Cybersecurity

Operations and Incident Response

4.1.1 Network Reconnaissance and Discovery Tools

What are the 18 command line tools used to gather network configuration information?

Overview
Given a scenario, the student will use the appropriate tool to assess organizational security.

Grade Level(s)
10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 4.1

- Given a scenario, use the appropriate tool to assess organizational security.
    - Network reconnaissance and discovery
        - tracert/traceroute
        - nslookup/dig
        - ipconfig/ifconfig
        - nmap
        - ping/pathping
        - hping
        - netstat
        - netcat
        - IP scanners
        - arp
        - route
        - curl
        - theHarvester
        - sn1per
        - scanless
        - dnsenum
        - Nessus
        - Cuckoo

Network Reconnaissance and Discovery Tools

Command Line Tools

Command line security tools perform many security functions. Most graphical user interface, or GUI,-based software tools simply automate much of the behind the scenes commands that actually harvest information and present it to the user. At first, the command line may seem confusing or hard to remember, but this is only because most users have little experience with the command line. With practice, the command line becomes as easy as a GUI (and sometimes faster). When connecting to a remote system, there may not always be a graphical user interface to interact with. In fact, most servers do not waste system resources providing a GUI. The command line is also powerful because of the ability to string commands together and make tools interact with one another in ways specific to the task at hand. With a GUI,

Teacher Notes:

a developer must envision what all possible needs are in order to create a menu to serve that purpose. With the command line, the user is in complete control to "do it yourself."

This lesson includes a sampling of the most basic command line tools used in cybersecurity. This is not an exhaustive list; it is only a starting point. This lesson mentions multiple command line ***IP scanners***, which is a tool that will scan a network for different IP addresses.

Network configuration: ipconfig, ifconfig, ip

The command ***ipconfig*** is a tool for Microsoft Windows systems that displays the network configuration information of the Windows machine where the command is run. Information like the IP address, MAC address, Subnet Mask, and DNS server(s) are listed. By passing various parameters, ipconfig can provide different functions. `ipconfig /all` provides the full detail about the network configuration. `ipconfig /release` instructs the interface to forget the current DHCP-assigned IP address. `ipconfig /renew` instructs the interface to renew its lease on the currently assigned IP address from the DHCP server. If no address is assigned, it will seek to get a new IP address assignment. `ipconfig /flushdns` tells the host to erase the local DNS cache and seek new DNS records from the DNS server for subsequent queries.

The command ***ifconfig*** is an aging Linux command line tool that provides interface configuration information for the Linux machine where the command was run. Information similar to ipconfig can be gleaned from the `ifconfig` command. Most often, `ifconfig` is used to locate the current machine's IP address, MAC address, subnet, and current state of the adapter. Unlike `ipconfig` on Windows, Linux's `ifconfig` does ***not*** manage the DHCP lease. DHCP in Linux is managed by a tool called `dhclient`. DNS settings and the local DNS cache are also not managed by `ifconfig`. There are a variety of tools to manage the local DNS cache, but the main DNS server is usually reflected in `/etc/resolv.conf`. Most current Linux systems require the user to have ***root*** access in order to interact with `ifconfig`. If this is the case with the system you are working with, be sure to use ***sudo*** when appropriate.

`ifconfig` has been around many years. Unfortunately, it has not kept up with current machine architecture and is in the process of being phased out and retired (in Linux parlance, it has become "deprecated"). The

Teacher Notes:

replacement for `ifconfig` is the short but appropriately named *ip* command. The `ip` command is actually a suite of replacement tools for many legacy networking command in Linux. `ip` can set and change the IP address, show current configuration, and enable or disable an interface all much like the old `ifconfig`. In addition, `ip` can also replace the `arp` and `netstat` commands covered later in this lesson.

Connectivity tools: ping and tracert

The *ping* command tests connectivity using ICMP packets. This command is used to determine if there is a route from the machine where the command is run to the target host. The target can be specified by IP address or hostname. The round trip time for a message to be returned is measured in milliseconds. Many gamers are familiar with the operation of the ping command because most online multiplayer games provide a measure of latency between the player and the game server. `ping` operates very similarly between Windows and Linux devices with one key difference. On Linux, ping will continue to run until the user halts the command with CTRL+C or some other command interruption. On Windows, ping will only send and receive 4 ping requests. It is possible to limit the number of pings sent on Linux, and it is possible to tell Windows to ping ceaselessly. Both operations are unique to that operating system's `ping` command.

Traceroute is used to determine the route a packet takes over a network to reach a target host. This tool provides information such as all of the intermediate IP addresses, called hops, of the machines that process a packet as it travels to the destination. On Linux and Mac systems, the command is `traceroute`. On Windows, the command is `tracert`. As with `ping`, the results are very similar. Each operating system provides options to enable or disable resolving the hostname of the IP addresses encountered along the path.

A mixture of `tracert` and `ping` is the `pathping` command for Windows operating systems. This command not only provides the path packets take between hosts (like `tracert`), but it also tells the time each hop takes (like `ping`). This command takes much more time to complete because it will discover the amount of hops and then test each hop for 25 seconds. Thus, if a route consists of 11 hops, it will take at least 4.5 minutes.

Teacher Notes:

TCP/IP Packet Analyzer

The command **`hping`** is used to test the security of a network. Pentesters can use this command to audit networks by testing firewalls, open/closed ports, analyzing traffic, etc.… This command allows the pentester to create their own TCP/IP packets in order to test certain things. The **`hping`** command is available on both Windows and Linux OSs.

DNS tools: nslookup and dig

Both ***nslookup*** and ***dig*** are commands used to query DNS information available from a name server.

The ***nslookup*** command displays the IP address(es) associated with a domain name and vice versa. It provides the most basic of DNS information about a host and is quite limited in its capability for looking up a domain name on a name server.

The ***dig*** command provides more extensive and detailed DNS record information about a domain. From the results, a user can determine several details about a domain such as the mail exchange server address, the authoritative name server responsible for this particular address, and any other records associated with the domain. There are many DNS record types that may be returned in the results from using dig. The most common are A, AAAA, MX, NS, SOA, and TXT. The A record is the Address record, which provides an IP address to the domain name. The AAAA record is an extension of the A record and provides the IPv6 address for the domain name if IPv6 is in use. The MX record provides the name and/or IP address of the Mail Exchange server, which is the server that handles the email for the domain. The NS record provides the authoritative DNS for the record. Many domain name servers may provide information about a domain, but the NS listed for a record will always be the most accurate and contain updates made on the domain by the owner. The SOA is the Start of Authority record and provides administrative contact information about who owns the domain name. Lastly, the TXT record is a simple text entry record. This is sometimes used to provide proof of ownership of the domain to a third party provider. Tools like Google Docs will require the domain administrator to create a TXT record with a special key to provide proof they own and have control of a domain before Google will provide services for that domain.

Teacher Notes:

arp and route

ARP stands for Address Resolution Protocol. ARP is used for determining which IP address belongs with which MAC address. The `arp` command allows the user to see the arp table for the host. The arp table stores the MAC addresses and associated IP addresses, which frees the host from having to search for the MAC address for each IP every time an operation needs this information. Use of the `arp` command can help identify which IP address is assigned to a host if the MAC is known or which MAC address belongs to a device if the IP address is known. Inspecting the arp table also allows for the discovery of hosts on a network and can also uncover if there is more than one device with a specified MAC address, which may be indicative of MAC spoofing.

One tool that shows a system's routing table and allows a user to modify is `route`. `Route` can be used on both Windows and Linux OSs but does vary in the syntax between the two. A routing table is data stored on a network (typically on the router) that lists routes to different hosts on that network. Using `route`, a user can view certain routes and alter them for various reasons. A static route is what a route is called when a user has manually changed a certain route.

netstat

netstat is the network statistics tool. It can showcase the current routing table used by the local host, the current network activities, and the number of packets sent and received by a particular interface. `netstat` can display all the ports on the machine it is run on and their status. This is particularly useful for determining if a service like a webserver, NTP server, SSH, or even a backdoor is operational and which port it is active on. `netstat` is operationally similar on both Linux and Windows machines, but there are subtle differences. As with `ifconfig` being replaced by the more modern `ip` command, `netstat` is deprecated and has been replaced by the tool `ss` on most modern Linux distributions.

nmap and Nessus

The ***nmap*** tool is a very common and popular network mapper and port scanner. It searches a network for hosts by scanning an IP range on a network and identifying if any of the IP addresses are responsive. Once a

Teacher Notes:

host responds, `nmap` can also scan the available ports to determine which ports are open, filtered, or closed. Open or filtered ports on registered ports can usually convey which services are available on that host. `nmap` can also provide operating system fingerprinting of the hosts on the network to determine the operating system on the target host. While not expressly illegal in most jurisdictions, port scanning is usually a very suspicious activity since it is largely done by outsiders seeking to find and exploit some vulnerability on a network. It is similar to going to a bank after hours and jiggling door handles to see if the doors are locked or unlocked. That act itself is not illegal, but a police officer arriving on the scene might have a lot of questions to ask!

While nmap will identify open ports, protocols, versions, etc…, a tool called *Nessus* can take these open ports and scan them for vulnerabilities. Companies use Nessus because it not only shows them where vulnerabilities exist, but it provides the company with how to fix/patch the vulnerabilities. Nessus is an open source software that is used alongside other tools, like Nexpose or OpenVAS, to run a full audit of systems to detect vulnerabilities and figure out how to patch them.

netcat and curl

The *netcat* command can read and write directly to network interfaces. This command is a network version of the `cat` command found on the Linux command line. It is often abbreviated as simply `nc`. Netcat can allow the user to test communications with a service to ensure basic operations, step through operations manually, or read response data that may otherwise get displayed differently in an application like a web browser. Netcat can also create a backdoor in which to exfiltrate data from a host. Using netcat on a remote machine, the remote machine can listen for data being piped out through the netcat tunnel. Netcat can also write data directly to a network host in order to test how the host responds to various requests. This allows for testing security provisions in order to anticipate a response from an Intrusion Prevention System (discussed in 3.2.1). Perhaps most useful for security auditors is the ability for netcat to perform "banner grabbing," which was covered in the previous lesson.

Curl is a common tool used to transfer data from one server to another. This can be done using a variety of protocols, like HTTP, IMAP, SMTP, etc.… When a simple `curl` command is run, it will fetch the headers, like a GET header used in simple HTTP protocol.

Teacher Notes:

Data Gathering Tools

One way to gather intelligence without giving away your own IP address is through a tool called `scanless`. `Scanless` uses multiple port scanners to run the scans for you, thus you never leave a trace back to your IP address. This tool makes it look like the scan came from different websites used within the total scan. `Scanless` checks for open ports on both servers and hosts which could be used to enter a system maliciously.

`theHarvester` is another open source tool that gathers information about a company or domain that is already out there. This is the same as running a Google search or social media search into a company, but `theHarvester` does all the work from the command line. A malicious actor could use this tool to gather information about the employees of a company, like their email addresses, to run/attempt certain attacks against them. A company could use `theHarvester` to see what information is public facing from their company; this can help them see if they have a potential weakness. `theHarvester` can use different services such as Twitter, Google, Yahoo, Bing, LinkedIn, etc… to gather the information about a company and its employees.

`Sn1per` is a tool that combines `whois`, `ping`, multiple port scanning tools, nmap, etc… to gather intelligence against an organization. Unlike theHarvester, `sn1per` uses the actual system's tools to gather the intelligence, thus the intelligence gathering can be traced back more easily. This tool gathers a lot of information and automates a lot of pentesting tools.

Another data gathering tool is `dnsenum`. This is a tool that not only finds DNS records, but also can try to get a hostname given an IP address or even attempt to get multiple IP addresses by brute forcing queries. This also works for mail servers, name servers, etc.… The goal of `dnsenum` is to gather all the servers and DNS entries for an organization, not just one server that a system is connected with at a certain time.

Cuckoo

Cuckoo is a sandboxed environment that a company is able to put a file into and find out how it will act in the isolated environment. Companies can use this tool to test out programs before putting them on their networks and figuring out if they are malware or not. If it is malware, they should know in

Teacher Notes:

a matter of minutes what type of malware it is as well as how dangerous it is. Companies might also use Cuckoo to analyze network traffic or even tracking calls on certain components.