Who Plugged That In?

DISCOVERING WHAT IS ON YOUR NETWORK WITH NMAP AND OTHER OPEN SOURCE TOOLS

MY VIEWS ARE MINE AND DO NOT REPRESENT MY EMPLOYER'S.

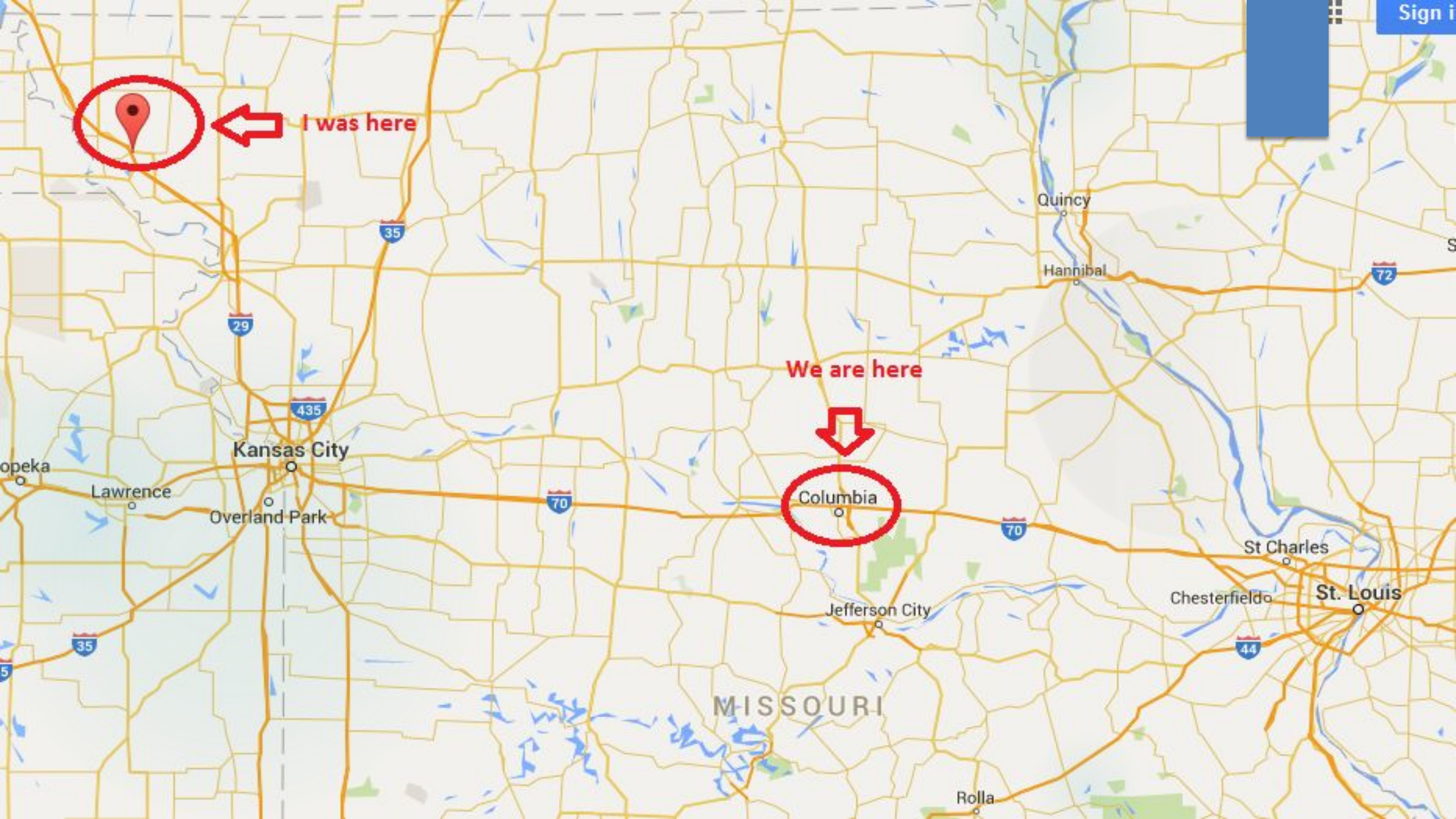
I'm not responsible for how you use this information. Use at your own risk. Sorry…..

:'(

TWITTER: @JEREDBARE
EMAIL: JEREDBARE@GMAIL.COM
CELL: 573-355-0676

Who am I?

- IT Security Analyst at CarFax
- From a small town called Mound City, MO


I was here
We are here
Quincy
Hannibal
Kansas City
Lawrence
Overland Park
Columbia
Jefferson City
St Charles
Chesterfield
St. Louis
MISSOURI
Rolla
35
29
435
70
72
44

Who am I?

- IT Security Analyst for CarFax
- From a small town called Mound City, MO.
- Currently Live in CoMo, Central MO for six years.
- Working in IT for nine years (Tech, Sysadmin, Security).
- SANS Courses
  - 505 Securing Windows
  - 504 Hacker Tools, Techniques, and Incident Handling
    - GCIH Certified
    - Winning team for SANS 504 CTF
- Passion for Information Security.

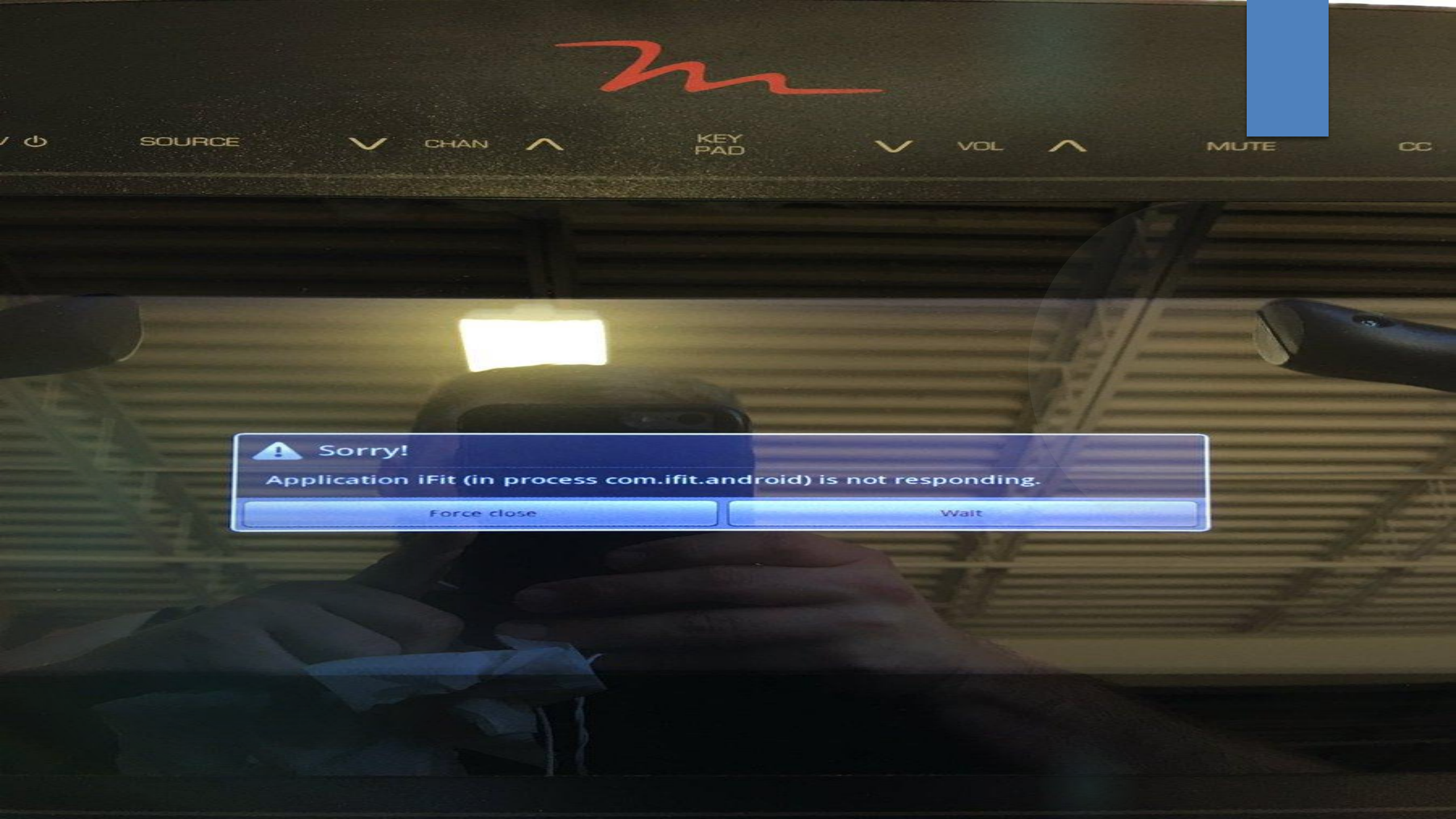
What exactly is on my network?

Why is this good to know?

- Help others secure their networks to prevent them from attacking ours.
- Maybe this is or is not your first time working with IT.
- Previous employee did not do a good job with IT or Security.
- Maybe this talk will get you involved in the community.

How this information can help you

- Critical Security Controls 1
  - Inventory of Authorized and Unauthorized Devices
- NIST Core Frameworks
  - ID.AM-1
  - ID.AM-3
  - ID.AM-4
  - PR.DS-3
- How do you know what to protect?
- Approved Software?
  - Dropbox
- IoT or IoE
  - Smart Phones, tablets, thermostats, treadmills, etc.


SOURCE
CHAN
KEY PAD
VOL
MUTE
CC
Sorry!
Application iFit (in process com.ifit.android) is not responding.
Force close
Wait

Remember Target?

- In 2013 Target was breached and the hackers were able to get access to 110 million people's credit and debit card information.
- HVAC Third Party vendor had a server that had access rights to the network. Failed to segment network.
- Home Depot, JP Morgan, Neiman Marcus

A Look Back at the Target Breach

Target settles for $39 million over data breach

One more company…….

THE EQUIFAX BREACH EXPOSES AMERICA'S IDENTITY CRISIS

EQUIFAX®

Equifax Breach Fallout: Your Salary History

Why the Equifax breach is very possibly the worst leak of personal info ever

Tools

Open Source Tools

- Internal Scanning
  - Command Line
    - NMAP
    - Passive Discovery Scripts
  - GUI
    - ZenMap
    - Sparta (Kali Linux)
    - Wireshark
- External Scanning
  - Certificate Logging Tools
  - Cloud Services
  - Shodan
  - Warberry Pi
  - RainMap
  - Automation/Scripting

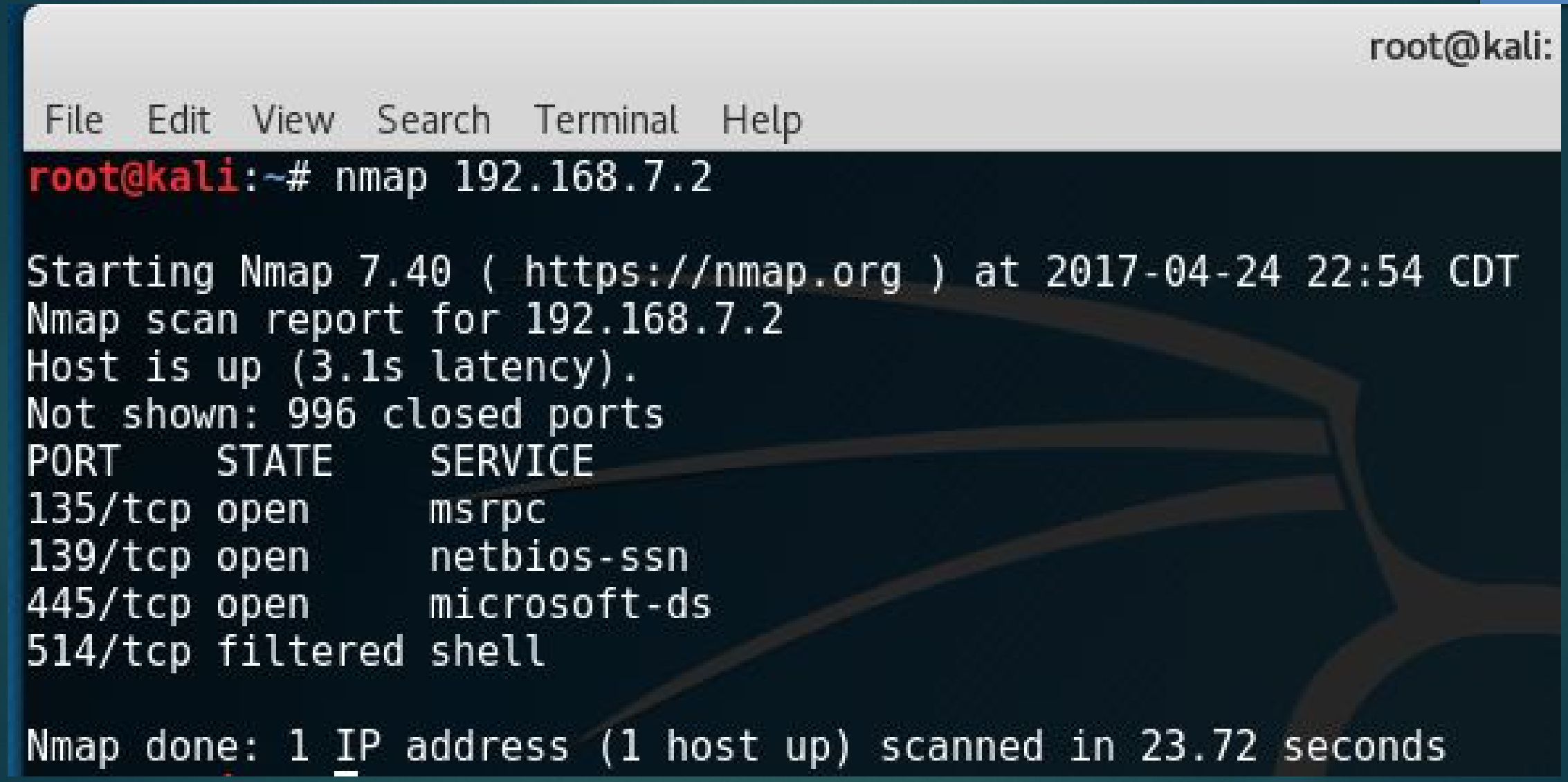
Why?

- Maximum Visibility
  - Known knows, know unknowns, unknown unknowns
- Open Source
  - Free!
  - Software kept up to date
  - Passionate Community

Command Line Tools

- NMAP
  - Network security scanner for network discovery and security auditing.
  - Built-in scripting engine to make it more than a port scanner.
  - Outstanding documentation and examples.
  - Universal Platform: Windows, Mac OSX, Linux.
  - nmap.org
- Passive Discovery Scripts
  - Set of scripts by Lee Baird
  - Scanning, Recon, Automation penetration testing for your network.
  - Use in Kali Linux. https://github.com/leebaird/discover

NMAP Scanning an IP and Subnet

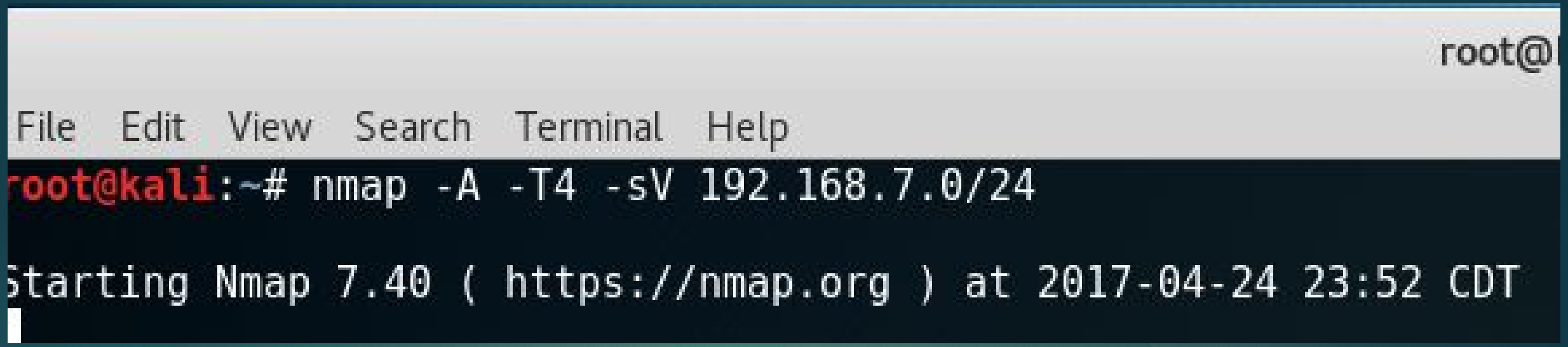


```
root@kali:~# nmap 192.168.7.0/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-24 23:37 CDT
Nmap scan report for 192.168.7.1
Host is up (0.0083s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
443/tcp open  https

Nmap scan report for 192.168.7.2
Host is up (0.015s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

NMAP Scanning a subnet



```
Nmap scan report for 192.168.7.2
Host is up (0.0011s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Windows XP microsoft-ds
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.40%E=4%D=4/24%OT=135%CT=1%CU=38453%PV=Y%DS=2%DC=T%G=Y%TM=58FED7
OS:12%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=I%TS=0)OPS(O1=M5B4N
OS:W0NNT00NNS%O2=M5B4NW0NNT00NNS%O3=M5B4NW0NNT00%O4=M5B4NW0NNT00NNS%O5=M5B4
OS:NW0NNT00NNS%O6=M5B4NNT00NNS)WIN(W1=FAF0%W2=FB90%W3=FC80%W4=FB40%W5=FB40%
OS:W6=FB8B)ECN(R=Y%DF=Y%T=80%W=FAF0%O=M5B4NW0NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S
OS:=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=N%T=80%W=0%S=Z%A=S+%
OS:F=AR%O=%RD=0%Q=)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=80%IPL=B0%UN=0%RIPL=G%RID=G%
OS:RIPCK=G%RUCK=G%RUD=G)IE(R=N)

Network Distance: 2 hops
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 7h50m43s, deviation: 0s, median: 7h50m43s
|_nbstat: NetBIOS name: VULNRXP, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:7e:1e:af (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: vulnrXP
|   NetBIOS computer name: VULNRXP\x00
|   Domain name: vulnr.local
|   Forest name: vulnr.local
|   FQDN: vulnrXP.vulnr.local
|_  System time: 2017-04-25T07:46:52-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
```

```
Nmap scan report for 192.168.7.4
Host is up (0.0026s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE           VERSION
53/tcp    open  domain            Microsoft DNS
88/tcp    open  kerberos-sec      Microsoft Windows Kerberos (server time: 2017-04-25 12:44:01Z)
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
389/tcp   open  ldap              Microsoft Windows Active Directory LDAP (Domain: vulnr.local, Site: Default-First-Site-Name
445/tcp   open  microsoft-ds      Windows Server 2012 R2 Datacenter 9600 microsoft-ds (workgroup: VULNR)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap              Microsoft Windows Active Directory LDAP (Domain: vulnr.local, Site: Default-First-Site-Name
3269/tcp  open  tcpwrapped
3389/tcp  open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=WINSERV-VULNR.vulnr.local
| Not valid before: 2017-02-28T09:34:08
|_Not valid after:  2017-08-30T09:34:08
|_ssl-date: 2017-04-25T12:46:52+00:00; +7h50m43s from scanner time.
49152/tcp open  msrpc             Microsoft Windows RPC
49153/tcp open  msrpc             Microsoft Windows RPC
49154/tcp open  msrpc             Microsoft Windows RPC
49155/tcp open  msrpc             Microsoft Windows RPC
49157/tcp open  ncacn_http        Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc             Microsoft Windows RPC
49159/tcp open  msrpc             Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Network Distance: 2 hops
Service Info: Host: WINSERV-VULNR; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 7h50m42s, deviation: 0s, median: 7h50m42s
|_nbstat: NetBIOS name: WINSERV-VULNR, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:b0:0d:b5 (VMware)
| smb-os-discovery:
|   OS: Windows Server 2012 R2 Datacenter 9600 (Windows Server 2012 R2 Datacenter 6.3)
```

NMAP Scripting Engine

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-25 00:01 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 192.168.7.2
Host is up (0.012s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 57.67 seconds
```

My Favorite NMAP Commands

- nmap –script ssl-cert,ssl-enum-ciphers –p 443 [network range]
  - Scans the network range for SSL certificates and their associated ciphers.
  - Good for finding weak signing alogrithms
- nmap –script=resolveall --script-args=newtargets, resolveall.hosts=example.com
  - Scans all IPs the hostname resolves to.
- nmap –A –T4 –sV –iL [document.txt]
  - Will scan a document full of hosts and IP Addresses.
- nmap –A –T4 –sV [ip address or subnet] –oN [document_name.txt]
  - Outputs nmap information into a document.
- nmap –A –T4 –sV [ip address or subnet] –oX [document_name.xml[
  - Outputs nmap information into a XML document.

NMAP Scripting Engine

NSEDoc

Index
NSE Documentation

Categories
auth
broadcast
brute
default
discovery
dos
exploit
external
fuzzer
intrusive
malware
safe
version
vuln

Scripts (show 561)
Libraries (show 125)

Scripts

acarsd-info	Retrieves information from a listening acarsd daemon. Acarsd decodes ACARS (Aircraft Communication Addressing and Reporting Sys and listening frequency.
address-info	Shows extra information about IPv6 addresses, such as embedded MAC or IPv4 addresses when available.
afp-brute	Performs password guessing against Apple Filing Protocol (AFP).
afp-ls	Attempts to get useful information about files from AFP volumes. The output is intended to resemble the output of `ls`.
afp-path-vuln	Detects the Mac OS X AFP directory traversal vulnerability, CVE-2010-0533.
afp-serverinfo	Shows AFP server information. This information includes the server's hostname, IPv4 and IPv6 addresses, and hardware type (for exan
afp-showmount	Shows AFP shares and ACLs.
ajp-auth	Retrieves the authentication scheme and realm of an AJP service (Apache JServ Protocol) that requires authentication.
ajp-brute	Performs brute force passwords auditing against the Apache JServ protocol. The Apache JServ Protocol is commonly used by web serv
ajp-headers	Performs a HEAD or GET request against either the root directory or any optional directory of an Apache JServ Protocol server and retu
ajp-methods	Discovers which options are supported by the AJP (Apache JServ Protocol) server by sending an OPTIONS request and lists potentially
ajp-request	Requests a URI over the Apache JServ Protocol and displays the result (or stores it in a file). Different AJP methods such as; GET, HEA
allseeingeye-info	Detects the All-Seeing Eye service. Provided by some game servers for querying the server's status.
amqp-info	Gathers information (a list of all server properties) from an AMQP (advanced message queuing protocol) server.
asn-query	Maps IP addresses to autonomous system (AS) numbers.
auth-owners	Attempts to find the owner of an open TCP port by querying an auth daemon which must also be open on the target system. The auth s
auth-spoof	Checks for an identd (auth) server which is spoofing its replies.
backorifice-brute	Performs brute force password auditing against the BackOrifice service. The `backorifice-brute.ports` script argument is mandato
backorifice-info	Connects to a BackOrifice service and gathers information about the host and the BackOrifice service itself.
bacnet-info	Discovers and enumerates BACNet Devices collects device information based off standard requests. In some cases, devices may not s Presence of this error positively identifies the device as a BACNet device, but no enumeration is possible.
banner	A simple banner grabber which connects to an open TCP port and prints out anything sent by the listening service within five seconds.
bitcoin-getaddr	Queries a Bitcoin server for a list of known Bitcoin nodes
bitcoin-info	Extracts version and node information from a Bitcoin server
bitcoinrpc-info	Obtains information from a Bitcoin server by calling `getinfo` on its JSON-RPC interface.
bittorrent-discovery	Discovers bittorrent peers sharing a file based on a user-supplied torrent file or magnet link. Peers implement the Bittorrent protocol and used to track the peers. The sets of peers and nodes are not the same, but they usually intersect.
bjnp-discover	Retrieves printer or scanner information from a remote device supporting the BJNP protocol. The protocol is known to be supported by r
broadcast-ataoe-discover	Discovers servers supporting the ATA over Ethernet protocol. ATA over Ethernet is an ethernet protocol developed by the Brantley Coile
broadcast-avahi-dos	Attempts to discover hosts in the local network using the DNS Service Discovery protocol and sends a NULL UDP packet to each host t
broadcast-bjnp-discover	Attempts to discover Canon devices (Printers/Scanners) supporting the BJNP protocol by sending BJNP Discover requests to the netwo
broadcast-db2-discover	Attempts to discover DB2 servers on the network by sending a broadcast request to port 523/udp.
broadcast-dhcp-discover	Sends a DHCP request to the broadcast address (255.255.255.255) and reports the results. The script uses a static MAC address (DE:A
broadcast-dhcp6-discover	Sends a DHCPv6 request (Solicit) to the DHCPv6 multicast address, parses the response, then extracts and prints the address along w
broadcast-dns-service-discovery	Attempts to discover hosts' services using the DNS Service Discovery protocol. It sends a multicast DNS-SD query and collects all the r

Passive Discovery Scripts

```
administrators-MacBook-Pro:Desktop jeredbare$ git clone https://github.com/leebaird/discover.git discover_scripts
Cloning into 'discover_scripts'...
remote: Counting objects: 6116, done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 6116 (delta 10), reused 17 (delta 6), pack-reused 6094
Receiving objects: 100% (6116/6116), 27.11 MiB | 5.59 MiB/s, done.
Resolving deltas: 100% (4156/4156), done.
```

```
root@kali:/opt/discover# ./discover.sh
```

By Lee Baird

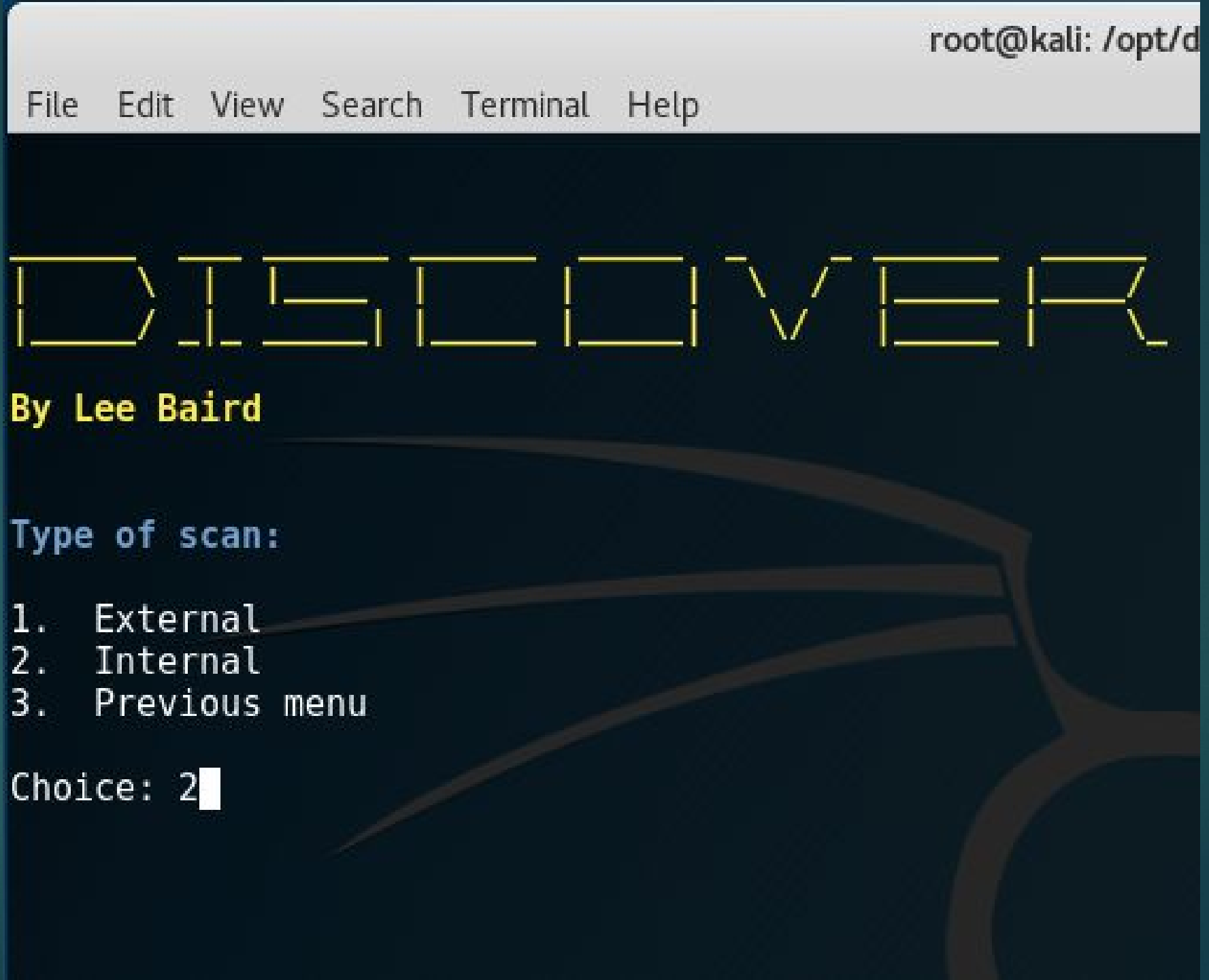
RECON
1. Domain
2. Person
3. Parse salesforce

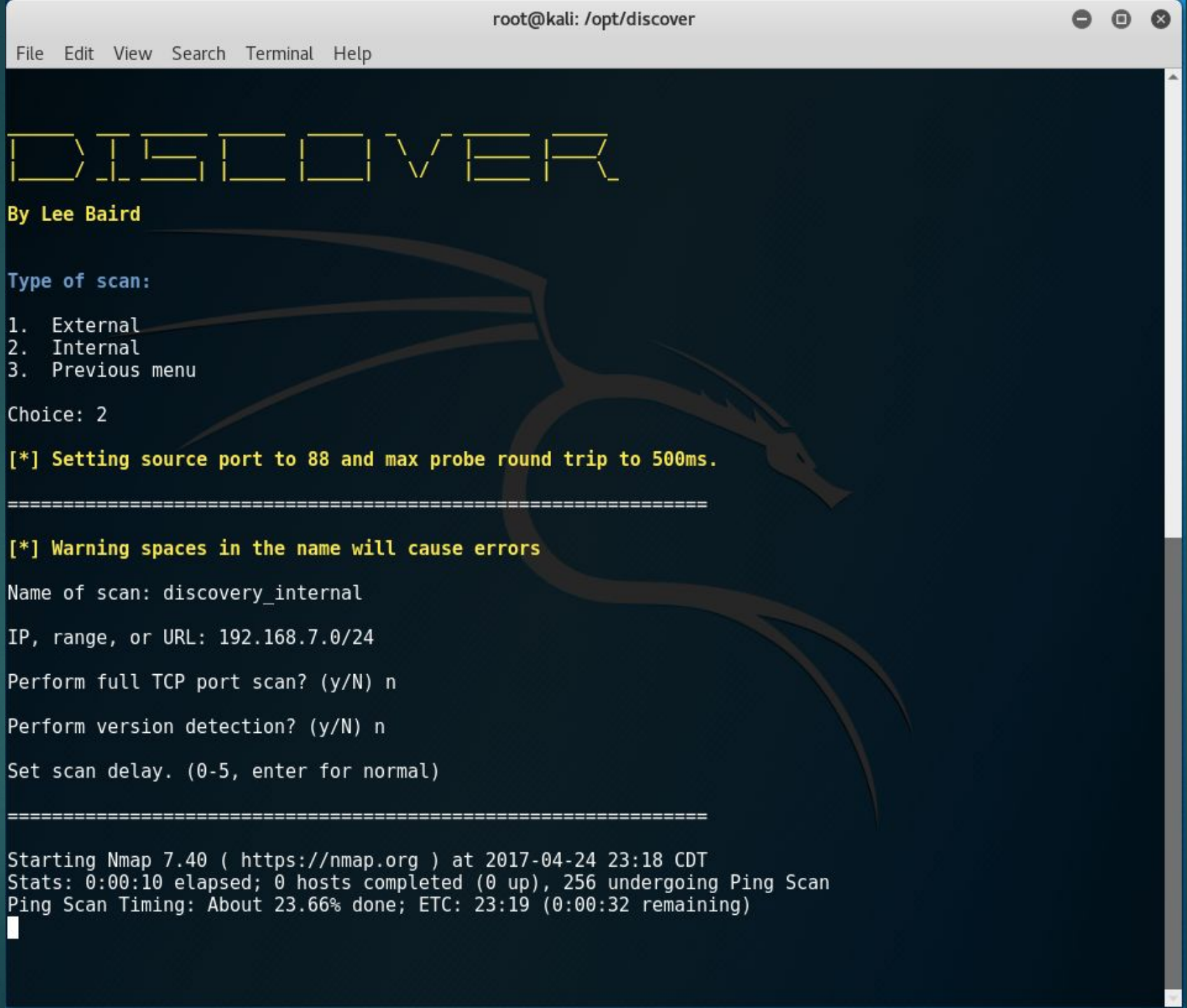
SCANNING
4. Generate target list
5. CIDR
6. List
7. IP, range, or URL
8. Rerun Nmap scripts and MSF aux.

WEB
9. Insecure direct object reference
10. Open multiple tabs in Firefox
11. Nikto
12. SSL

MISC
13. Crack WiFi
14. Parse XML
15. Generate a malicious payload
16. Start a Metasploit listener
17. Update
18. Exit

Choice:


root@kali: /opt/d
File Edit View Search Terminal Help
By Lee Baird
Type of scan:
1. External
2. Internal
3. Previous menu
Choice: 2


root@kali: /opt/discover
File Edit View Search Terminal Help
By Lee Baird
Type of scan:
1. External
2. Internal
3. Previous menu
Choice: 2
[*] Setting source port to 88 and max probe round trip to 500ms.
[*] Warning spaces in the name will cause errors
Name of scan: discovery_internal
IP, range, or URL: 192.168.7.0/24
Perform full TCP port scan? (y/N) n
Perform version detection? (y/N) n
Set scan delay. (0-5, enter for normal)
Starting Nmap 7.40 (https://nmap.org) at 2017-04-24 23:18 CDT
Stats: 0:00:10 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Ping Scan Timing: About 23.66% done; ETC: 23:19 (0:00:32 remaining)

How - GUI

- ZenMap
  - GUI interface to nmap.
  - Can run all the same commands as you would from the command line.
- Sparta
  - Network, port and vulnerability scanner.
  - Included in Kali Linux
  - Be careful with this tool!
- Wireshark
  - Network protocol analyzer.
  - Can see what is exactly going on in your network.
  - Universal Platform: Windows, Mac OSX, Linux.
  - https://www.wireshark.org/

Zenmap

Scan Tools Profile Help

Target: 192.168.7.2 Profile: Scan Cancel

Command: nmap -sV -T4 -A 192.168.7.2

Hosts Services

OS Host

192.168.7.2

work

Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sV -T4 -A 192.168.7.2 Details

```
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: vulnrXP
|   NetBIOS computer name: VULNRXP\x00
|   Domain name: vulnr.local
|   Forest name: vulnr.local
|   FQDN: vulnrXP.vulnr.local
|_  System time: 2017-04-25T07:37:10-05:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but
default)
|_smbv2-enabled: Server doesn't support SMBv2
protocol

TRACEROUTE (using port 199/tcp)
HOP RTT     ADDRESS
1   0.70 ms 192.168.4.1
2   1.78 ms 192.168.7.2

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

Zenmap

Scan Tools Profile Help

Target: 192.168.7.2 Profile: Scan Cancel

Command: nmap -sV -T4 -A 192.168.7.2

Hosts Services

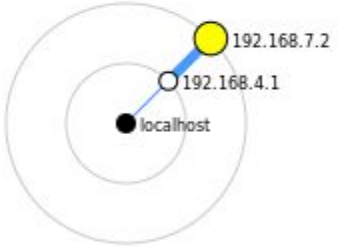
OS Host

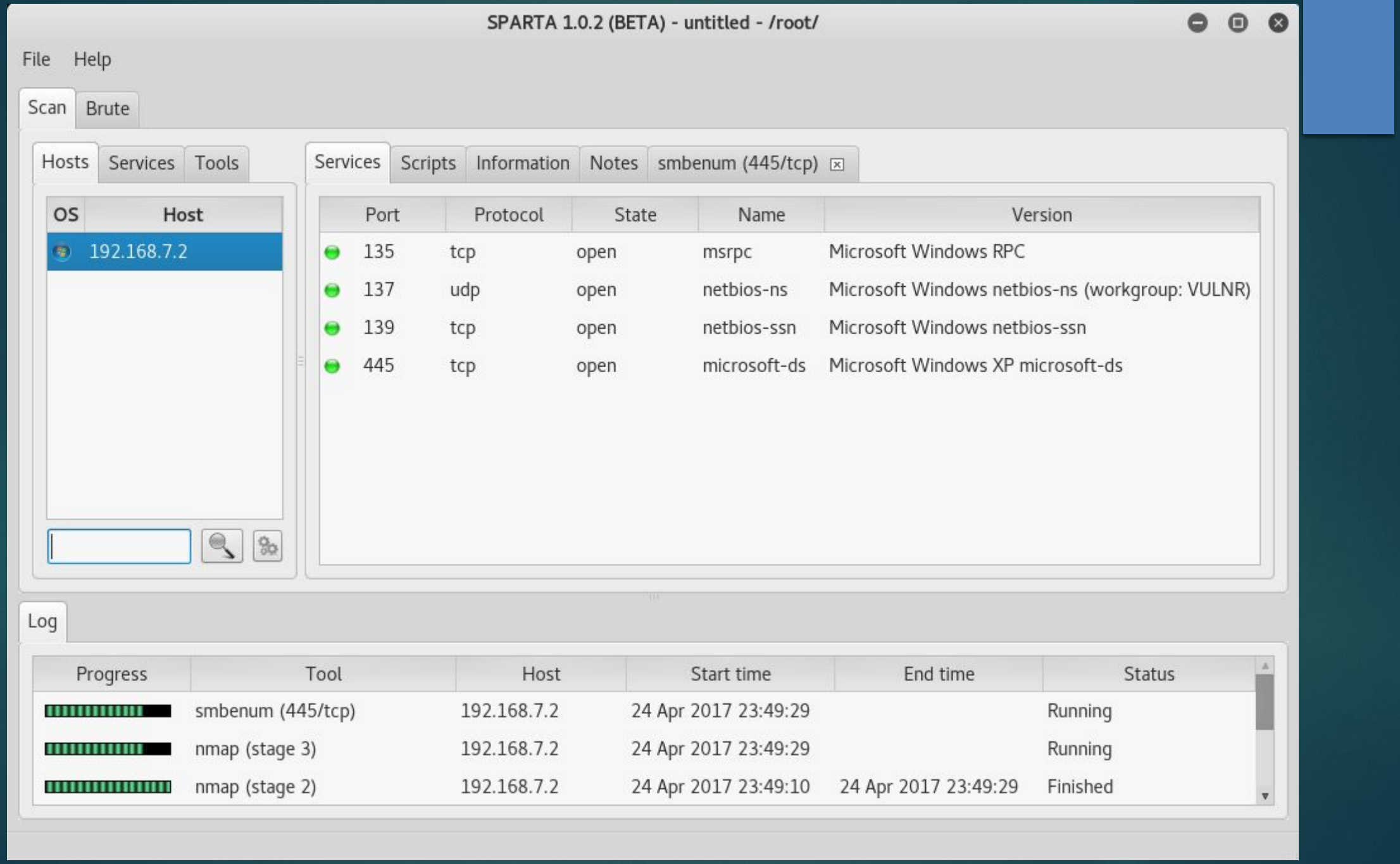
192.168.7.2

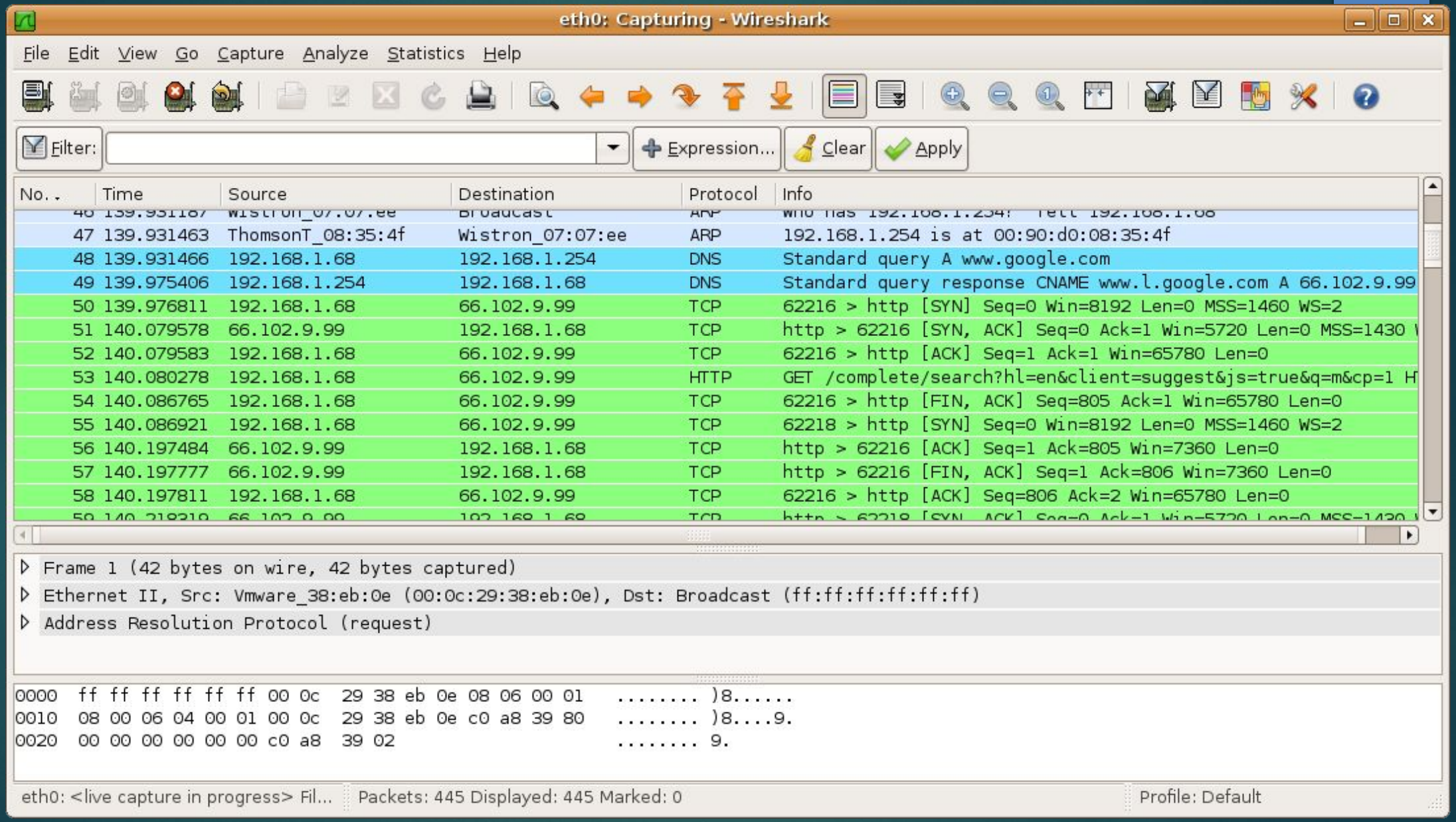
Filter Hosts

Nmap Output Ports / Hosts Topology Host Details Scans

Hosts Viewer Fisheye Controls Legend Save Graphic




SPARTA 1.0.2 (BETA) - untitled - /root/
File
Help
Scan
Brute
Hosts
Services
Tools
OS
Host
192.168.7.2
Services
Scripts
Information
Notes
smbenum (445/tcp)
Port
Protocol
State
Name
Version
135 tcp open msrpc Microsoft Windows RPC
137 udp open netbios-ns Microsoft Windows netbios-ns (workgroup: VULNR)
139 tcp open netbios-ssn Microsoft Windows netbios-ssn
445 tcp open microsoft-ds Microsoft Windows XP microsoft-ds
Log
Progress
Tool
Host
Start time
End time
Status
smbenum (445/tcp) 192.168.7.2 24 Apr 2017 23:49:29 Running
nmap (stage 3) 192.168.7.2 24 Apr 2017 23:49:29 Running
nmap (stage 2) 192.168.7.2 24 Apr 2017 23:49:10 24 Apr 2017 23:49:29 Finished


eth0: Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
47 139.931463 ThomsonT_08:35:4f Wistron_07:07:ee ARP 192.168.1.254 is at 00:90:d0:08:35:4f
48 139.931466 192.168.1.68 192.168.1.254 DNS Standard query A www.google.com
49 139.975406 192.168.1.254 192.168.1.68 DNS Standard query response CNAME www.l.google.com A 66.102.9.99
50 139.976811 192.168.1.68 66.102.9.99 TCP 62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
51 140.079578 66.102.9.99 192.168.1.68 TCP http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
52 140.079583 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
53 140.080278 192.168.1.68 66.102.9.99 HTTP GET /complete/search?hl=en&client=suggest&js=true&q=m&cp=1
54 140.086765 192.168.1.68 66.102.9.99 TCP 62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
55 140.086921 192.168.1.68 66.102.9.99 TCP 62218 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
56 140.197484 66.102.9.99 192.168.1.68 TCP http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
57 140.197777 66.102.9.99 192.168.1.68 TCP http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
58 140.197811 192.168.1.68 66.102.9.99 TCP 62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
Frame 1 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 0c 29 38 eb 0e 08 06 00 01 ....)8......
0010 08 00 06 04 00 01 00 0c 29 38 eb 0e c0 a8 39 80 ....)8....9.
0020 00 00 00 00 00 00 c0 a8 39 02 .... 9.
eth0: <live capture in progress> Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

How – Web Based/API

- Censys.io
  - Search Engine that allows to search for open devices and to see how they are configured. Shows various technologies open to the internet.
- Shodan
  - Search Engine that crawls the internet for open devices.
  - IP Cams, Virtualization Servers, Home servers.
- Certificate Logging Tools
  - Tool to find SSL certificates associated with your organization
  - Easy to use and setup.

How – Advanced - External

- Warberry Pi
  - Penetration testing tool suite on a Raspberry Pi
  - As soon as you plug in the device it will start running scripts.
  - Will monitor network activity, IP addresses, and MAC addresses.
  - https://github.com/secgroundzero/warberry/wiki
- RainMap
  - Web application that allows users to launch Nmap scans from their browser.
  - Easy to use and graphical interface.
  - https://github.com/cldrn/rainmap-lite
- Automation/Scripting
  - Write your own tools and use the advanced features of NMAP.
  - All of these tools can be ran on a small Linux Server.
- Cloud Scanning
  - DigitalOcean
  - Amazon AWS

Censys.io and Shodan.io

172.98.67.120

Summary | Details | JSON | WHOIS | Raw WHOIS

Basic Information

Network TOTAL-SERVER-SOLUTIONS — Total Server Solutions L.L.C., US

Routing 172.98.67.0/24 via AS7018, AS3257, AS5580, AS46562 AS46562 AS46562

Protocols 443/HTTPS, 22/SSH

22/SSH

Banner Grab

Details

Banner: SSH-2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8

Country United States (US)

Lat/Long 38.0, -97.0

TOTAL RESULTS

3

TOP COUNTRIES

United States	1
Brazil	1
Bulgaria	1

TOP SERVICES

55034	1
23499	1
8999	1

TOP ORGANIZATIONS

Verizon Fios	1
Tim Celular S.A.	1
Bulsatcom EAD	1

173.71.219.195

pool-173-71-219-195.clppva.fios.verizon.net

Verizon Fios

Added on 2017-04-03 09:31:47 GMT

United States, Fredericksburg

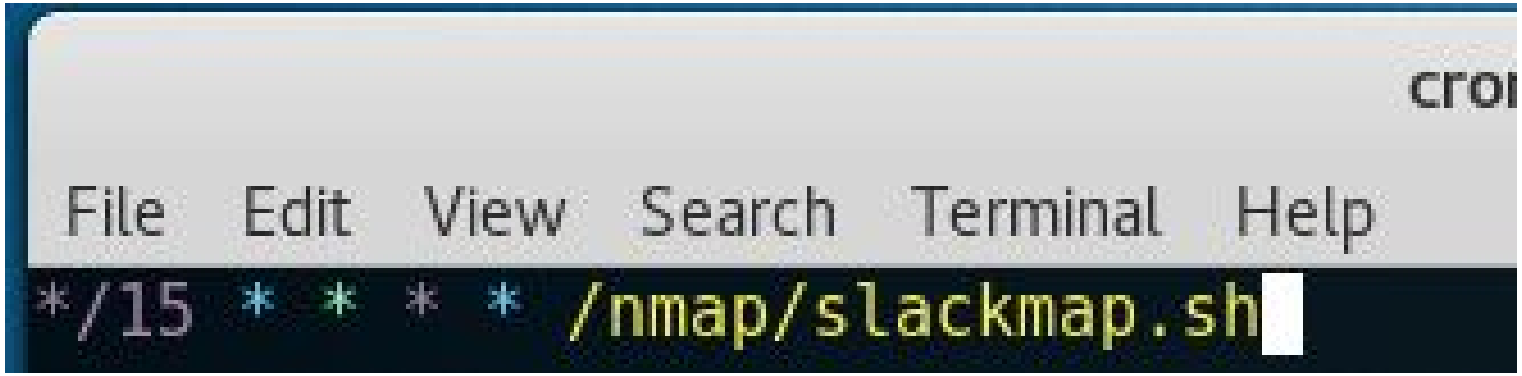
Details

DHT Nodes	
48.35.119.238	50069
93.184.63.211	52520
238.10.162.132	36427
178.118.172.75	17222
143.205.49.56	13916
80.50.91.119	38491
144.61.186.81	35923
68.154.23.169	47365
18.161.13.68	12712
41.186.67.106	12615
154.25.51.30	29205
168.59.54.146	11838
172.98.67.120	30633
50.91.29.175	49642
60.18.160...	

Automation/Scripting - Slackmap

```
#!/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
```



TeamHack
jgamblin

CHANNELS (9)
alerts
digicert
dnsrecon
general
nest
nmap
random
slash
vt

DIRECT MESSAGES (4)
slackbot
jgamblin (you)
networkalerts
networkchange
+ Invite people

#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

```
 box1269.bluehost.com, jerrygamblin.com (50.87.249.69):
 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

```
-iPad.gamblin.org (192.168.1.105, 6C:70:9F:7B:4B:C1):
+192.168.1.105:
-Host is up.
+Host is down.
-Not shown: 100 closed ports

 Macintosh.gamblin.org (192.168.1.115, A4:5E:60:DD:71:CB):
 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)

-iPhone-102.gamblin.org (192.168.1.164, A4:B8:05:C8:07:34):
+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

WannaCry :''(

- Remember WannaCry?
  - Ransomware attack released in May 2017. Affected all major Windows Operating Systems.
  - Utilized a SMB Flaw to run exploits.
  - So bad that Microsoft released patches for Windows XP and Server 2003
- How can we utilize tools to alert what machines are vulnerable to WannaCry?
- NMAP!!!

Example Usage

- `nmap -p445 --script smb-vuln-ms17-010 <target>`
- `nmap -p445 --script vuln <target>`

Script Output

```
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/
```

Requires

- **nmap**
- **smb**
- **vulns**
- **stdnse**
- **string**

Author:

Paulino Calderon <paulino()calderonpale.com>

```
administrators-MacBook-Pro:ms17_to_slack jeredbare$ nmap --script smb-vuln-ms17-010.nse 192.168.7.4

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-10 21:28 CDT
Nmap scan report for 192.168.7.4
Host is up (0.015s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown

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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 13.72 seconds
```

How can we alert for WannaCry?

- Utilize the script written by Paulino Calderon and upload the results to Slack.

```
#!/bin/bash
nmap --script smb-vuln-ms17-010.nse -p445 192.168.7.4 >> ms17-010_hosts.txt
curl -F file=@"ms17-010_hosts.txt" -F initial_comment="MS17-010 Vulerable Machines" -F channels=#general -F token=
[token here] https://slack.com/api/files.upload >> /dev/null
```

```
administrators-MacBook-Pro:ms17_to_slack jeredbare$ sudo vi ms017-010_slack.sh
Password:
administrators-MacBook-Pro:ms17_to_slack jeredbare$ sudo ./ms017-010_slack.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  3319  100  1874  100  1445   4080   3146 --:--:-- --:--:-- --:--:--  4854
```

alertbot APP 9:38 PM

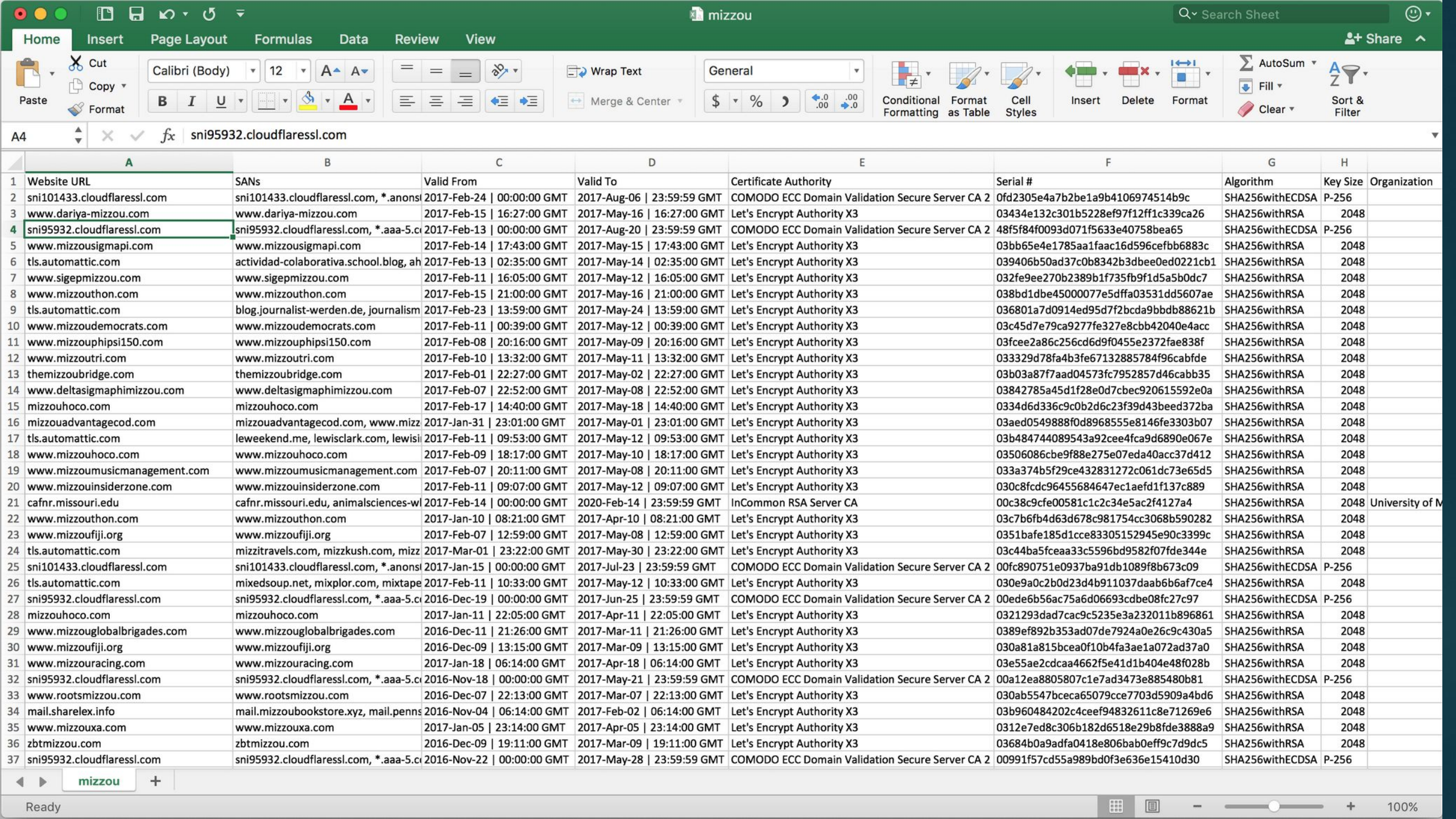
added and commented on this Plain Text snippet: **ms17-010 hosts**

```
1
2  Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-10 21:37 CDT
3  Nmap scan report for 192.168.7.4
4  Host is up (0.0033s latency).
5
6  PORT    STATE SERVICE
7  445/tcp open  microsoft-ds
8
9  Host script results:
10 | smb-vuln-ms17-010:
11 |   VULNERABLE:
12 |   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
13 |     State: VULNERABLE
14 |     IDs:  CVE:CVE-2017-0143
15 |     Risk factor: HIGH
16 |       A critical remote code execution vulnerability exists in Microsoft
   SMBv1
17 |        servers (ms17-010).
18 |
19 |     Disclosure date: 2017-03-14
20 |     References:
21 |       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-
   guidance-for-wannacrypt-attacks/
22 |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
23 |_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
24
25 Nmap done: 1 IP address (1 host up) scanned in 13.49 seconds
26
```

> MS17-010 Vulerable Machines

Certificate Logging Tools

```
#!/bin/bash
search=$1
curl -s "https://cryptoreport.websecurity.symantec.com/chainTester/webservice/ctsearch/download?keyword=${search}"
```



mizzou

Search Sheet

Home Insert Page Layout Formulas Data Review View Share

Paste Cut Copy Format Calibri (Body) 12 Wrap Text General Conditional Formatting Format as Table Cell Styles Insert Delete Format AutoSum Fill Clear Sort & Filter

A4 sni95932.cloudflaressl.com

	A	B	C	D	E	F	G	H	
1	Website URL	SANs	Valid From	Valid To	Certificate Authority	Serial #	Algorithm	Key Size	Organization
2	sni101433.cloudflaressl.com	sni101433.cloudflaressl.com, *.anonsl	2017-Feb-24 | 00:00:00 GMT	2017-Aug-06 | 23:59:59 GMT	COMODO ECC Domain Validation Secure Server CA 2	0fd2305e4a7b2be1a9b4106974514b9c	SHA256withECDSA	P-256	
3	www.dariya-mizzou.com	www.dariya-mizzou.com	2017-Feb-15 | 16:27:00 GMT	2017-May-16 | 16:27:00 GMT	Let's Encrypt Authority X3	03434e132c301b5228ef97f12ff1c339ca26	SHA256withRSA	2048	
4	sni95932.cloudflaressl.com	sni95932.cloudflaressl.com, *.aaa-5.c	2017-Feb-13 | 00:00:00 GMT	2017-Aug-20 | 23:59:59 GMT	COMODO ECC Domain Validation Secure Server CA 2	48f5f84f0093d071f5633e40758bea65	SHA256withECDSA	P-256	
5	www.mizzousigmapi.com	www.mizzousigmapi.com	2017-Feb-14 | 17:43:00 GMT	2017-May-15 | 17:43:00 GMT	Let's Encrypt Authority X3	03bb65e4e1785aa1faac16d596cefbb6883c	SHA256withRSA	2048	
6	tls.automattic.com	actividad-colaborativa.school.blog, ah	2017-Feb-13 | 02:35:00 GMT	2017-May-14 | 02:35:00 GMT	Let's Encrypt Authority X3	039406b50ad37c0b8342b3dbee0ed0221cb1	SHA256withRSA	2048	
7	www.sigepmizzou.com	www.sigepmizzou.com	2017-Feb-11 | 16:05:00 GMT	2017-May-12 | 16:05:00 GMT	Let's Encrypt Authority X3	032fe9ee270b2389b1f735fb9f1d5a5b0dc7	SHA256withRSA	2048	
8	www.mizzouthon.com	www.mizzouthon.com	2017-Feb-15 | 21:00:00 GMT	2017-May-16 | 21:00:00 GMT	Let's Encrypt Authority X3	038bd1dbe45000077e5dffa03531dd5607ae	SHA256withRSA	2048	
9	tls.automattic.com	blog.journalist-werden.de, journalism	2017-Feb-23 | 13:59:00 GMT	2017-May-24 | 13:59:00 GMT	Let's Encrypt Authority X3	036801a7d0914ed95d7f2bcda9bbdb88621b	SHA256withRSA	2048	
10	www.mizzoudemocrats.com	www.mizzoudemocrats.com	2017-Feb-11 | 00:39:00 GMT	2017-May-12 | 00:39:00 GMT	Let's Encrypt Authority X3	03c45d7e79ca9277fe327e8cbb42040e4acc	SHA256withRSA	2048	
11	www.mizzouphipsi150.com	www.mizzouphipsi150.com	2017-Feb-08 | 20:16:00 GMT	2017-May-09 | 20:16:00 GMT	Let's Encrypt Authority X3	03fcee2a86c256cd6d9f0455e2372fae838f	SHA256withRSA	2048	
12	www.mizzoutri.com	www.mizzoutri.com	2017-Feb-10 | 13:32:00 GMT	2017-May-11 | 13:32:00 GMT	Let's Encrypt Authority X3	033329d78fa4b3fe67132885784f96cabfde	SHA256withRSA	2048	
13	themizzoubridge.com	themizzoubridge.com	2017-Feb-01 | 22:27:00 GMT	2017-May-02 | 22:27:00 GMT	Let's Encrypt Authority X3	03b03a87f7aad04573fc7952857d46cabb35	SHA256withRSA	2048	
14	www.deltasigmaphimizzou.com	www.deltasigmaphimizzou.com	2017-Feb-07 | 22:52:00 GMT	2017-May-08 | 22:52:00 GMT	Let's Encrypt Authority X3	03842785a45d1f28e0d7cbec920615592e0a	SHA256withRSA	2048	
15	mizzouhoco.com	mizzouhoco.com	2017-Feb-17 | 14:40:00 GMT	2017-May-18 | 14:40:00 GMT	Let's Encrypt Authority X3	0334d6d336c9c0b2d6c23f39d43beed372ba	SHA256withRSA	2048	
16	mizzouadvantagecod.com	mizzouadvantagecod.com, www.mizz	2017-Jan-31 | 23:01:00 GMT	2017-May-01 | 23:01:00 GMT	Let's Encrypt Authority X3	03aed0549888f0d8968555e8146fe3303b07	SHA256withRSA	2048	
17	tls.automattic.com	leweekend.me, lewisclark.com, lewisi	2017-Feb-11 | 09:53:00 GMT	2017-May-12 | 09:53:00 GMT	Let's Encrypt Authority X3	03b484744089543a92cee4fca9d6890e067e	SHA256withRSA	2048	
18	www.mizzouhoco.com	www.mizzouhoco.com	2017-Feb-09 | 18:17:00 GMT	2017-May-10 | 18:17:00 GMT	Let's Encrypt Authority X3	03506086cbe9f88e275e07eda40acc37d412	SHA256withRSA	2048	
19	www.mizzoumusicmanagement.com	www.mizzoumusicmanagement.com	2017-Feb-07 | 20:11:00 GMT	2017-May-08 | 20:11:00 GMT	Let's Encrypt Authority X3	033a374b5f29ce432831272c061dc73e65d5	SHA256withRSA	2048	
20	www.mizzouinsiderzone.com	www.mizzouinsiderzone.com	2017-Feb-11 | 09:07:00 GMT	2017-May-12 | 09:07:00 GMT	Let's Encrypt Authority X3	030c8fcdc96455684647ec1aefd1f137c889	SHA256withRSA	2048	
21	cafnr.missouri.edu	cafnr.missouri.edu, animalsciences-wl	2017-Feb-14 | 00:00:00 GMT	2020-Feb-14 | 23:59:59 GMT	InCommon RSA Server CA	00c38c9cfe00581c1c2c34e5ac2f4127a4	SHA256withRSA	2048	University of M
22	www.mizzouthon.com	www.mizzouthon.com	2017-Jan-10 | 08:21:00 GMT	2017-Apr-10 | 08:21:00 GMT	Let's Encrypt Authority X3	03c7b6fb4d63d678c981754cc3068b590282	SHA256withRSA	2048	
23	www.mizzoufiji.org	www.mizzoufiji.org	2017-Feb-07 | 12:59:00 GMT	2017-May-08 | 12:59:00 GMT	Let's Encrypt Authority X3	0351bafe185d1cce83305152945e90c3399c	SHA256withRSA	2048	
24	tls.automattic.com	mizzitravels.com, mizzkush.com, mizz	2017-Mar-01 | 23:22:00 GMT	2017-May-30 | 23:22:00 GMT	Let's Encrypt Authority X3	03c44ba5fceaa33c5596bd9582f07fde344e	SHA256withRSA	2048	
25	sni101433.cloudflaressl.com	sni101433.cloudflaressl.com, *.anonsl	2017-Jan-15 | 00:00:00 GMT	2017-Jul-23 | 23:59:59 GMT	COMODO ECC Domain Validation Secure Server CA 2	00fc890751e0937ba91db1089f8b673c09	SHA256withECDSA	P-256	
26	tls.automattic.com	mixedsoup.net, mixplor.com, mixtape	2017-Feb-11 | 10:33:00 GMT	2017-May-12 | 10:33:00 GMT	Let's Encrypt Authority X3	030e9a0c2b0d23d4b911037daab6b6af7ce4	SHA256withRSA	2048	
27	sni95932.cloudflaressl.com	sni95932.cloudflaressl.com, *.aaa-5.c	2016-Dec-19 | 00:00:00 GMT	2017-Jun-25 | 23:59:59 GMT	COMODO ECC Domain Validation Secure Server CA 2	00ede6b56ac75a6d06693cdbe08fc27c97	SHA256withECDSA	P-256	
28	mizzouhoco.com	mizzouhoco.com	2017-Jan-11 | 22:05:00 GMT	2017-Apr-11 | 22:05:00 GMT	Let's Encrypt Authority X3	0321293dad7cac9c5235e3a232011b896861	SHA256withRSA	2048	
29	www.mizzouglobalbrigades.com	www.mizzouglobalbrigades.com	2016-Dec-11 | 21:26:00 GMT	2017-Mar-11 | 21:26:00 GMT	Let's Encrypt Authority X3	0389ef892b353ad07de7924a0e26c9c430a5	SHA256withRSA	2048	
30	www.mizzoufiji.org	www.mizzoufiji.org	2016-Dec-09 | 13:15:00 GMT	2017-Mar-09 | 13:15:00 GMT	Let's Encrypt Authority X3	030a81a815bcea0f10b4fa3ae1a072ad37a0	SHA256withRSA	2048	
31	www.mizzouracing.com	www.mizzouracing.com	2017-Jan-18 | 06:14:00 GMT	2017-Apr-18 | 06:14:00 GMT	Let's Encrypt Authority X3	03e55ae2cdcaa4662f5e41d1b404e48f028b	SHA256withRSA	2048	
32	sni95932.cloudflaressl.com	sni95932.cloudflaressl.com, *.aaa-5.c	2016-Nov-18 | 00:00:00 GMT	2017-May-21 | 23:59:59 GMT	COMODO ECC Domain Validation Secure Server CA 2	00a12ea8805807c1e7ad3473e885480b81	SHA256withECDSA	P-256	
33	www.rootsmizzou.com	www.rootsmizzou.com	2016-Dec-07 | 22:13:00 GMT	2017-Mar-07 | 22:13:00 GMT	Let's Encrypt Authority X3	030ab5547bceca65079cce7703d5909a4bd6	SHA256withRSA	2048	
34	mail.sharelex.info	mail.mizzoubookstore.xyz, mail.penns	2016-Nov-04 | 06:14:00 GMT	2017-Feb-02 | 06:14:00 GMT	Let's Encrypt Authority X3	03b960484202c4ceef94832611c8e71269e6	SHA256withRSA	2048	
35	www.mizzouxa.com	www.mizzouxa.com	2017-Jan-05 | 23:14:00 GMT	2017-Apr-05 | 23:14:00 GMT	Let's Encrypt Authority X3	0312e7ed8c306b182d6518e29b8fde3888a9	SHA256withRSA	2048	
36	zbtmizzou.com	zbtmizzou.com	2016-Dec-09 | 19:11:00 GMT	2017-Mar-09 | 19:11:00 GMT	Let's Encrypt Authority X3	03684b0a9adfa0418e806bab0eff9c7d9dc5	SHA256withRSA	2048	
37	sni95932.cloudflaressl.com	sni95932.cloudflaressl.com, *.aaa-5.c	2016-Nov-22 | 00:00:00 GMT	2017-May-28 | 23:59:59 GMT	COMODO ECC Domain Validation Secure Server CA 2	00991f57cd55a989bd0f3e636e15410d30	SHA256withECDSA	P-256	

mizzou

Ready 100%

Failures and Challenges

- Logging and Alerting
  - How exactly are you going to log these actions?
  - How are you going to alert for these actions?
- Actionable vs Informational
  - If a port comes open and then closes, does that mean its an issue?
- This stuff takes time
  - Will need some down time to learn and set all of this up.

Well…this is great and all; but how do I get started?

GET Permission

May I….hack..I mean Port Scan our network?

- From Your Boss/Their Boss/Their Boss and so on.
  - Get it in writing. CYA.
- Assessment Scope.
  - Develop a document of what you are testing, what you are planning to do and who exactly to contact if issues happen.
  - Not a question of if, but when something breaks
  - Get sign off from the top.
- Inform Departments of what you are doing.
  - Call and talk with your SysAdmins, HelpDesk, Developers, etc.

Options to Build Your Tools

- Old Machine
  - Have an old machine? Use it strictly for a discovery box!
    - Dual Core Processor
    - 4GB of RAM
    - Linux (Debian Preferred)
    - Gigabit network card
- Cloud Options

These options usually have a request form for Scanning/Pen testing services externally.

  - DigitalOcean
  - Amazon
  - Heroku
- Virtual Machine
  - Local or server.

Recap

- Finding information on your network does not need to be hard or costly.
- Utilize Open Source tools to your advantage.
- Learn the tools and build better ones! Become apart of the community!

http://www.hackersforcharity.org/puerto-rico-relief-efforts/

Contact

Twitter: @jeredbare
Email: jeredbare@gmail.com
Cell: 573-355-0676
https://github.com/jeredbare/whopluggedthatin

Demo