Network Audit

Writing a formatted host inventory with service details

Type of Systems: All hosts on the network except networking equipment.
Necessary Skills: Basic Linux and Windows command-line

Complete Goal: To inventory all computers on the competition network. This process will create a formatted document that lists each host's operating system, hostname, IP address, accounts, services, and open ports. Along with these basics, there is also the need to provide sufficient details and clear language for non-technical people to understand (such as the CEO).

Steps:

1. ONE PERSON: Before collecting information, a document must be created for the host inventory. In the doc, create tables using the following format for each host. Each team member will contribute their system information to the doc.

Relevant information in the table:

- Host Name
- Services
- Open Ports
- OS
- IP

Information that will go in the sheet:

- All above information
- MAC Address
- User Accounts
- Changed Password

Host	IP	Services	Open Ports	OS
Regulus	10.0.201.30	MySQL, SSH,	22, 3306, 9090	Centos Stream

2. ONE PERSON: run a quick nmap scan to discover hosts on the network.
    a. nmap command: `nmap -sn xxx.xxx.xxx.0/24`
    b. If unknown hosts are found, try to login to those boxes.
    c. If login is impossible, do two nmap scans on those hosts:
    `nmap -sV` and `nmap -O`
    Those nmap scans should provide enough information to document the rogue host in the inventory.

3. ALL: obtain hostname and local network IPv4 address of the primary network adapter.

4. ALL: obtain operating system:
    Linux: `lsb_release -a`
    `Hostnamectl`
    `cat /etc/os-release`
    Windows: `systeminfo`

5. ALL: obtain users:
    Linux:
```
awk -F'[/:]' '{if (($3 == 0) || $3 >= 1000 &&
$3 != 65534) print $1}' /etc/passwd
```
    This command will only list users that a person can login as, not all users in

/etc/passwd.
Windows: `net user`

6. ALL: obtain service information:
   Linux: `systemctl list-units --type=service --state=running`
   Lists all running services.
   Windows: CMD: `services.msc` → Sort by status to see “started” or “running” services first.

7. ALL: obtain port connection information:
   Linux: `sudo ss -lnutp`
   (list listening ports with associated process names)
   `sudo ss -tulp`
   This command provides connections with service names.
   The output of these two commands can be compared to associate services with port numbers.
   Windows: `CMD: netstat -o`

8. All: Check SSH Keys:
   Linux: `cat ~/.ssh/authorized_keys`
   The authorized_keys file in the .ssh folder of any user will show the public key that can be used to remotely connect to the user@host.

9. ONE PERSON: The last step is to do an external nmap scan to verify the results of the internal commands. If possible, this should be done on a workstation that is outside of the services network.
   Linux:
   a. Download nmap: `sudo apt-get install nmap`
   b. Run an nmap scan: `nmap -sV xxx.xxx.xxx.0/24`
      The nmap scan will provide all open ports, service details, and version numbers.
   c. Run an nmap scan: `nmap -O xxx.xxx.xxx.0/24`
      This nmap scan will perform OS detection.

   Windows (Zenmap):
   a. Visit bit.ly/1uiBjNp
   b. Under the section “Microsoft Windows binaries,” download “nmap-7.60-setup.exe”
   c. Install the executable. All the default installation settings are fine.

   d. Open Zenmap. Enter `nmap -sV xxx.xxx.xxx.0/24` in the "Command" field and run the scan.
      The nmap scan will provide all open ports, service details, and version numbers.
      After the first scan, run another scan with `nmap -O xxx.xxx.xxx.0/24`
      This nmap scan will perform OS detection.

10. ONE PERSON: Copy the network topology from the team packet onto the end of the host inventory to provide a visual perspective of the network.
    a. If there is no provided network topology, use the following images, and create your own.

Relevant Info:

- Step 2: The Windows command will work no matter whether you are connected to the domain or not. Just remember that if you are connected to the domain, the listed users are **not** local users, they are domain users.
- Step 4: `ss` command output syntax:
    - **:portName/Num* → This process listening is listening on all IPs your computer has.
    - **:** → IPv4: Any IPv4 address can connect, and their connections can originate from any port.
    - *:::** → IPv6: any IPv6 address can connect, and their connection can originate from any port.

Digital sources of info

- Nmap scans
- Pandora
- DHCP leases (from DHCP host)
- systemctl
- Wazuh inventory info
- Commands on hosts
    - ss or netstat -lnutp (on linux)
    - hostnamectl (linux)

View Documentation Checklist and create documents.

- Incident response template
- Change management guide
- Create running services data dump document
    - May be useful to compare if red team adds malicious services

Down the line

- systemctl list-units --type=service --state=running

Appendix:

Linux list users: bit.ly/2CWBOL9 | Netstat meaning of *, *:* → bit.ly/2mi9SHy | Netstat meaning of :::* → bit.ly/2mjQAS0 | systemctl man page: http://bit.ly/2FCnm96 | Linux obtain OS details: http://bit.ly/2DeHuzB| nmap host discovery scans: http://bit.ly/2D2YCos