!
   a. Check out https://nmap.org/nsedoc/categories/brute.html

What else was listening on the host?

```
Jereds-MacBook-Pro:~ jeredbare$ nmap -sV evilsite.pw

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-20 18:20 CDT
Nmap scan report for evilsite.pw (45.55.195.152)
Host is up (0.071s latency).
Not shown: 988 closed ports
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 3.0.3
22/tcp   open     ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
23/tcp   open     telnet       Linux telnetd
80/tcp   open     http         Apache httpd 2.4.18 ((Ubuntu))
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     ssl/ssl      Apache httpd (SSL-only mode)
445/tcp  filtered microsoft-ds
1023/tcp filtered netvenuechat
1720/tcp open     h323q931?
2967/tcp filtered symantec-av
9898/tcp filtered monkeycom
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.62 seconds
```

Testing TLS

1. Checking the certificate (expiration, self-signed)
    a. nmap --script ssl-cert

```
Jereds-MacBook-Pro:~ jeredbare$ nmap -sV --script ssl-cert evilsite.pw

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-20 18:22 CDT
Nmap scan report for evilsite.pw (45.55.195.152)
Host is up (0.083s latency).
Not shown: 988 closed ports
PORT     STATE    SERVICE      VERSION
21/tcp   open     ftp          vsftpd 3.0.3
22/tcp   open     ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
23/tcp   open     telnet       Linux telnetd
80/tcp   open     http         Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     ssl/ssl      Apache httpd (SSL-only mode)
|_http-server-header: Apache/2.4.18 (Ubuntu)
| ssl-cert: Subject: commonName=Quit Checking/organizationName=Totally Not a Self-Signed Cert/stateOrProvinceName=Missouri/countryName=US
| Issuer: commonName=Quit Checking/organizationName=Totally Not a Self-Signed Cert/stateOrProvinceName=Missouri/countryName=US
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-06-13T04:00:41
| Not valid after:  2018-06-13T04:00:41
| MD5:   ce15 3433 bec7 3c46 8f6a 6cbc 80e8 b015
|_SHA-1: 7cb3 be56 2443 5633 7b01 3f5d 5046 9ad2 4007 0b1d
445/tcp  filtered microsoft-ds
1023/tcp filtered netvenuechat
1720/tcp open     h323q931?
2967/tcp filtered symantec-av
9898/tcp filtered monkeycom
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
 ssl-cert: Subject: commonName=Quit Checking/organizationName=Totally Not a Self-Signed Cert/stateOrProvinceName=Missouri/countryName=US
 Issuer: commonName=Quit Checking/organizationName=Totally Not a Self-Signed Cert/stateOrProvinceName=Missouri/countryName=US
 Public Key type: rsa
 Public Key bits: 1024
 Signature Algorithm: sha256WithRSAEncryption
 Not valid before: 2017-06-13T04:00:41
 Not valid after:  2018-06-13T04:00:41
 MD5:   ce15 3433 bec7 3c46 8f6a 6cbc 80e8 b015
_SHA-1: 7cb3 be56 2443 5633 7b01 3f5d 5046 9ad2 4007 0b1d
```

Testing TLS

1. Checking the certificate (expiration, self-signed).
    a. nmap --script ssl-cert [host]
2. Check the ciphers.
    a. nmap --script ssl-enum-ciphers [host]

```
443/tcp  open     ssl/ssl      Apache httpd (SSL-only mode)
|_http-server-header: Apache/2.4.18 (Ubuntu)
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_SEED_CBC_SHA (dh 1024) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (brainpoolP256r1) - D
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (brainpoolP256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (brainpoolP256r1) - A
|       TLS_ECDHE_RSA_WITH_RC4_128_SHA (brainpoolP256r1) - D
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - D
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 1024) - D
|       TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - D
|       TLS_RSA_WITH_SEED_CBC_SHA (rsa 1024) - A
|     compressors:
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
```

```
|   TLSv1.1:
|     ciphers:
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 1024) - A
|       TLS_DHE_RSA_WITH_SEED_CBC_SHA (dh 1024) - A
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (brainpoolP256r1) - D
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (brainpoolP256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (brainpoolP256r1) - A
|       TLS_ECDHE_RSA_WITH_RC4_128_SHA (brainpoolP256r1) - D
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - D
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 1024) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 1024) - D
|       TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - D
|       TLS_RSA_WITH_SEED_CBC_SHA (rsa 1024) - A
|     compressors:
|       NULL
|     cipher preference: client
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
```

```
    TLSv1.2:
      ciphers:
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - D
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - A
        TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 1024) - A
        TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 1024) - A
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - A
        TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 1024) - A
        TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 1024) - A
        TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 1024) - A
        TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 1024) - A
        TLS_DHE_RSA_WITH_SEED_CBC_SHA (dh 1024) - A
        TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (brainpoolP256r1) - D
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (brainpoolP256r1) - A
        TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (brainpoolP256r1) - A
        TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (brainpoolP256r1) - A
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (brainpoolP256r1) - A
        TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (brainpoolP256r1) - A
        TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (brainpoolP256r1) - A
        TLS_ECDHE_RSA_WITH_RC4_128_SHA (brainpoolP256r1) - D
        TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - D
        TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - A
        TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 1024) - A
        TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 1024) - A
        TLS_RSA_WITH_AES_256_CBC_SHA (rsa 1024) - A
        TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 1024) - A
        TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 1024) - A
        TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 1024) - A
        TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 1024) - A
        TLS_RSA_WITH_RC4_128_MD5 (rsa 1024) - D
        TLS_RSA_WITH_RC4_128_SHA (rsa 1024) - D
        TLS_RSA_WITH_SEED_CBC_SHA (rsa 1024) - A
      compressors:
        NULL
      cipher preference: client
      warnings:
        64-bit block cipher 3DES vulnerable to SWEET32 attack
        Broken cipher RC4 is deprecated by RFC 7465
        Ciphersuite uses MD5 for message integrity
_   least strength: D
```

Trivia

TLS 1.0 is Vulnerable to what?

TLS 1.0 is Vulnerable to what?

POODLE ATTACK!

Testing TLS

1. Checking the certificate (expiration, self-signed)
    a. nmap --script ssl-cert [host]
2. Check the ciphers
    a. nmap --script ssl-enum-ciphers [host]
    b. Find the vulnerable protocol.
3. ATTACK

FYI: you can combine scripts, see example below

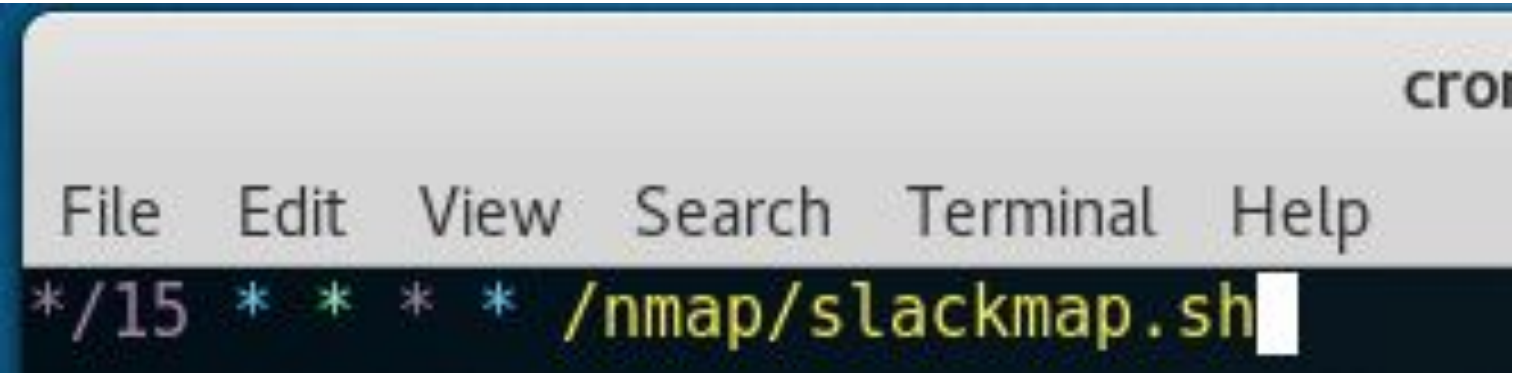
- nmap --script ssl-cert,ssl-enum-ciphers -p [port] [host]

Advanced NMAP

1. Build your own scripts.
    a. Use the power of your favorite scripting language to build scripts.
        i. Bash, python
    b. Practice building an NSE Script.
        i. Get familiar with LUA.
2. Automate tasks.
    a. If using Linux or Mac OSX, setup CRON jobs to sweep your network.
        i. Check for self-signed certs in your environment.
        ii. Test to see if there are open ports in a sensitive environment (CDE).
3. Contribute to the community by building your own NSE Script.
    a. Write it in the LUA language or C.

```
#!/bin/sh
TARGETS="192.168.1.0/24"
OPTIONS="-v -T4 -F -sV"
date=$(date +%Y-%m-%d-%H-%M-%S)
cd /nmap/diffs
nmap $OPTIONS $TARGETS -oA scan-$date > /dev/null
slack(){
curl -F file=@diff-$date -F initial_comment="Internal Port Change Detected" -F channels=#alerts -F token=xxxx-xxxx-xxxx https://slack.com/api/files.upload
}

if [ -e scan-prev.xml ]; then
ndiff scan-prev.xml scan-$date.xml > diff-$date
[ "$?" -eq "1" ] && sed -i -e 1,3d diff-$date && slack
fi
ln -sf scan-$date.xml scan-prev.xml
```



#alerts
1 | 0 | Add a topic

Search

Set a purpose + Add an app or custom integration Invite others to this channel

Today

networkalerts BOT 4:37 PM
added and commented on a Plain Text snippet: **diff-2016-11-05-21-37-38**

```
 PORT   STATE SERVICE    VERSION
-26/tcp open  smtp       Exim smtpd 4.86_1
+26/tcp open  tcpwrapped
```

External Port Change Detected

networkalerts BOT 4:45 PM
added and commented on a Plain Text snippet: **diff-2016-11-05-14-41-26**

```
+192.168.1.105:
-Host is up.
+Host is down.
-Not shown: 100 closed ports

 Macintosh
 PORT   STATE SERVICE      VERSION
-88/tcp open  kerberos-sec Heimdal Kerberos (server time: 2016-11-05 21:37:54Z)
+88/tcp open  kerberos-sec Heimdal Kerberos (server time: 2016-11-05 21:42:52Z)

+192.168.1.164:
-Host is up.
+Host is down.
-Not shown: 88 closed ports
 PORT      STATE    SERVICE          VERSION
-79/tcp    filtered finger
-106/tcp   filtered pop3pw
-179/tcp   filtered bgp
-543/tcp   filtered klogin
-646/tcp   filtered ldp
-3000/tcp  filtered ppp
-3128/tcp  filtered squid-http
-4899/tcp  filtered radmin
-5060/tcp  filtered sip
-5631/tcp  filtered pcanywheredata
-8081/tcp  filtered blackice-icecap
-10000/tcp filtered snet-sensor-mgmt
```

Internal Port Change Detected

Message #alerts

Vulnerability Detection

1. Using NMAP as a vulnerability scanner.
   a. nmap --script vuln [host].
2. Check for WannaCry vunlerable hosts
   a. nmap --script smb-vuln-ms17-010
3. Check for the infamous ms08-067 (I hope not) :(
   a. nmap --script smb-vuln-ms08-067

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-20 22:27 CDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for evilsite.pw (45.55.195.152)
Host is up (0.071s latency).
Not shown: 988 closed ports
PORT     STATE    SERVICE
21/tcp   open     ftp
|_sslv2-drown:
22/tcp   open     ssh
23/tcp   open     telnet
80/tcp   open     http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
443/tcp  open     https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| ssl-dh-params:
```

```
  ssl-dh-params:
    VULNERABLE:
    Diffie-Hellman Key Exchange Insufficient Group Strength
      State: VULNERABLE
        Transport Layer Security (TLS) services that use Diffie-Hellman groups
        of insufficient strength, especially those using one of a few commonly
        shared groups, may be susceptible to passive eavesdropping attacks.
      Check results:
        WEAK DH GROUP 1
              Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
              Modulus Type: Safe prime
              Modulus Source: RFC2409/Oakley Group 2
              Modulus Length: 1024
              Generator Length: 8
              Public Key Length: 1024
      References:
        https://weakdh.org
_
_sslv2-drown:
445/tcp  filtered microsoft-ds
1023/tcp filtered netvenuechat
1720/tcp open     h323q931
2967/tcp filtered symantec-av
9898/tcp filtered monkeycom
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 13:33 CDT
Nmap scan report for vulnr-host-inside-the-network (127.0.0.1)
Host is up (0.00048s latency).
PORT    STATE SERVICE
445/tcp open  microsoft-ds
Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
```

Disclaimers

1. NMAP is kind of a controversial tool.
2. You can and will go to jail.
3. If used or not approve through the proper chain, it could end up very bad for you.
4. Always, always get permission: in writing and in blood.

Summary

1. NMAP is a free and widely supported tool that can be used in your arsenal.
2. There is not a huge learning curve and anyone can learn the program.
3. It’s highly customizable to fit whatever environment you work in.
4. Last but not least, IT’S FUN!

Resources

1. https://nmap.org
2. https://nmap.org/nsedoc/index.html
3. https://www.lua.org/

Thank you!

Slides will be posted to my github later today.

Let’s Connect:

Twitter: @jeredbare

Linkedin: jeredbare

Help us get better!

Please provide feedback on…		
my talk	**the conference**	**anything else**
		
http://bit.ly/BSidesKC2018-TalkEval	http://bit.ly/BSidesKC2018-EventEval	http://bit.ly/IqT6zt