Section 4: Tools of the Trade

41. OS Utilites, Part 1

ALL THESE ARE ON THE EXAM

1. Ping
    1. Scenarios:
    1. Is DNS working? -Check the FQDM with ping (e.g. ping www.totalsem.com)
    2. Can I connect to Someone? (e.g. ping www.google.com)
    1. -4 ---> IPv4 (e.g. ping -4 www.google.com)
    2. -6 ---> IPv6
    3. Do I have an intermittent issue? Ping -t www.google.com
    1. -t (in windows means 'just keep running')
    2. Linux defaults to 'just keep running'
2. netstat (What Sessions a systme is running)
    1. Who am I talking to? netstat -n
    1. -n ---> Numbers only
    2. Who is trying to talk to me? netstat -a
    1. -a ---> Show me all open ports including the ones I am not connected to
3. traceroute/tracert
    1. ex. tracert www.google.com
    2. If you can't traceroute someone if it happens on the first or second line then it is an inhouse issue. If its stuff later its the ISP or someone else.
4. ARP (Address Resolution protocol)
    1. Run are because you're afraid someone is doing bad things to your switches (ARP poison)
    2. arp -a is the arp cache

Quick Review:

- Ping is a DNS tool, it resolves web addresses to an IP address
- netstat can detect what hosts are connected to you
- netstat -a can detect all ports that are opento see what ports are listening
- tracert can help see what routers are being hit, both internal and external

---

42. OS Utilites, Part 2

ALL THESE ARE ON THE EXAM

1. ipconfig(Windows), ifconfig(Linux)
    1. Shows IPv6 address, Link local IPv6, IPv4 address, Subnet mask, Default gateway
    2. ipconfig /all - A Lot more information
    3. ip addr (linux)

2. nslookup(windows), dig(Linux)
    1. DNS information
    2. What is my DNS server?
    3. Is this particular system a DNS server?
    4. Change DNS server (nslookup ---> server '8.8.8.8')

    dig:
    1. dig www.totalsem.com
    2. Change the server (dig @8.8.8.8 www.totalsem.com)
    3. Find the mail server (dig MX www.totalsem.com) --> Shows they use outlook
3. netcat (Can open and listen on ports and it can open and act as a client on any port you want)
    1. sudo netcat -l 232 (opens port 232 as a listening port)
    2. You can open a port as a client (you can take a text file)
    3. **A tool for an aggressive action**
    4. Used for pentesting

Quick Review:
- ipconfig provides the IP address and ethernet details, and the -all option finds the MAC address
- nslookup provides information on the DNS server
- Dig is a Linux utility that functions like nslookup, but dig allows for further functionality
- netcat can open and listen on ports, and be an aggressive tool for reconnaissance.

---

43. Network Scanners

1. nmap
    1. zenmap (gui for nmap)
2. Advanced Port Scanner (Free tool that works great and works like nmap)

    Three big areas where you will use network scanners
    1. You're looking for open ports
    2. Network Inventory (wireshark SB Network Inventory)
    3. look for Rogue Systems

Quick Review:
- Nmap is useful for hardware inventory and reconnaissance of your system
- Network Scans can be done to detect open ports, protocols, hardware and rogue systems
- Scans can be a resoure intensive, so plan accordingly to maintain system availability

---

44. Protocol Analyzers

Two pieces to any protocol analzyer:
1. Sniffer: usually has the name 'pcap' - grabs all the data that is coming out of a particular interface.
2. Anazlyer: Reads PCAP data

1. Wireshark
    1. Completely free
    2. On the SEC+

3. Filters information
4. Need to play with wireshark to really figure it out.

*The one downside to wireshark: Sometimes it missing incoming and outgoing packets. So instead of using the built in wireshark sniffer people use 3rd party sniffers.
- TCP dump is a common sniffer that is used instead of using the built in wirehark sniffer.

Quick Review:
- Protocol analyzers have two functions; sniffing and analyzing the data
- Wireshark allows us to filter the data by services and protocols
- Using a network analyzer we can look closely at ann activity taking place with that session

---

**45.SNMP **
Simple Network Management Protocol (SNMP) - A tool that allows us to administer and manage network devices from a single devices

TERMs:

Managed Device:

Agent - Software built in that gives the device (a printer) to used SNMP

Individual devices listen on **UDP 161** if they are unencrypted
If encrypted they listen using TLS on **UDP port 10161**

SNMP Manager:

Running some kind of interface called a NMS (Network management station)
Unencrypted, listen on Port UDP 161
Encrypted, Listening on TLS Port UDP 10162

How to communicate between NMS and Managed Device:

SNMP is not just for printers. It is for many things so when setting up SNMP network you (which is build into every managed device) a:

MIB (Management Informaton Base) - Database that we query to be able to talk to that device. Different devices have different MIBs.

When setting up our NMS we download command lists from the internet that allows us to query devices on our network

Communications that are on the test:

*Get - NMS sends a get to the Managed device and the managed device sends back information
*Trap - Set up on managed devices and then the trap is sent to the NMS if there is an issue
*Walk/SNMPWalk - Batch process of Gets (Asking a lot of stuff from a managed device)
**Study more SNMP commands

Versions of SNMP (3):
-Differences:
- - SNMP V1 does not support encryption

- - SNMP V2 added basic encryption
- - SNMP V3 add Robust TLS encryption
* Its common to have different versions of SNMP in an enterprise and its okay because the NMS can talk to them all

*Community - An organization of managed devices
*RO (Read Only) - A setting that you can set up that you can only read on the managed device

Configuring an NMS Using Cacti - Cacti is an open-source NMS for graphing SNMP data

NMS to check out: Nagios, Zabbix, Spiceworks

Review:

*SNMP uses UDP port 161 or port 10161 when using TLS
*SNMP-managed devices run an agent that talks with a Network Managemnt Station(NMS)
*Rembember the differences between the SNMP versions

46.Logs

1. Non-Network logs
   Non-Network Events: happen on a host even though its not connected to a network

```
Types of None Network Events:
        1. Operating System Events
                1. Host starting
                2. Host shutdown
                3. Reboot
                4. Services starting, stopping, and failing
                5. OS updates

        2. Application Events
                1. Application installation
                2. Application starts, stops, or crashes

        3. Security Events
                1. Logons
                2. Logon successes and failures

Non-Network Events Will have:
        1. Date
        2. Time
        3. Process/Source
        4. Account
```

```
5. Event Number
6. Event Description
```

2. Network logs
   Network Events: deal with the communication between the host and something on the network.

```
Types of Network Events:
        1. OS level or system level
                1. Remote longons (fail or not)

        2. Application level
                1. Shared applications/Resources
                        1. Activity on web server
                        2. Firewall

Network Events Will have:
        1. Date
        2. Time
        3. Source Address (MAC, IP, or both)
        4. Destination (MAC, IP, or both)
        6. Event Description
```

   *Decentralized Logging: By Default all computers/host will have all their log files and you have to go to computers individually
   *Centralized Logging:
   1. Use a Central Repository
   1. Drag on system
   2. Use SNMP systems
   1. Pulls information needed and generates graphs and charts
   MaaS (Monitoring as a Service)
   1. often times people will pay 3rd parties to monitor their logs

Exam has tons of questions that will need you to read log files.
*REWATCH THE EXAMPLES IN THIS SECTION #46

QUICK REVEIW:

- There are many types of logs (event, security, audit, etc)
- There are two types of events (network and non-network events)
- Log data should look like: event, time, proces/source, account, event Number, event description

---

QUIZ

Question 1:

Which of the following items are used to resolve the MAC address to an IP Address?

- ping
- netstat
- tracert
- arp

Question 2:

Which of the following utilities will open a port and put in listening mode?

- ping
- netcat
- dig
- ipconfig

Question 3:

When scanning a network, which of the following is a consideration?

- Network scans should only be run at a set time and schedule
- Network scans can't detect what protocols are running
- When doing a network scan, the Web server needs to be shut off
- Network scans can be resource intensive

Question 4:

When a NIC in the network continuously transmits large quantities of arbitrary garbage and communication this is called:

- ○ RFI interruption
- ◉ Broadcast storm
- ○ Wireshark
- ○ Loopback

Question 5:

What do you call a device (such as a printer) that is set up to run on an SNMP network?

- ○ Master
- ○ Client
- ○ Network management station
- ◉ Managed device

Question 6:

True or false: Activity on the Web server is a network event.

- ◉ True
- ○ False