



Day 1

“Security is all about controlling and minimizing the damage”

what is your critical data, where it located and who has access to it.

Everything we do in security is all about managing, mitigating, understanding and reducing the risk to your critical information.

Three Questions before putting any kind of security investment:

what is the risk, is it the highest prosperity risk, is it this solution the most cost effective way of reducing it.

Network Security Essentials

Defensible Network Architecture

Network Architecture:

- Conceptual Design

Conceptual Design

- High-level design
- Includes the core components of a network architecture
- Helps to understand a picture of the overall purpose of the network and why the solution was designed
- Required for integration or general functionality, data flow, and high level system behavior.
- Utilizes “black box” diagramming

Have segmented network instead of flat network.

- Logical Design

Logical Design

- Represents each logical function in the system
- More detailed
- Includes all the major components in the network plus their relationships
- Detailed data flows and connections are also mapped out
- Created primarily for developers and security architects
- Includes business services, application names, and other relevant information

- [Physical Design](#)

Physical Design

- Has all the major components and entities identified within specific physical servers and locations
- Usually the last design created before final implementation
- Contains all known details such as operating systems, version numbers, and even relevant patches
- Includes any physical constraints or limitations

- [Understand Communication Flow](#)

Understand Communication Flow

- Begins with the logical architecture
- Shows how data can flow in and out of the network
- Maps every communication flow, whether for data exchange or control messages
- Used to understand exposure and visibility of key components
- Forms the foundation for threat mapping

Assets Inventory, what are your critical assets, Configuration management, How are they Configured, Data Discovery, Where in your critical data in Environment.

Descope the problem

-  Know where your Valuable Data Is

Know Where Your Valuable Data Is

- Also begins with the logical architecture
- To secure a network, you need to know where every piece of your valuable data resides.
- Focuses on critical intellectual property:
 - What is your critical information
 - Where it is located
 - Who has access to it
 - Who should have access to it

 Attack Against Network Devices:

Its a continuous process

Threat Enumeration

Threats drive the risk calculation and important for understanding the adversary:

- List All Possible Threat Agents
- List the Attack Methods
- List the System-level Objectives

Threat Enumeration is the process of tracking and understanding critical threats to your system or network

Threat Agents

- An individual, organization, or group that is capable and motivated to carry out an attack of one sort or another
 - Differing attacker groups target and attack different types of systems in different ways for different reasons
-
- Key questions:
 1. How active is each threat agent?
 2. How might a successful attack serve a particular threat agent's goals?

A router is a device that connects two or more networks together.

A switch connects computers together.

Attacks Against Routers

The types of Router Attacks are:

- Denial of Service
- Distributed Denial of Service
- Packet Sniffing
- Packet Misrouting
- Cross-Site Scripting (XSS)

- Cross-Site Request Forgery (CRSF)
- SYN Flood
- TCP Reset Attack
- Routing Table Poisoning
- Malicious Insider / Disgruntled Employee

Attacks Against Switches

- CDP Manipulation
- MAC Flooding
- DHCP spoofing
- STP Attacks
- VLAN hopping attack
- Telnet Attack

As more and more security is integrated into a switch, they are becoming a prime target for attack

Think of the impact to your security if your switches are compromised by an adversary

Network Topologies:

Physical and Logical Topologies

Physical topologies:

- How the network is actually connected
- How the data actually flows
- Wired or wireless
- Verification of physical topology is critical to ensure security
- Star topology most common

Logical topologies:

- How you communicate across wires
- Meaning of the information
- Language
- Ethernet most common (CSMA/CD)

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free. The collision detection technology detects collisions by sensing transmissions from other stations. On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

Ethernet

Ethernet is shared media:

- CSMA/CD (carrier sense multiple access with collision detection)

Most common logical topology or layer 2 protocol

Steps taken to communicate:

- Listen before transmitting
- Make sure only one station transmits at a time
- Monitor transmissions to check for collisions

On an Ethernet network, only a single node should transmit a frame at a time. If multiple systems transmit simultaneously, a collision occurs.

Network Design:

Approaches to Network Design

Segmentation

- Network Segment
- Implement Controls at Multiple Layers
- Least Privilege Rule
- Segment Based on Security Requirements
- Whitelisting

Protected Enclave

Software Defined Networking (SDN)

- Micro-segmentation

The goal of security is focused on controlling the damage caused by an adversary

Question: If one node on your network was compromised, how much damage could the adversary cause?

Network Architecture Design

Prioritized Protection of Key Resources

Data Flow Analysis

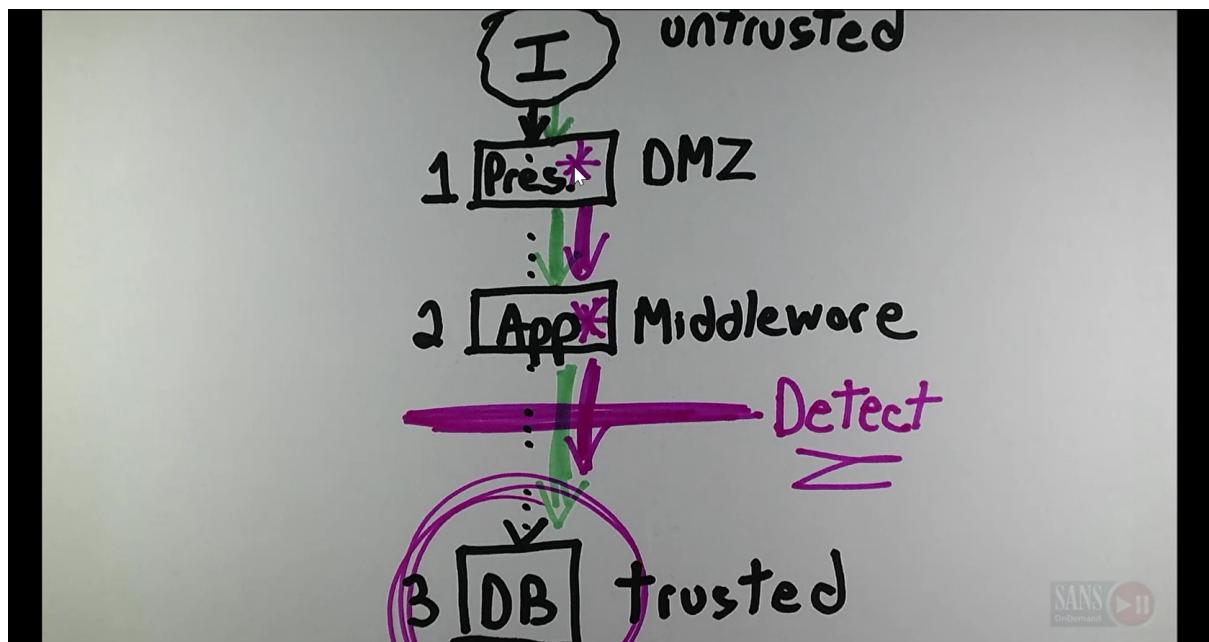
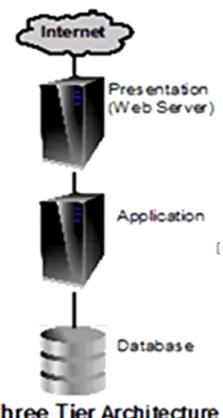
- Aids with Incident Response
- Provides Situational Awareness
- Reduces Cost of Network Monitoring
- Enables Attack Detection

Most enterprise networks are relatively flat and offer little resistance once the perimeter is breached and endpoint systems are the most likely target for malware

Prevention is ideal, Detection is must.

Network Design Objectives

- Provide appropriate access from the internal network to the Internet
- Protect the internal network from external attacks
- Provide defense-in-depth through a tiered architecture
- Control the flow of information between systems



Network Sections (1 of 2)

- **Public:** Internet
- **Semi-public (DMZ):** Web, Mail, and DNS servers
- **Middleware:** Separate DMZ from the private network
- **Private:** Internal systems

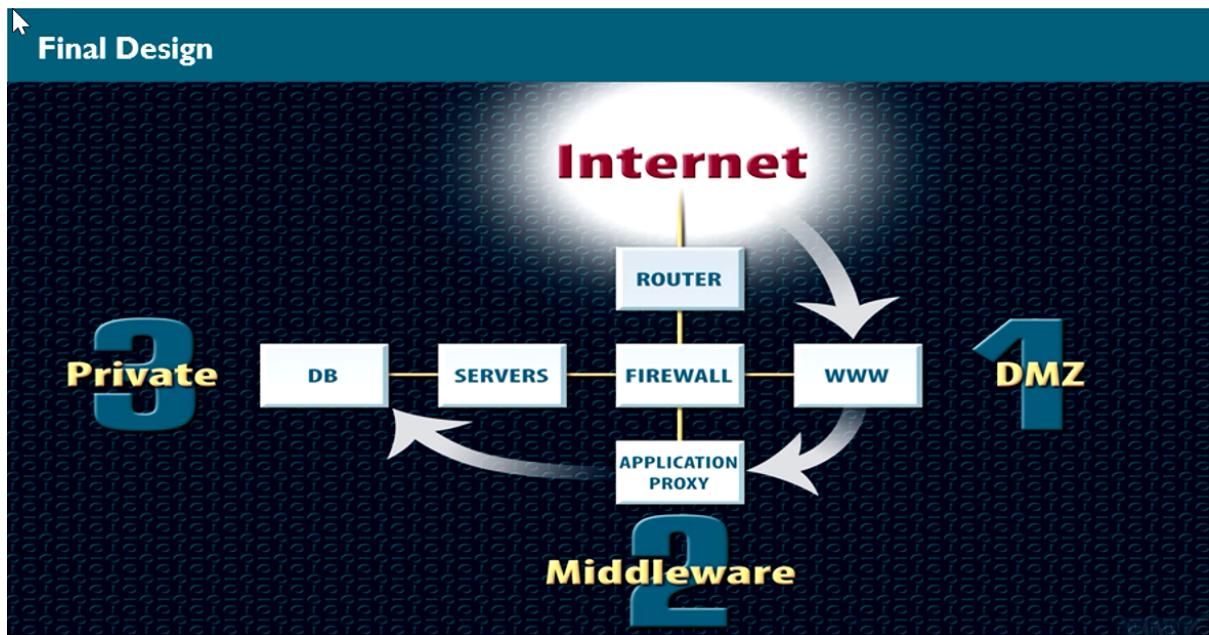
Locate firewalls:

- Between the Internet and the other networks
- Between the semi-public and private network
- Between sections of varying trust levels

Network Sections (2 of 2)

Three goals of network design:

1. Any system visible from the Internet must reside on the DMZ and cannot contain sensitive information
2. Any system with sensitive information must reside on the private network and not be visible from the Internet
3. The only way a DMZ system can communicate with a private network system is through a proxy on the middleware tier



Summary

- Understanding network technologies, physical and logical topologies, and network design is vital to create and maintain a secure network
- To secure a network, we must understand how it works
- Security must be embedded into the network and not be an afterthought
- Only by understanding how components on a network work and through a proper network architecture design can an organization achieve a secure network

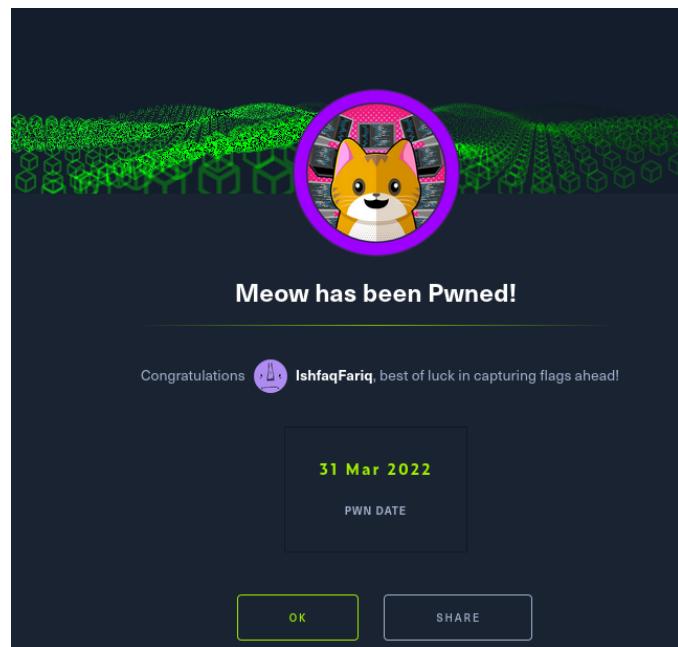
[NSE 2 Network Security Associate](#)

Finished the Network Security Associate Course.

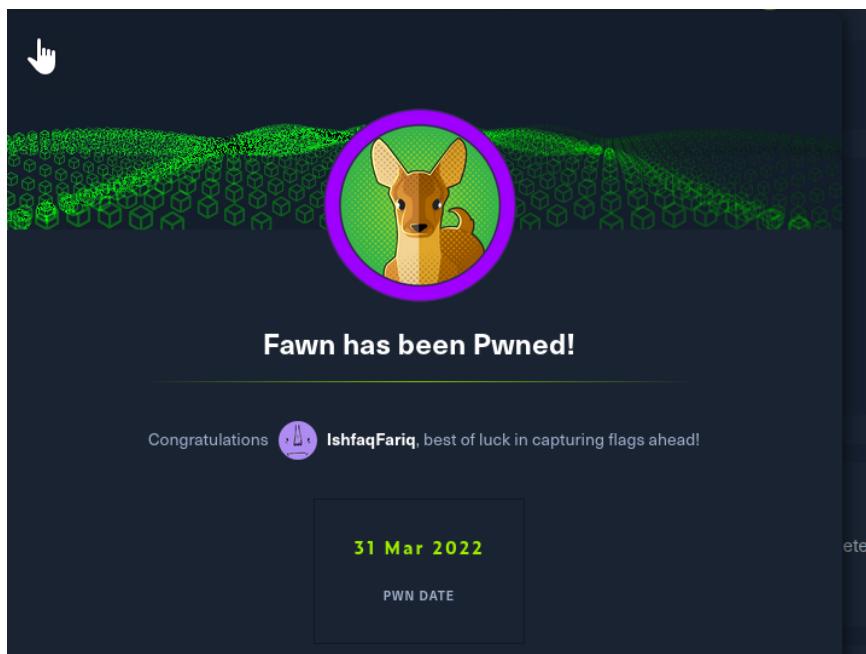
Solved Starting point labs on HTB

In Meow lab I learned bit about Telnet, Nmap, Basic linux Commands, Default credentials, TCP.

FTP is built on a client–server model architecture using separate control and data connections between the client and the server.



In Fawn lab I learned bit about FTP, How to login as anonymous, NMAP, and bit about Searchsploit .



Nmap Switches:

- p- to search all ports without this it only scans top 1k ports
- SV to see the versions of all the services running
- SC to use default script
- O for OS detection
- A for Aggressive scan
- oX for XML output

```

-OG for graphical output
-OA for all format
-SS for stealth scan
-T4 for speed
T:22,23,U:11 for checking these specific TCP ports and UDP ports

```

Searchsploit "Service version here"

searchsploit -m "path" to copy the script at your pwd

searchsploit -x "path" to read the script in terminal

Common Ports

Port Number	Protocol	Usage
20	TCP	File Transfer Protocol (FTP) Data Transfer
21	TCP	FTP Command Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet - Remote login service, unencrypted text messages
25	TCP	Simple Mail Transfer Protocol (SMTP) E-mail Routing
53	TCP and UDP	Domain Name System (DNS)
67 and 68	UDP	Dynamic Host Configuration Protocol (DHCP)
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol (POP3) used by e-mail clients to retrieve e-mail from a server
119	TCP and UDP	Network News Transfer Protocol (NNTP)
123	UDP	Network Time Protocol (NTP)
137 and 138 and 139	TCP and UDP	NetBIOS
143	TCP	Internet Message Access Protocol (IMAP) Management of Digital Mail
161 and 162	TCP and UDP	Simple Network Management Protocol (SNMP)
194	TCP and UDP	Internet Relay Chat (IRC)
389	TCP and UDP	Lightweight Directory Access Protocol (LDAP)
443	TCP	HTTP Secure (HTTPS) HTTP over TLS/SSL
3389	TCP and UDP	Microsoft Terminal Server (RDP)

TCP/UDP Port Numbers					
7 Echo	554 RTSP	2745 Bagle.H	6891-6901	Windows Live	
19 Chargen	546-547 DHCPv6	2967 Symantec AV	6970	Quicktime	
20-21 FTP	560 rmonitor	3050 Interbase DB	7212	GhostSurf	
22 SSH/SCP	563 NNTP over SSL	3074 XBOX Live	7648-7649	CU-SeeMe	
23 Telnet	587 SMTP	3124 HTTP Proxy	8000	Internet Radio	
25 SMTP	591 FileMaker	3127 MyDoom	8080	HTTP Proxy	
42 WINS Replication	593 Microsoft DCOM	3128 HTTP Proxy	8086-8087	Kaspersky AV	
43 WHOIS	631 Internet Printing	3222 GLBP	8118	Privoxy	
49 TACACS	636 LDAP over SSL	3260 iSCSI Target	8200	VMware Server	
53 DNS	639 MSDP (PIM)	3306 MySQL	8500	Adobe ColdFusion	
67-68 DHCP/BOOTP	646 LDP (MPLS)	3389 Terminal Server	8767	TeamSpeak	
69 TFTP	691 MS Exchange	3689 iTunes	8866	Bagle.B	
70 Gopher	860 iSCSI	3690 Subversion	9100	HP JetDirect	
79 Finger	873 rsync	3724 World of Warcraft	9101-9103	Bacula	
80 HTTP	902 VMware Server	3784-3785 Ventrilo	9119	MXit	
88 Kerberos	989-990 FTP over SSL	4333 mSQL	9800	WebDAV	
102 MS Exchange	993 IMAP4 over SSL	4444 Blaster	9898	Dabber	
110 POP3	995 POP3 over SSL	4664 Google Desktop	9988	Rbot/Spybot	
113 Ident	1025 Microsoft RPC	4672 eMule	9999	Urchin	
119 NNTP (Usenet)	1026-1029 Windows Messenger	4899 Radmin	10000	Webmin	
123 NTP	1080 SOCKS Proxy	5000 UPnP	10000	BackupExec	
135 Microsoft RPC	1080 MyDoom	5001 Slingbox	10113-10116	NetIQ	
137-139 NetBIOS	1194 OpenVPN	5001 iperf	11371	OpenPGP	
143 IMAP4	1214 Kazaa	5004-5005 RTP	12035-12036	Second Life	
161-162 SNMP	1241 Nessus	5050 Yahoo! Messenger	12345	NetBus	
177 XDMCP	1311 Dell OpenManage	5060 SIP	13720-13721	NetBackup	
179 BGP	1337 WASTE	5190 AIM/ICQ	14567	Battlefield	
201 AppleTalk	1433-1434 Microsoft SQL	5222-5223 XMPP/Jabber	15118	Dipnet/Oddbob	
264 BGMP	1512 WINS	5432 PostgreSQL	19226	AdminSecure	
318 TSP	1589 Cisco VQP	5500 VNC Server	19638	Ensim	
381-383 HP Openview	1701 L2TP	5554 Sasser	20000	Usermin	
389 LDAP	1723 MS PPTP	5631-5632 pcAnywhere	24800	Synergy	
411-412 Direct Connect	1725 Steam	5800 VNC over HTTP	25999	Xfire	
443 HTTP over SSL	1741 CiscoWorks 2000	5900+ VNC Server	27015	Half-Life	
445 Microsoft DS	1755 MS Media Server	6000-6001 X11	27374	Sub7	
464 Kerberos	1812-1813 RADIUS	6112 Battle.net	28960	Call of Duty	
465 SMTP over SSL	1863 MSN	6129 DameWare	31337	Back Orifice	
497 Retrospect	1985 Cisco HSRP	6257 WinMX	33434+	traceroute	
500 ISAKMP	2000 Cisco SCCP	6346-6347 Gnutella			Legends
512 rexec	2002 Cisco ACS	6500 GameSpy Arcade			
513 rlogin	2049 NFS	6566 SANE			
514 syslog	2082-2083 cPanel	6588 AnalogX			
515 LPD/LPR	2100 Oracle XDB	6665-6669 IRC			
520 RIP	2222 DirectAdmin	6679/6697 IRC over SSL			
521 RIPng (IPv6)	2302 Halo	6699 Napster			
540 UUCP	2483-2484 Oracle DB	6881-6999 BitTorrent			

SSH-tunneled FTP is called secure FTP or FTP over SSH.

Server Message Block (SMB) is a communication protocol that Microsoft created for providing shared access to files and printers across nodes on a network.

SMB uses either IP port 139 or 445.

SMB uses client-server model

smbclient is a command line tool similar to a ftp connection while smbfs allows you to mount a SMB file share. Once a SMB share is mounted it acts similar to a local hard drive (you can access the SMB share with your file browser (nautilus, konqueror, thunar, other))

The smbclient can be used for different actions but the most popular usage is listing the shares for the specified SMB/CIFS Windows share service for the remote system. The -L option is used with the smbclient command to list all shares.

**Windows uses the backslash (\) for the file system delimiter.
For everything else the forward slash is used (/). Linux uses front /**

FTP AND SMB PROVIDES SAME COMMANDS

Learned bit about SMB and Nmap, How we connect with SMB in linux, flag or switch we use to list contents of the share. Commands to download file within SMB

