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:

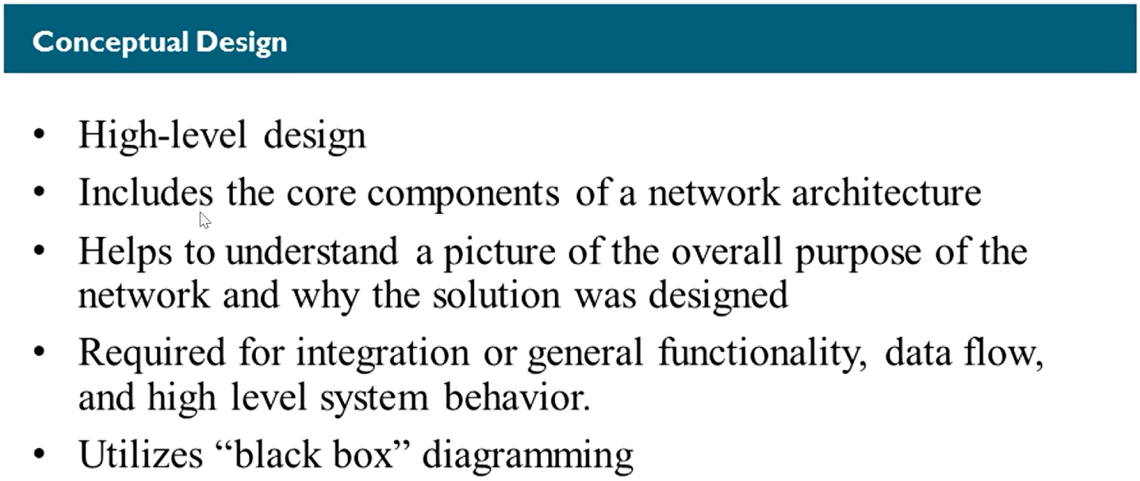
what is the risk, is it the highest prosperity risk, is it this solution the most cost effective way of reducing it.

`Network Security Essentials`

Defensible Network Architecture

`Network Architecture:`

- `Conceptual Desg`



Have segmented network instead of flat network.

- `Logical Design`

Logical Design

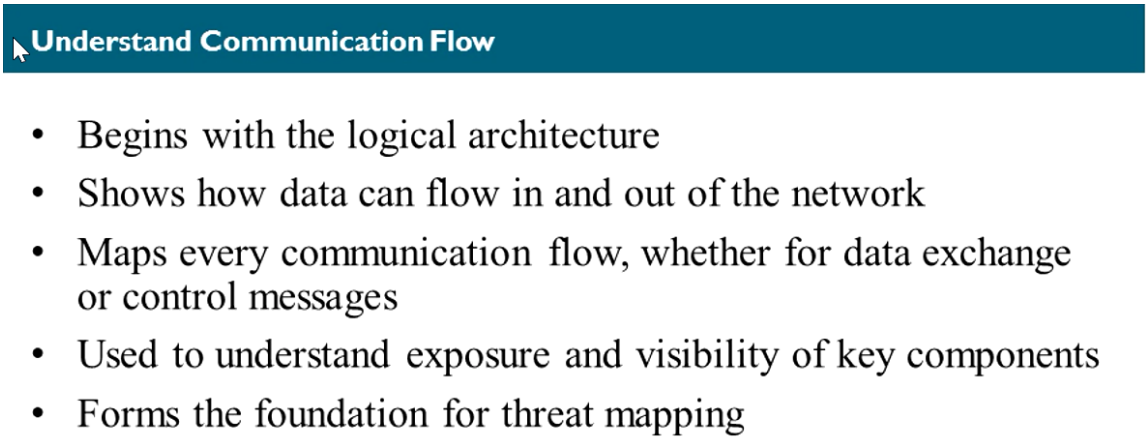
- Represents each logical function in the system
- More detailed
- Includes all the major components in the network plus their relationships
- Detailed data flows and connections are also mapped out
- Created primarily for developers and security architects
- Includes business services, application names,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

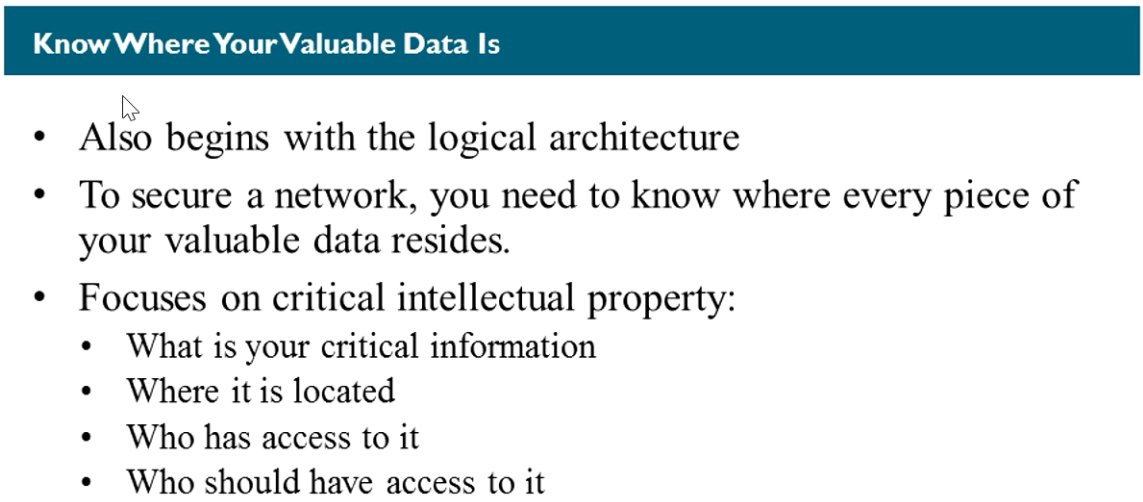
- `Understand Communication Flow`



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`



`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

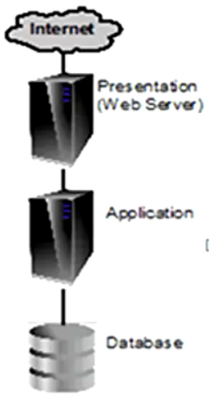
- Aids with Incident Response
- Provides Situational Awareness
- Reduces Cost of Network Monitoring
- Enables Attack Detection

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

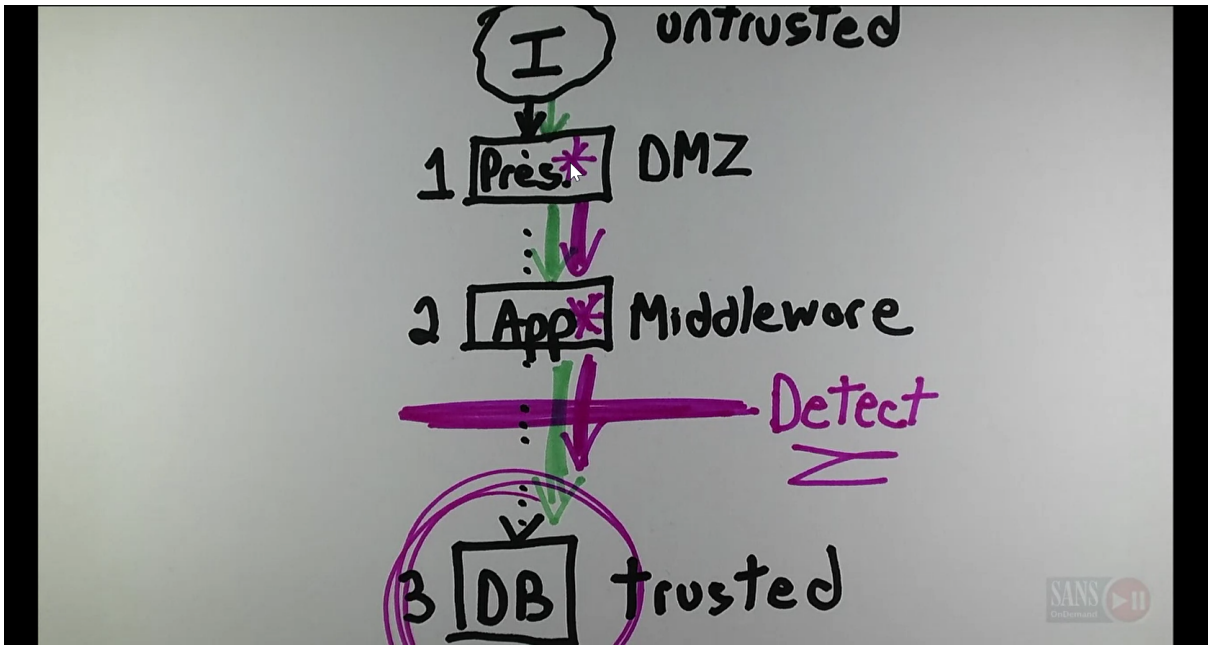
Prevention is ideal, Detection is must.

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



Three Tier Architecture



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

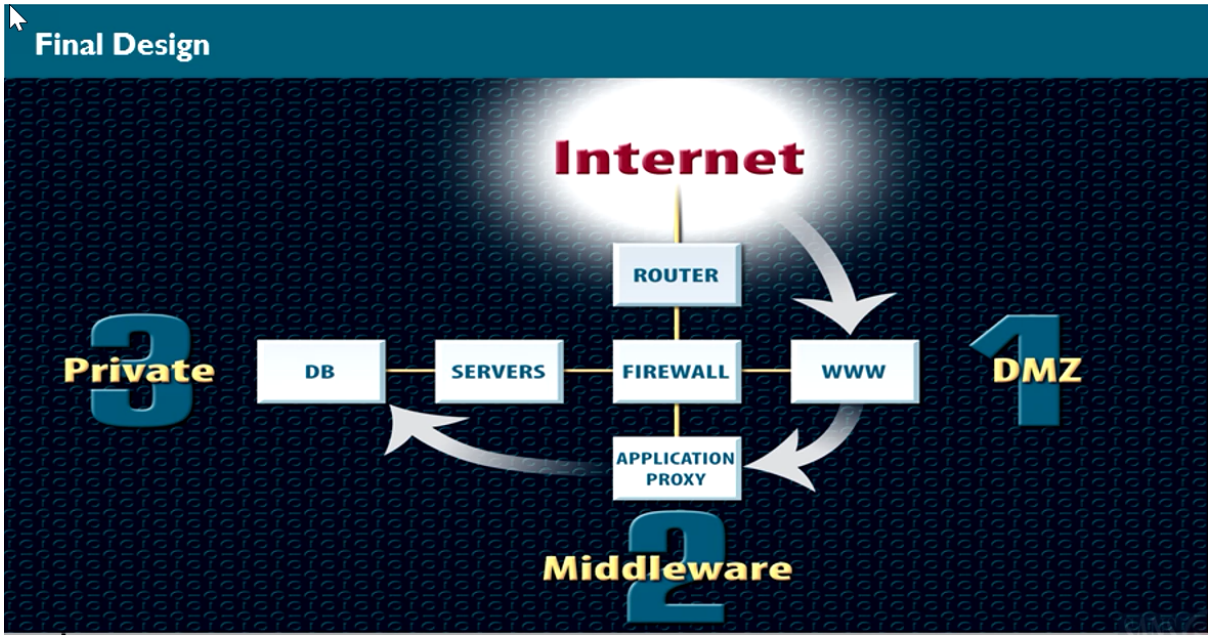
Locate firewalls:

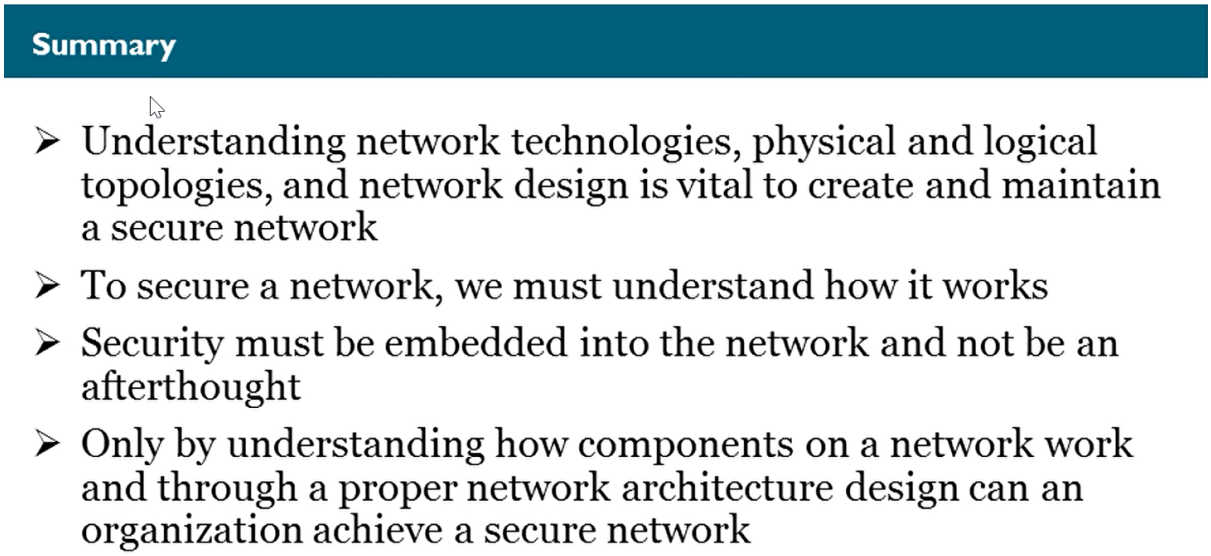
- Between the Internet and the other networks
- Between the semi-public and private network
- Between sections of varying trust levels

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





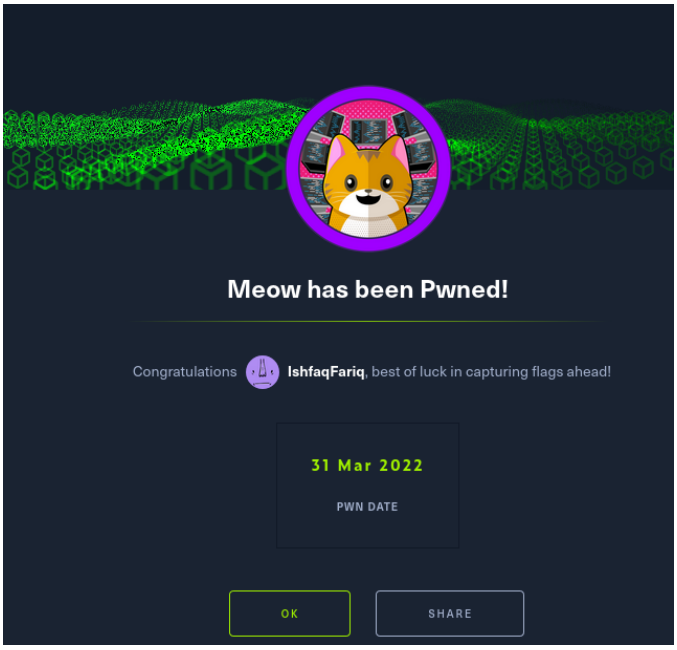
`NSE 2 Network Security Associate`

Finished the Network Security Associate Course.

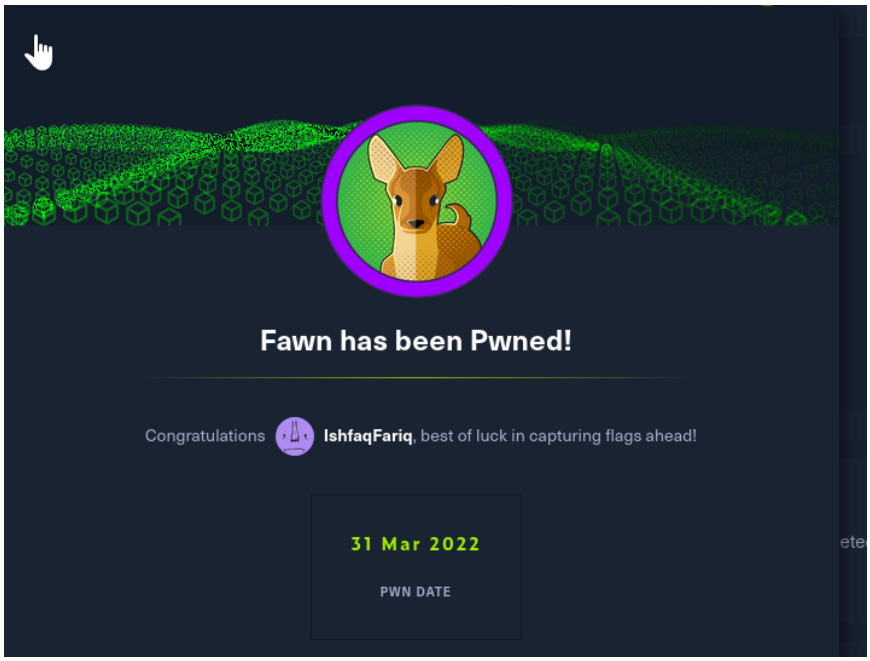
Solved Starting point labs on HTB

`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`

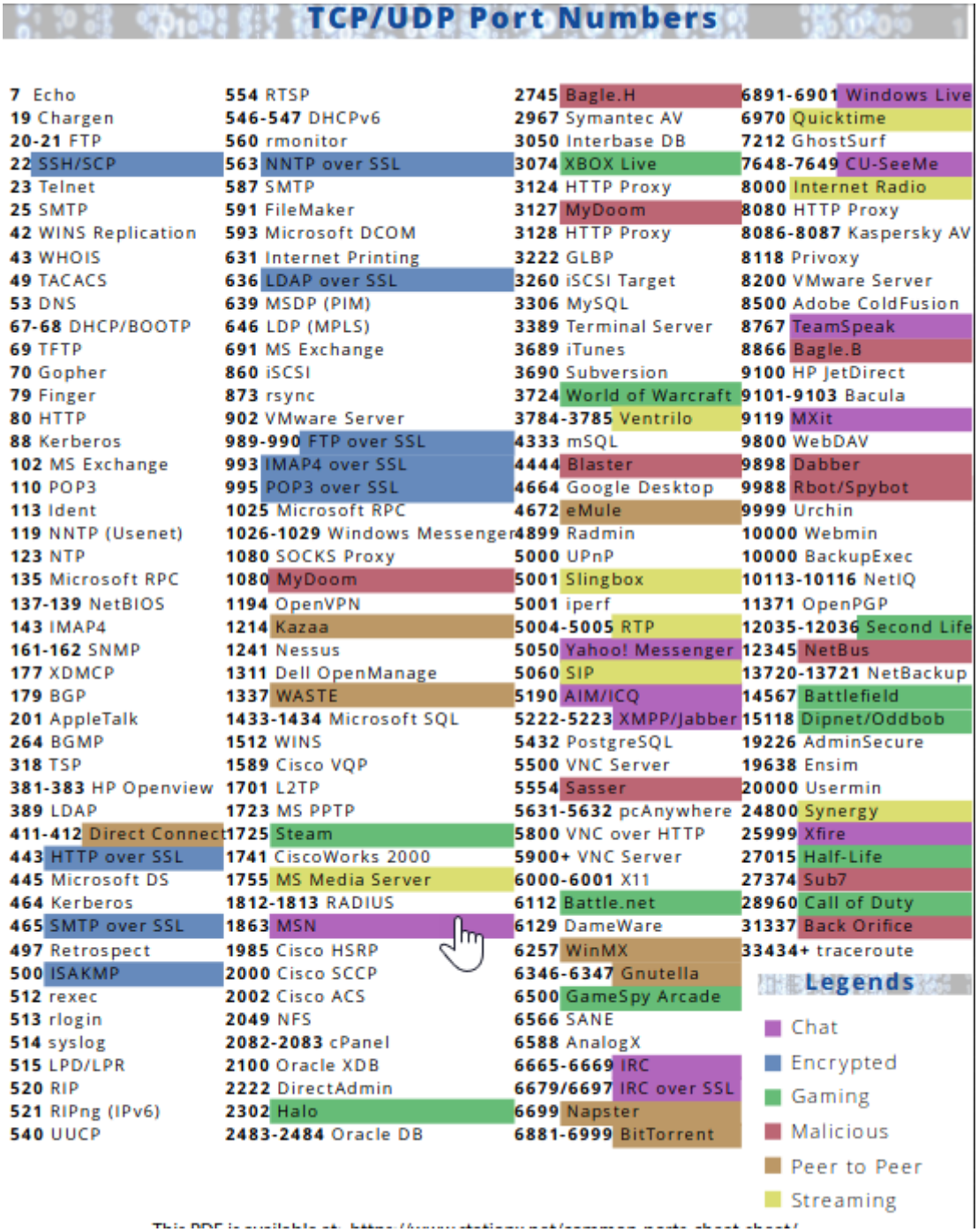
Searchsploit ”Service version here”

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)



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