Chapter 1 Scanning Overview and Methodology

01_01 Roadmapping a Scan

No links

01_02 Scanning Techniques

To see a list of the different TTL values for various operating systems, visit: https://subinsb.com/default device-ttl-values/

Visit Chris Sanders page https://chrissanders.org/packet-captures/ which will direct you to his GitHub page:

https://github.com/chrissanders/packets. Select activeosfinger printing.pcapng, and open in Wireshark.

Scanning vs Penetration Testing

To see a list of SecTools's top 125 network security tools, visit: https://sectools.org/tag/vuln-scanners/

Ethical Hacking: Scanning Networks with Lisa Bock 2 of 5

01_04 Examining IPv6 Networks

The adoption of Ipv6 is slow but steady. Here, we can see a graph of Ipv6 use worldwide: https://www.google.

com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-adoption

01_05 Counteracting Port Scanning

No links

01_06 CHALLENGE: Compare Pen Test from a Vulnerability Scan

To see a comparison of Pen Test versus vulnerability scanning, visit: https://positiveprocessing.wordpress.

vulnerability-scanning-vs-pen-testing/

01_07 RESPONSE: Compare Pen Test from a Vulnerability Scan

To see a comparison of Pen Test versus vulnerability scanning, visit: https://positiveprocessing.wordpress.

vulnerability-scanning-vs-pen-testing/

Diving into the Network

*02_01 Reviewing the Three-Way Handshake

*02_02 Scanning the Ports

To view a hints file that holds the information on root name servers, visit: https://www.internic.net/domain/

named.root

For a who is directory information of example.com, visit: http://www.whois.com/whois/example.com

Visit the Google apps toolbox to view information on a website: https://toolbox.googleapps.com/apps/

dig/#NS/example.com

For information on a domain name, visit: https://dnsdumpster.com/

*Employing ICMP

*02_07 Grabbing the Banner

Ethical Hacking:

To do a browser check for your system, visit: https://browsercheck.qualys.com/

For a complete set of networking tools in one stop, visit: https://w3dt.net

Using Online Tools for Discovery

Using online tools at https://w3dt.net/, answer the following:

Complete an HTTP Header Retrieval with the target: http://scanme.nmap.org - What type of server is in use?

If we have a MAC address: 00:C0:4F:CC:6C:8F, what is the manufacturer?

What is the default password for Netgear?

Any other interesting tools?

Response Using Online Tools for Discovery

Same as above

Blueprint the Network

03_01 Mapping Networks using Nmap

To see a list of nmap commands, visit: https://svn.nmap.org/nmap/docs/nmap.usage.txt

Visit https://macaddress.webwat.ch/ if you need to know the vendor of a NIC card.

Using this site, you can run a quick port scan. NOTE: Only scan a network you are authorized to scan: https://hackertarget.com/nmap-online-port-scanner/

SSDP for Discovery

To see a capture containing SSDP packets, go to: https://www.cloudshark.org/captures/73d574c3ed0d

Identifying Other Network Mapping Tools

Op manager gives a nice graphical user interface so you can easily monitor your network. https://www.

manageengine.com/network-monitoring/

SolarWinds has a network topology mapper. Although this is a paid product, you can get a free trial: https://

www.solarwinds.com/network-topology-mapper

The Dude is a network monitoring tool that you can find here: http://www.mikrotik.com/thedude

Spiceworks also has a free network monitoring tool: http://www.spiceworks.com/free-network-monitoring management-software/. Once there, you'll need to create an account.

NetworkMiner is an open-source Network Forensic Analysis Tool (NFAT) for Windows, found here: http://www.

netresec.com/?page=NetworkMiner