TABSHOW
AUGUST 7 - 8, 2024

CYBERSECURITY PRECAUTIONS & VERIFICATION

Wayne M. Pecena CPBE, CBNE
Texas A&M University

CYBERSECURITY PRECAUTIONS & VERIFICATION

TABSHOW AUGUST 7 - 8, 2024

Cybersecurity continues to be a challenge and a priority for broadcast engineers. Proper cybersecurity precautions must be implemented to protect the IP dependent broadcast plant from cyber threats. Threats are constantly evolving, and cybersecurity precautions implemented must evolve as well. Proactive precautions must be in place and must be verified before any unknown gaps are exploited by the cyber-criminal. This presentation will provide practical to-do cybersecurity precaution steps and techniques to verify precautions thought to be in place are effectively implemented.

Outline:

- Cyber Threat Introduction
- Cybersecurity Principals & Standards
- Cybersecurity Mitigations Steps
- Closing Thoughts & Resources

Presentation goal:

Provide a understanding of cybersecurity basics in the broadcast station for the management and the engineers.

Provide practical and understandable implementation steps.

Cyber threats are alive & well

- Attack focus – broadcast IP infrastructure:
  - System tampering
  - System access
  - Information destruction
  - Information extortion
  - Operations disruption
- What are the threats:
  - Ransomware ← **#1 threat today**
  - Malware infection (virus, spyware)
  - Denial of Service (DDoS)
- Who is the Threat Actor?
  - Hacktivist
  - Criminal
  - Corporate Espionage
  - Terrorist
  - Cyber Warfare

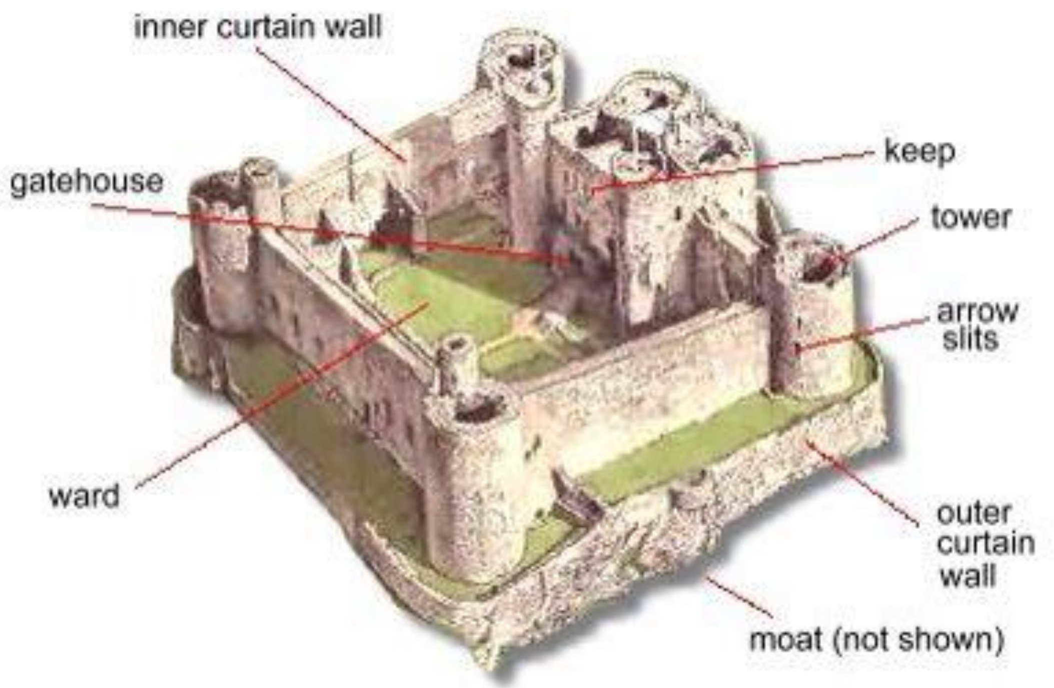
The Cyber Attack

Prevent Reconnaissance
Exploration or Probing
of the Network

Stage	Description
Reconnaissance	C:\>ping
Weaponization	Malware created tailored to target
Delivery to Target	Delivered to target **Dwell introduced**
Exploitation	Malware triggered
Access	Backdoor access implemented
C & C Access	Access established & maintained
Objective Archived	**Goal achieved!** Data destruction, data exfiltration, encryption

Key Cybersecurity Principles

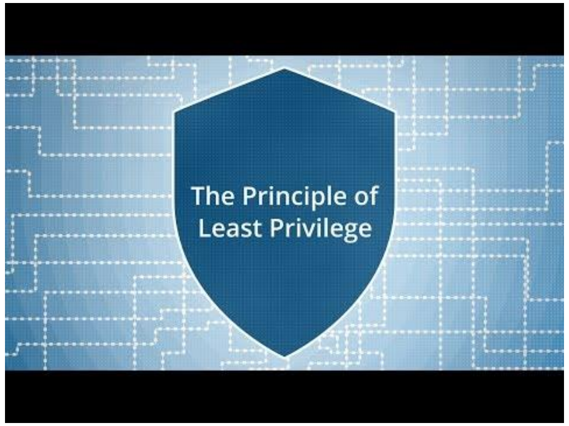
- Defense-in-Depth
  - Strategy to deploy multiple security barriers
- Least Privilege
  - Concept of granting minimum access to resources
- CIA Triad
  - Core objective of IT security:
    - Confidentially
    - Integrity
    - Availability
- NIST Framework
  - Structured best practices
  - Industry baseline



Harlech Castle, North Wales, built in 1283 AD

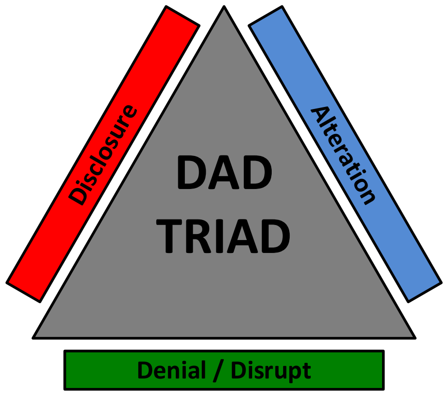
Key Cybersecurity Principles

- Defense-in-Depth
  - Strategy to deploy multiple security barriers
- Least Privilege
  - Concept of granting minimum access to resources
- CIA Triad
  - Core objective of IT security:
    - Confidentially
    - Integrity
    - Availability
- NIST Framework
  - Structured best practices
  - Industry baseline



Key Cybersecurity Principles

- Defense-in-Depth
  - Strategy to deploy multiple security barriers
- Least Privilege
  - Concept of granting minimum access to resources
- CIA Triad
  - Core objective of IT security:
    - Confidentially
    - Integrity
    - Availability
- NIST Framework
  - Structured best practices
  - Industry baseline



Key Principles

- Defense-in-Depth
  - Strategy to deploy multiple security barriers
- Least Privilege
  - Concept of granting minimum access to resources
- CIA Triad
  - Core objective of IT security:
    - Confidentially
    - Integrity
    - Availability
- NIST Framework
  - Structured best practices
  - Industry baseline

Function	Category	Subcategory
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected
		PR.DS-2: Data-in-transit is protected

PR.DS-2: Data-in-transit is protected	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12

SC-8 TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Control: The information system protects the [*Selection (one or more): confidentiality; integrity*] of transmitted information.

Supplemental Guidance: This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile

Control Enhancements:

(1) *TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC OR ALTERNATE PHYSICAL PROTECTION*

The information system implements cryptographic mechanisms to [*Selection (one or more): prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*Assignment: organization-defined alternative physical safeguards*].

Supplemental Guidance: Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.

Adopt a Heightened Cybersecurity Posture

- Minimize Attack Surface
  - Reduce risk of an attack
- Monitor & Protect Network
  - Detect cyber attack
- Develop & Exercise Incident Response Plan
  - Be prepared to respond to a cyber event
- Insure Operational Resilience
  - Backups / Redundancy

www.cisa.gov/shields-up

Minimize Attack Surface

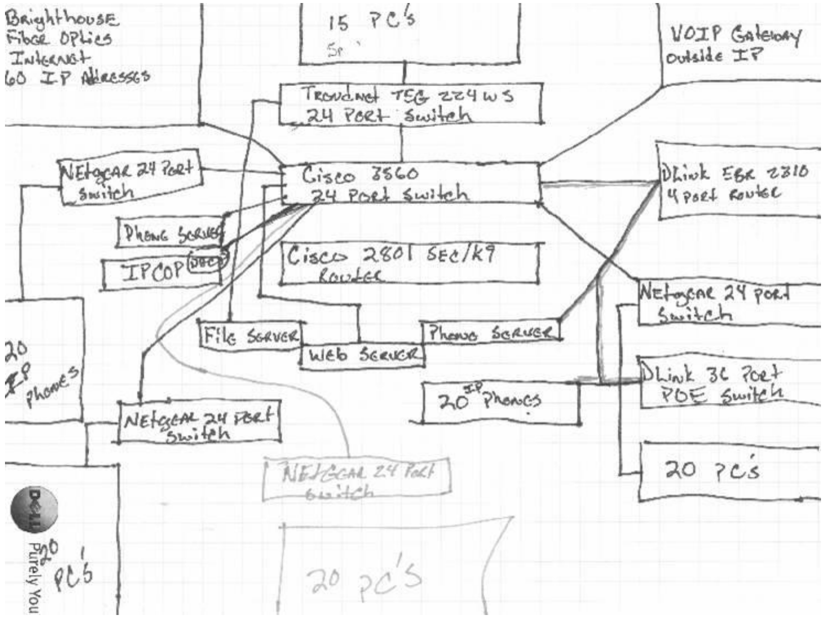
Harden Infrastructure

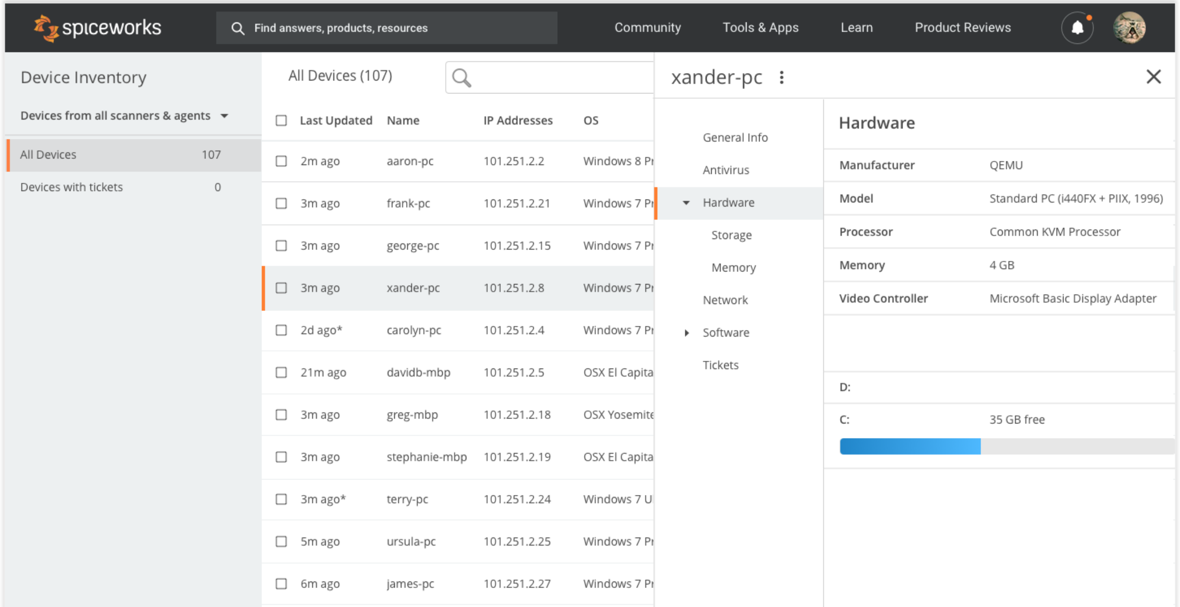
- Adopt cyber hygiene practices:
  - Maintain software / patch updates
  - Maintain regular vulnerability scans
  - Maintain antivirus software
  - Maintain spam filtering
  - Harden systems – remove unnecessary accounts, services & software
  - Implement MFA (multi-factor authentication)
  - Insure defaults logins are changed – enforce "strong" password policies

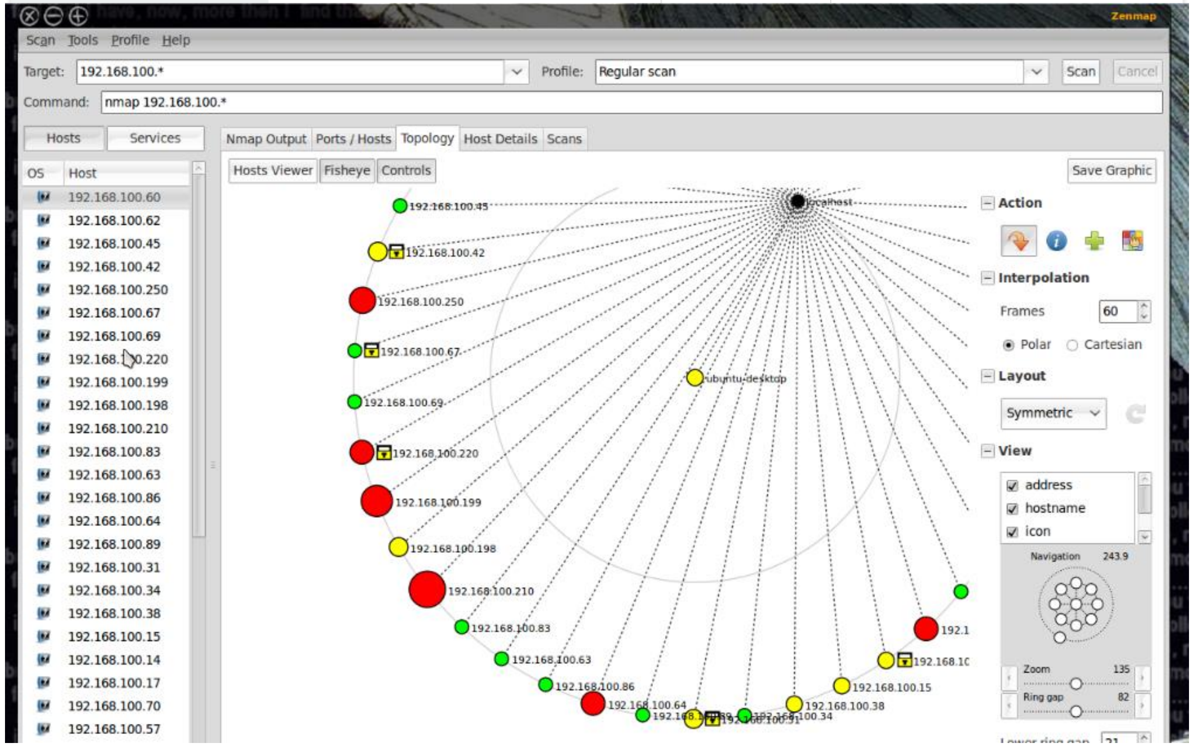
www.cisa.gov/shields-technical-guidance

My mitigation steps:

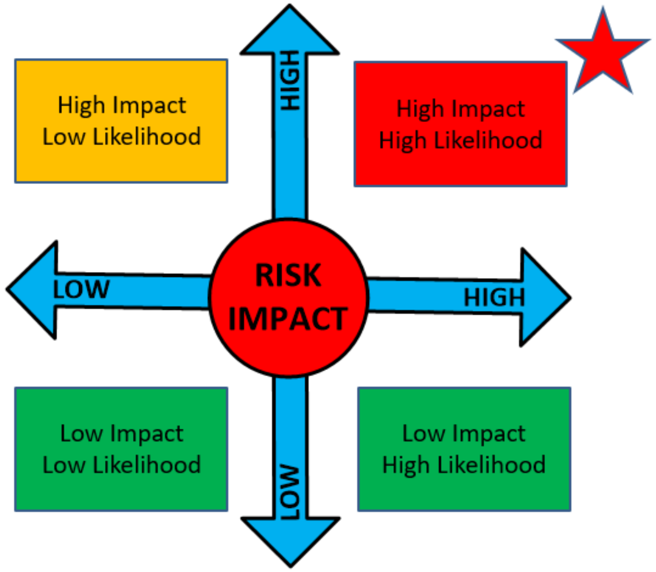
- Inventory
- Network architecture
- Physical security
- Ethernet switch port security
- Packet filtering / encryption
- Application focused
- Harden host devices
- Monitor
- Have a restoration plan
- Verification




spiceworks
Find answers, products, resources
Community
Tools & Apps
Learn
Product Reviews
Device Inventory
Devices from all scanners & agents
All Devices 107
Devices with tickets 0
All Devices (107)
Last Updated
Name
IP Addresses
OS
2m ago aaron-pc 101.251.2.2 Windows 8 Pr
3m ago frank-pc 101.251.2.21 Windows 7 Pr
3m ago george-pc 101.251.2.15 Windows 7 Pr
3m ago xander-pc 101.251.2.8 Windows 7 Pr
2d ago* carolyn-pc 101.251.2.4 Windows 7 Pr
21m ago davidb-mbp 101.251.2.5 OSX El Capita
3m ago greg-mbp 101.251.2.18 OSX Yosemite
3m ago stephanie-mbp 101.251.2.19 OSX El Capita
3m ago* terry-pc 101.251.2.24 Windows 7 U
5m ago ursula-pc 101.251.2.25 Windows 7 Pr
6m ago james-pc 101.251.2.27 Windows 7 Pr
xander-pc
General Info
Antivirus
Hardware
Storage
Memory
Network
Software
Tickets
Hardware
Manufacturer QEMU
Model Standard PC (i440FX + PIIX, 1996)
Processor Common KVM Processor
Memory 4 GB
Video Controller Microsoft Basic Display Adapter
D:
C: 35 GB free

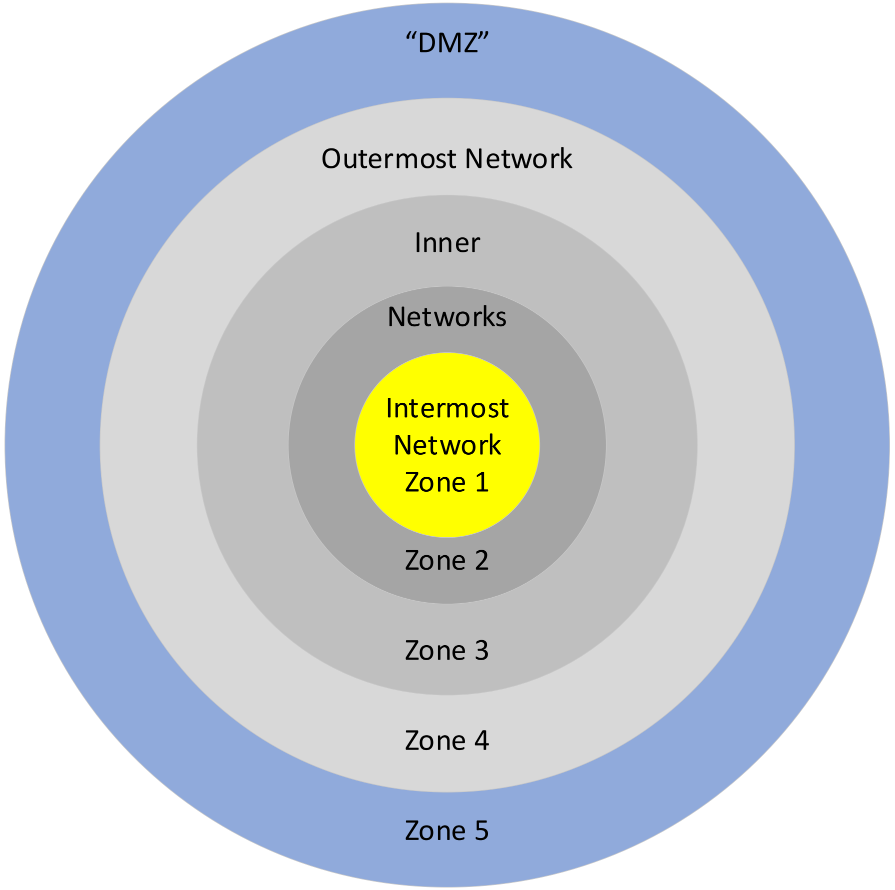

Zenmap
Scan Tools Profile Help
Target: 192.168.100.*
Profile: Regular scan
Scan
Cancel
Command: nmap 192.168.100.*
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
192.168.100.60
192.168.100.62
192.168.100.45
192.168.100.42
192.168.100.250
192.168.100.67
192.168.100.69
192.168.100.220
192.168.100.199
192.168.100.198
192.168.100.210
192.168.100.83
192.168.100.63
192.168.100.86
192.168.100.64
192.168.100.89
192.168.100.31
192.168.100.34
192.168.100.38
192.168.100.15
192.168.100.14
192.168.100.17
192.168.100.70
192.168.100.57
Hosts Viewer
Fisheye
Controls
Save Graphic
localhost
ubuntu-desktop
Action
Interpolation
Frames 60
Polar
Cartesian
Layout
Symmetric
View
address
hostname
icon
Navigation 243.9
Zoom 135
Ring gap 82


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
CISA Known Exploited Vulnerabilities Catalog

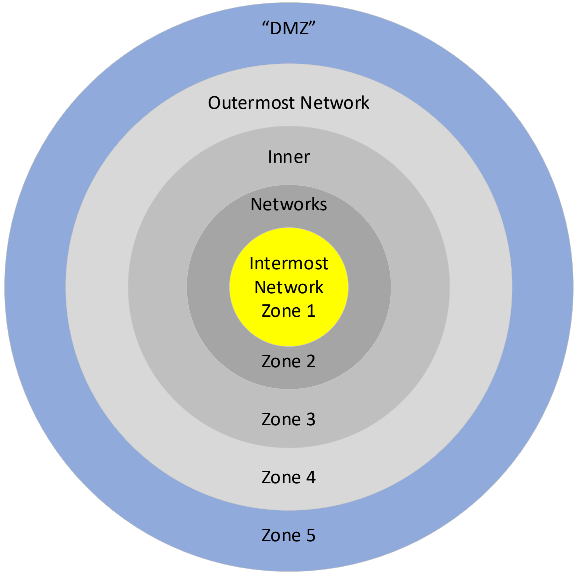

High Impact
Low Likelihood
High Impact
High Likelihood
HIGH
LOW
RISK
IMPACT
HIGH
LOW
Low Impact
Low Likelihood
Low Impact
High Likelihood

My mitigation steps:

- Inventory
- Network architecture
- Physical security
- Ethernet switch port security
- Packet filtering / encryption
- Application focused
- Harden host devices
- Monitor
- Have a restoration plan
- Verification

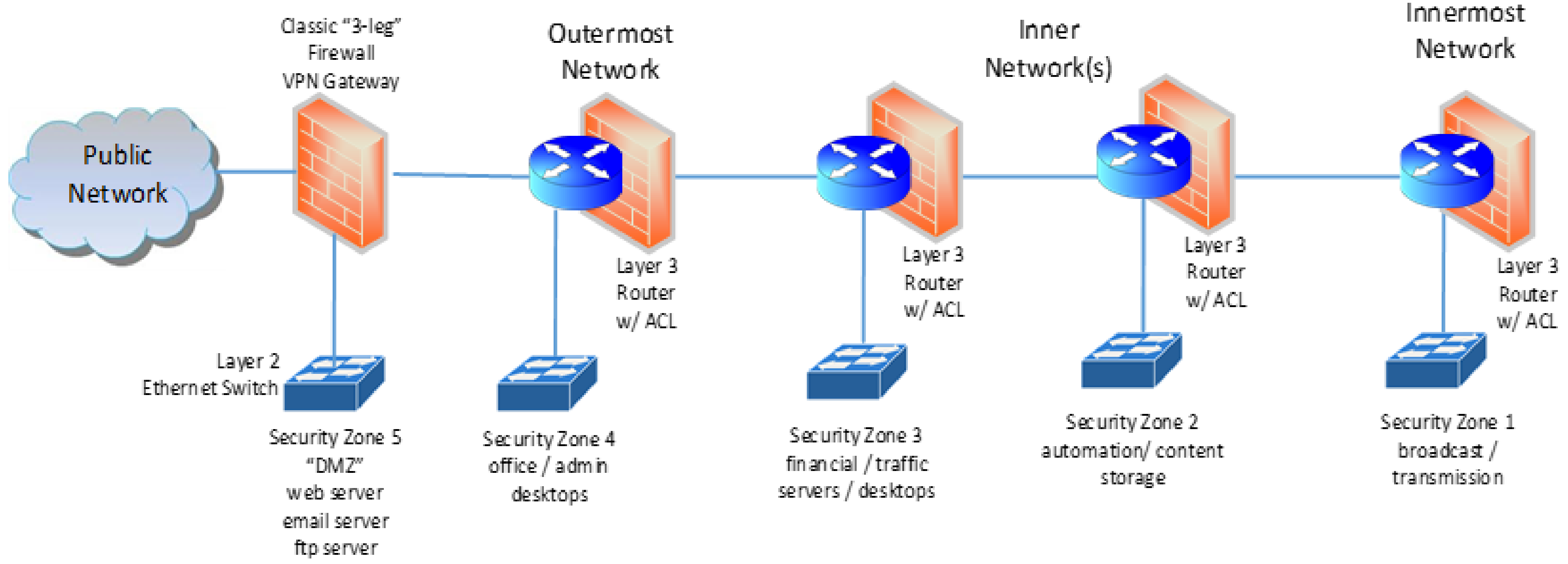


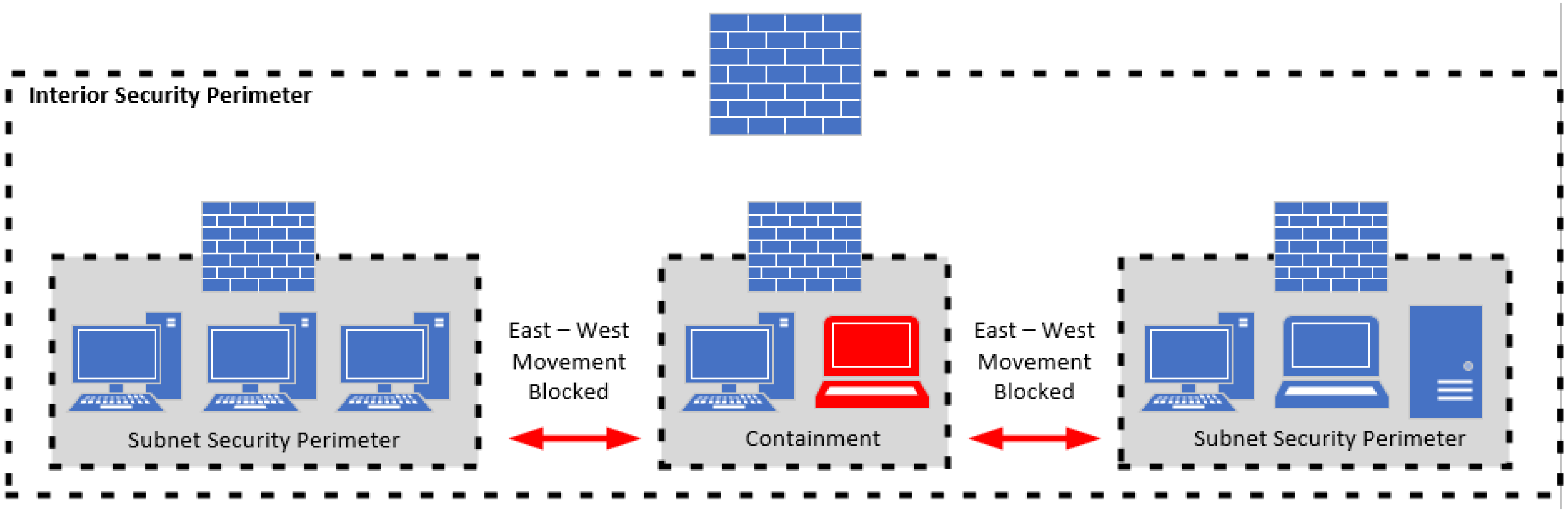
The Segmented Network



- Design architecture that divides a network into smaller, unique, compartmentalized sub-networks.
- Advantages: (CompTIA)
  - Reduces the attack plane.
  - Reduces the compliance scope requirements related to auditing.
  - Limit impact of a cyber attack due to smaller attack surface.
  - Improves network access control.
  - Allows enhanced network monitoring, network access and network devices.
  - Improves protection of endpoint devices (specific to IoT devices)
  - Improves network performance due to network traffic containment/reduction.

Layered, segmented, hierarchical network





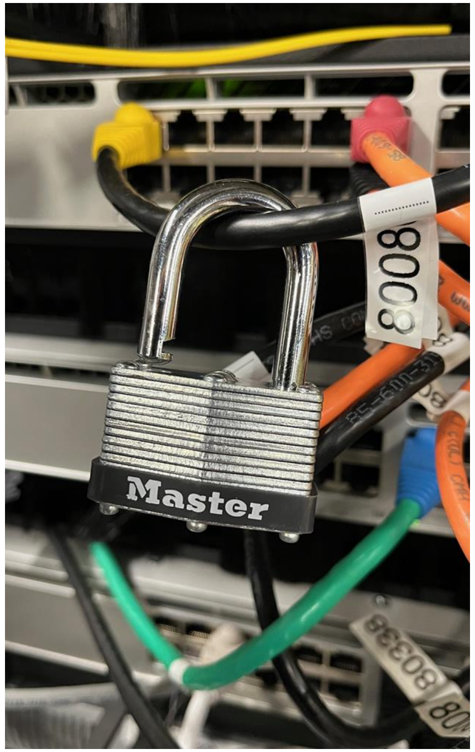
My mitigation steps:

- Inventory
- Network architecture
- Physical security
- Ethernet switch port security
- Packet filtering / encryption
- Application focused
- Harden host devices
- Monitor
- Have a restoration plan
- Verification

- Protection of IT assets from loss or damage by deterring unauthorized access
- Framework focus:
  - Monitoring (surveillance)
  - Access controlled environment
  - Audit logging
- Defend against:
  - Intentional damage/sabotage
  - Human error

My mitigation steps:

- Inventory
- Network architecture
- Physical security
- Ethernet switch security
- Packet filtering / encryption
- Application focused
- Harden host devices
- Monitor
- Have a restoration plan
- Verification



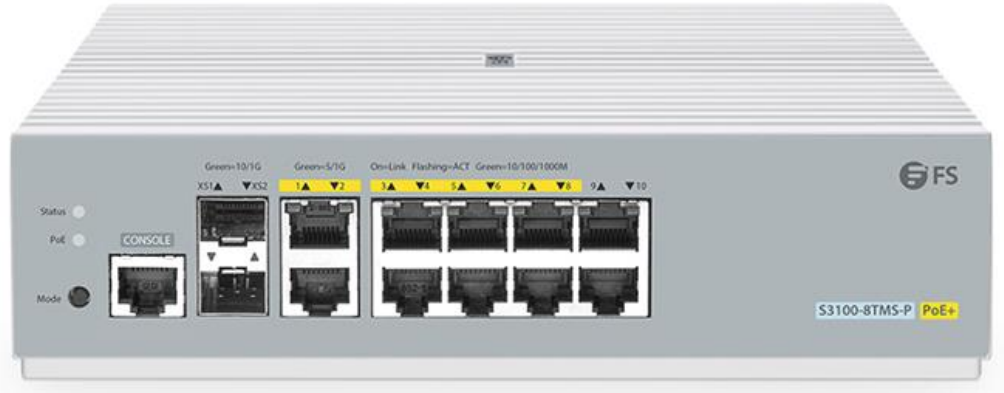
Ethernet switch security

- Common Ethernet switch exploits:
  - Bridge table flooding
  - MAC address spoofing
- Mitigation:
  - Port Security
  - Snooping detection / prevention
  - Flooding protection

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0006.2ac1.2886    DYNAMIC     Fa0/1
   1    0009.7cdc.1420    DYNAMIC     Fa0/3
   1    0060.7052.2182    DYNAMIC     Fa0/4
   1    0090.2b27.d6c7    DYNAMIC     Fa0/2
Switch#
```



MAC Address Formats

Always 48 Bits – Expressed as Hexadecimal

Can Be Represented in Several Formats:

00:A0:C9:14:C8:29

00-A0-C9-14-C8-29

00A0.C914.C829

Switch best practices

Disable unused ports

Avoid use of VLAN 1 (default)

Enable port security:
1 - MAC address violation occurs
2 - Port drops frames (protect mode)
3 - SNMP trap generated (violation notification)

VLAN 100 VLAN 200 VLAN 300

Segment networks

Allow only 1 MAC address / port

Configure "trunk" or "tagged" port VLAN's only when required

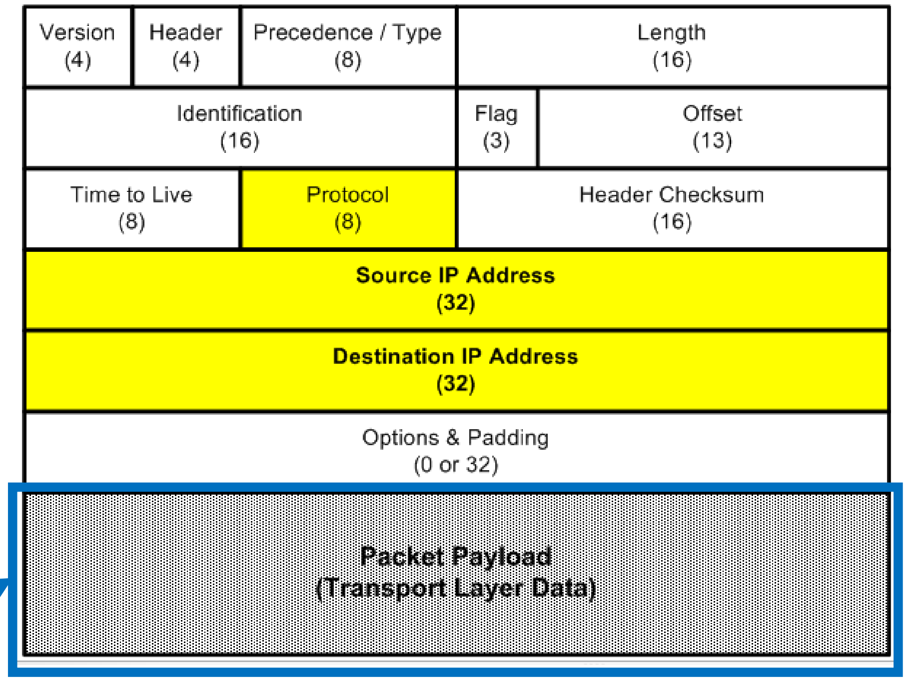
My mitigation steps:

- Inventory
- Network architecture
- Physical security
- Ethernet switch security
- **Packet filtering / encryption**
- Application focused
- Harden host devices
- Monitor
- Have a restoration plan
- Verification

Packet Filtering

- Packet header decoded
- Decision based upon pre-defined rule – **Permit or Deny** (Block)
- Header info considered:
  - IP Address (source & destination)
  - Protocol
  - Port (source & destination)
- Applied to Ingress and/or Egress interface(s)
- ACL packet filtering:
  - Stateless Packet Filtering – fixed rule based
- Firewall packet filtering:
  - Stateless Packet Filtering – fixed rule based
  - Stateful Packet Filtering – Flow or conversation based

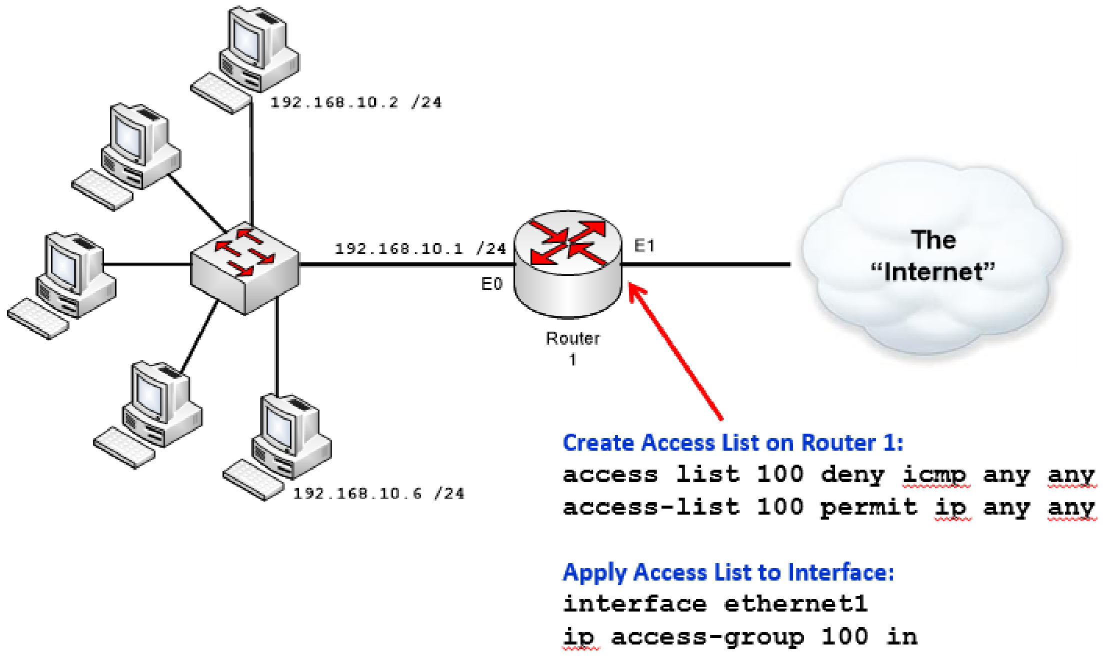
IPv4 Packet Header

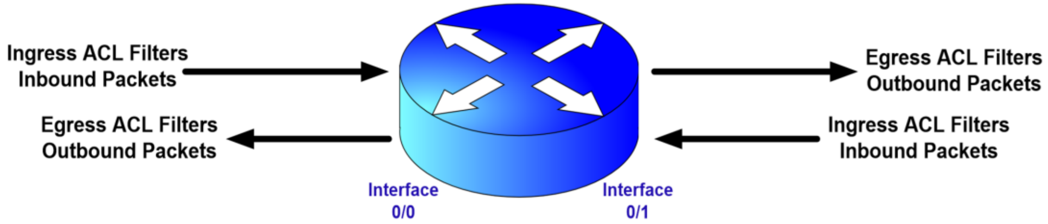


Payload is NOT examined

Access Control List

- Provides “Basic” Network Access Control
- **Filter** IP Network Packets:
  - Forwarded @ Egress Interface
  - Blocked @ Ingress Interface
- **Standard** Access List:
  - Can Only Permit or Deny The Source Host IP Address
- **Extended** Access List:
  - Can Permit or Deny Based Upon:
    - Source IP Address
    - Destination IP Address
    - TCP Port #
    - UDP Port #
    - TCP/IP Protocol





The Firewall

“State”:
A dynamic rule created by the firewall based upon a host-host source destination address-port combination

Stateless Firewall

Filtering Parameters:
IP Source Address
IP Destination Address
Protocol
Connection Status
Source Port Number
Destination Port Number

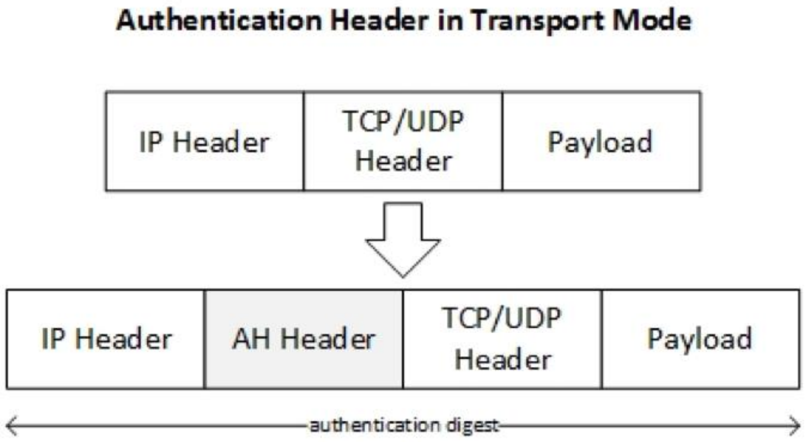
Stateful Firewall

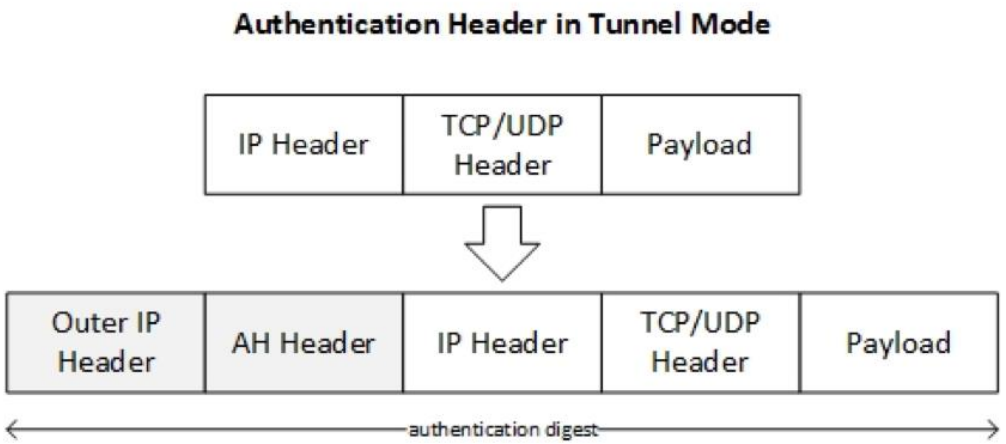
Aware of connections between protected network host & un-protected host.
Maintains connection “state table” to implement security policy

Filtering Parameters:
IP Source Address
IP Destination Address
Protocol
Connection Status
Source Port Number
Destination Port Number

Internet Protocol Security “IPSec”

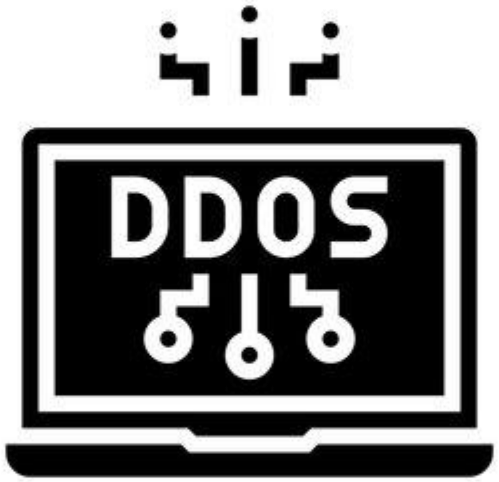
- IP Security “IPsec”
  - End-to-End Scheme to Encrypt Communications
  - Layer 3 Implementation
- Modes:
  - Transport (Host-to-Host Payload) Implementation
  - Tunnel Implementation (VPN Packet Encapsulation)





My mitigation steps:

- Inventory
- Network architecture
- Physical security
- Ethernet switch security
- Packet filtering / encryption
- Application focused
- Harden host devices
- Monitor
- Have a restoration plan
- Verification



Application focused security:

- Layer 7 is closest to the user – potentially most vulnerable – popular attack vector!
- Layer 7 attacks – targets applications:
    - Distribution Denial of Service “DDoS” (SYN flood, HTTP flood,)
    - Web related (http GET, POST)
    - SQL injection
    - Cross-Site Scripting (XSS)

- Mitigating:
    - Deploy active network monitoring, alerting, rate limiting, filtering & redundancy
    - Proper application design (validate input data, least privilege access)
    - Use Hypertext Transfer Protocol Secure “https”
    - Captcha test, Multifactor Authentication (MFA), Passkey

My mitigation steps:

- Inventory
- Network architecture
- Physical security
- Ethernet switch security
- Packet filtering / encryption
- Application focused
- Harden host devices
- Monitor
- Have a restoration plan
- Verification

Securing the Host Devices

- Hardening is a process to reduce the attack surface of a host device operating system
- Implementation activities typically include:
  - Change default passwords – implement strong password management
  - Remove / disable un-used applications / services (de-bloating)
  - Remove / disable unencrypted remote services (IE Telnet, FTP)
  - Restrict physical access (console, aux, tty ports)
  - Use secure services (SNMPv3, SFTP, FTPS, SSH)
  - Control remote access (ACL)
  - Delete un-used / stale accounts
  - Backup configurations – store offline
  - Keeping updates & patches up-to-date
  - Closing network “back doors”

Microsoft Windows

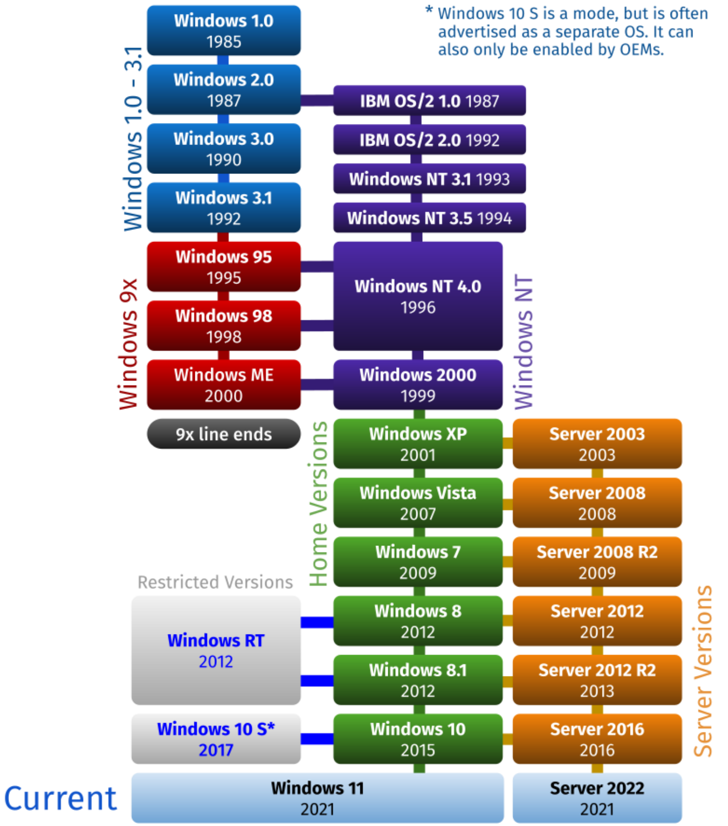
Linux

CISCO IOS

MikroTik RouterOS

Windows Op System (10/11)

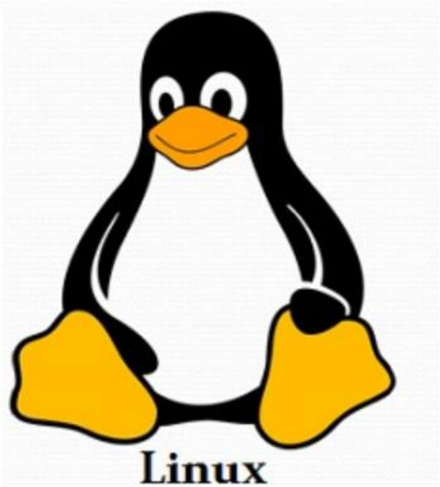
- Separate user and admin account(s) – non admin user accounts
- Obfuscate local admin account (rename)
- Disable “guest” account(s)
- Disable LAN Manager
- Use “strong” password management
- Utilize data encryption (BitLocker)
- Create a system Restore Point
- Insure “drivers” are up-to-date
- Insure “bundled” applications are up-to-date OR remove
- Remove / disable “un-needed” services
- Utilize “domain controller” to administer multiple hosts w/ extreme caution



Graphic source: CrustyCaverns

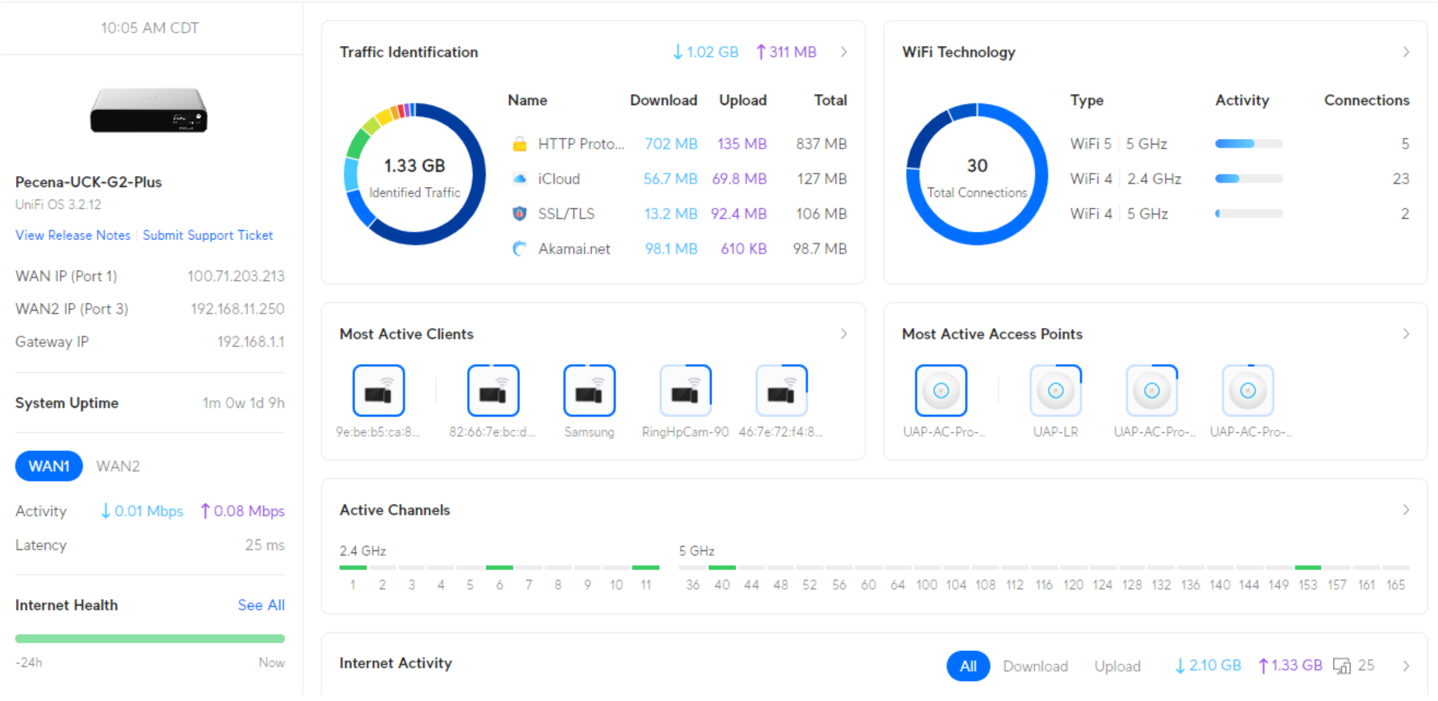
Linux Op System

- Password protect the host BIOS
- Enable disk encryption
- Lock boot directory (read-only)
- Implement Brute Force Detection (BFD)
  Lock accounts after x failed login attempts (3-5)
- Disable USB storage
- Maintain system (kernel) updates & patches
- Disable / remove any un-used services (ie telnet, tftp, etc)
- Check for open ports (pen test)
- Secure SSH (change port, disable root login)
- Utilize SELinux (Security Enhanced Linux)
- Disable network parameters:
  - IP Forwarding
  - ICMP Re-Directs
  - Send Packet Re-Directs
- Set a “strong” password hashing algorithm (SHA512)
- Insure permissions are valid



My mitigation steps:

- Inventory
- Network architecture
- Physical security
- Ethernet switch security
- Packet filtering / encryption
- Application focused
- Harden host devices
- **Monitor**
- Have a restoration plan
- Verification

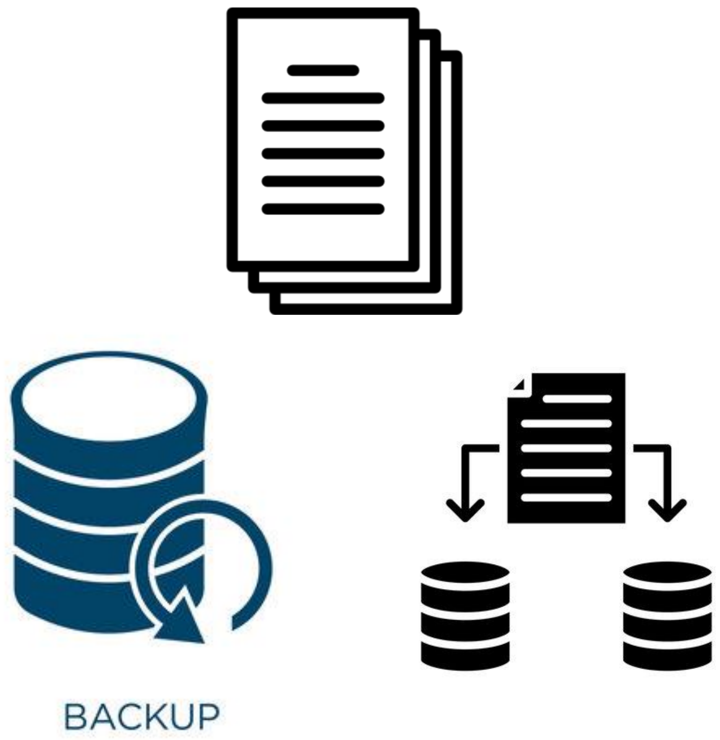


Monitor

- Monitor IT systems - Know what is normal
  - Know when an abnormality occurs
  - Know when performance changes
- What to monitor:
  - Network infrastructure (avail & utilization)
  - Servers (memory & processor utilization)
  - Storage system (capacity & activity)
  - Application availability & performance (APM)
  - Service availability (premise & cloud)
  - User activity
- Alerting:
  - Urgency levels – error aggregation
  - Email, SMS

My mitigation steps:

- Inventory
- Network architecture
- Physical security
- Ethernet switch security
- Packet filtering / encryption
- Application focused
- Harden host devices
- Monitor
- Have a restoration plan
- Verification



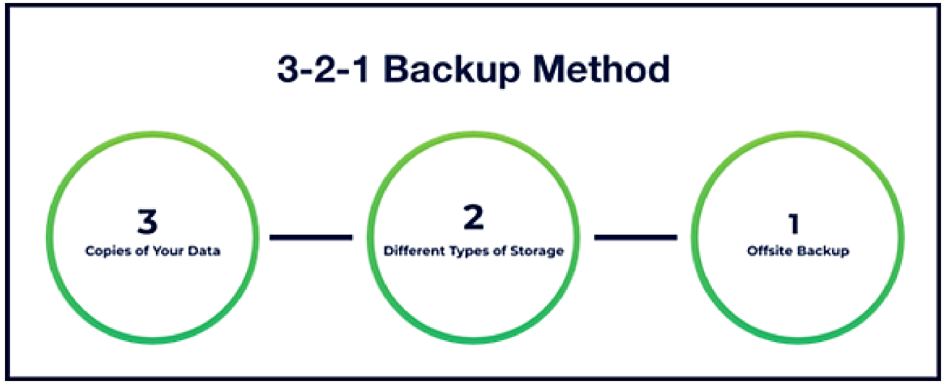
Restoration Plan

- Respond & Recover, with a recovery plan:
  - Cyber event
  - Human error or natural disaster
- Incident Response Plan (NIST):
  - Preparation
  - Detection & analysis
  - Containment, eradication and recovery
  - Post-event activity
- Recovery plan:
  - Fault tolerant & redundant hardware
  - Redundant network infrastructure
  - Maintain data backups

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Data Backup Practices

- Provides the "best" defense, but last resort
- Backup "best practices":
  - Match backup practices to your business workflow:
    - Full dataset
    - Incremental / Differential dataset
    - Image backup (data block)
    - Recovery point objective (RPO) / Recovery time objective (RTO)
  - Use "intelligent" backup solutions – isolate backups:
    - Mount target drive when required
    - Use "immutable" storage "WORM"
    - Use caution when "mounting" drives – set to RO after write
  - Keep multiple copies at multiple locations - "3-2-1" rule
- Restoration:
  - Recovery plan – know how to restore
  - Know the restoration priority – dependencies of backups
  - Know the restoration time required (RTO)
  - TEST, TEST, TEST restoration – insure you can restore!
  - Data backups & data retention is not the same!



My mitigation steps:

- Inventory
- Network architecture
- Physical security
- Ethernet switch security
- Packet filtering / encryption
- Application focused
- Harden host devices
- Monitor
- Have a restoration plan
- Verification

Verification with Penetration Testing

- Penetration Testing (pen test or pen testing):
  - Evaluates cybersecurity validity & effectiveness
  - Is a key component of security audit
  - Is a simulated (controlled) cyberattack
- Test Scope:
  - Physical security
  - Network infrastructure
  - Software applications
  - Mobile device (BYOD)
  - WiFi, remote access, VPN

  All
- Test categories:
  - Port scanning
  - Traffic analysis
  - Proxy interception
  - Password crack
  - Vulnerability scanning
- Important Note - Vulnerability scanning & penetration testing are not the same!

Tools of the Threat Actor & Penetration Tester

Most Popular

- Nmap (port scanner)
- Kali Linux (suite of tools including Metraploit)
- Burp Suite (MitM proxy)
- Wireshark (network traffic analyzer)
- John the Ripper (password cracker)
- Hashcat (password cracker)
- Invicti (application vulnerability assessment)

Online Tools:

Shodan

Censys

nmap

Uses of nmap includes:

- Create network host map
- Network host discovery
- Determine the host OP system & version
- Determine open ports/active services & version
- Security audit & vulnerability assessment
- Over 125 commands:
  - Scan Single Host
  - Scan Multiple Hosts
  - Scan Range of IP Addresses
  - Scan a Subnet
  - Perform an Aggressive Scan
  - Firewall Evasion Techniques
  - Discovery Attempt: No Ping
  - Discovery Attempt: Ping Only
  - Discovery Attempt: Host OS

```
Initiating Parallel DNS resolution of 1 host. at 10:29
Completed Parallel DNS resolution of 1 host. at 10:29, 0.00s elapsed
Initiating SYN Stealth Scan at 10:29
Scanning dasdec-tv-ebs106ddd.kamu.tamu.edu (128.194.247.138) [1000 ports]
Discovered open port 80/tcp on 128.194.247.138
```

```
Discovered open port 80/tcp on 128.194.247.138
Discovered open port 443/tcp on 128.194.247.138
Discovered open port 22/tcp on 128.194.247.138
Discovered open port 631/tcp on 128.194.247.138
Completed SYN Stealth Scan at 10:29, 4.91s elapsed (1000 total ports)
```

Registered Ports:
80 - HTTP
443 - HTTPS
22 - SSH
631 - IPP

```
Completed NSE at 10:29, 7.10s elapsed
Initiating NSE at 10:29
Completed NSE at 10:29, 0.00s elapsed
Nmap scan report for dasdec-tv-ebs106ddd.kamu.tamu.edu (128.194.247.138)
Host is up (0.00017s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE  VERSION
```

```
PORT      STATE  SERVICE   VERSION
22/tcp    open   ssh       OpenSSH 6.9 (protocol 2.0)
| ssh-hostkey:
|   1024 b7:24:25:72:89:f1:d3:8b:5a:82:44:0b:86:58:89:4c (DSA)
|   2048 e4:96:eb:de:a0:b5:65:b5:30:ab:aa:57:f5:09:5e:f8 (RSA)
|_  256 e2:54:4a:21:b2:66:c0:b6:46:ec:17:7b:ae:1e:f3:63 (ECDSA)
80/tcp    open   http      Apache httpd 2.2.26-31 ((Unix))
| http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_  Potentially risky methods: TRACE
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.2.26-31 (Unix)
|_http-title: *******The Digital Alert Systems DASDEC Base Page*
443/tcp   open   ssl/http Apache httpd 2.2.26-31 ((Unix))
```

SHODAN

What is SHODAN?

- Shodan is a "search engine"
  - A unique search engine – discovers IP host devices
  - Scans public Internet for IP devices with open ports (port=service availability)
  - Captures detail information when an open port is found
  - Compiles gathered information into a database available for query
- Useful for:
  - A quick view of Internet facing visibility
  - Initial step to map an organizations network "network reconnaissance"
  - Exploring specific host device types
  - Subscription levels offer continuous visibility monitoring services

- What can be found:
  - Webcams & Security Cameras, Servers, Ethernet switches & routers, Firewalls, VoIP desk sets, IoT devices (thermostats, lights, appliances, etc), Industrial control systems (SCADA, PLC, etc), IP enable broadcast equipment

SHODAN

https://www.shodan.io

Mitigation Step Summary:

- Inventory of IT assets – prioritize based on risk
- Start with a segmented network architecture
- Secure physical network & IT components
- Utilize Ethernet switch security capabilities
- Utilize packet filtering (ACL / firewall) & encryption to control access
- Utilize application security
- Harden host devices
- Monitor infrastructure – known when something is not right
- Have a restoration plan – know how to restore
- Verify cybersecurity protections

Closing thoughts:

- Accept - Their is **NO SINGLE** Solution! - Implement multiple protections through **“DiD”**
- Know what you need to protect – **IT inventory and access risk**
- **Segment** your network (VLAN) – reduce attack surface & east-west movement - enhance performance
- Utilize Ethernet switch **port security** features
- Change **default** login credentials - Use **unique** & **strong** passwords (paraphrases)
- **Separate** Admin & User accounts on hosts (WIN)
- **Limit** access (users & applications) – apply principal of “**least privilege**”
- Control access - use packet **filtering** - (ACL and/or firewall) – **deny by default** – SSH & MFA
- **Disable / minimize** services not required – close/block ports – **minimize** macros / RDP use
- **Monitor** you IT infrastructure / network – **review logs** - know what is normal
- Use “**intelligent**” host backup solutions – **test** backup restoration – follow “**3-2-1**” rule
- Keep systems **updated** / **patched –** use **KEV** to guide priorities
- Utilize **signature based** deep-packet inspection antivirus/malware – keep updated (often daily)
- Perform routine **vulnerability** scans and periodic visibility assessment through **pen testing**
- Don’t overlook **social engineering** – engage & educate users – **phishing** is alive and effective!

A single successful Social Engineering “phishing” attempt can instantly negate your efforts!

Social Engineering

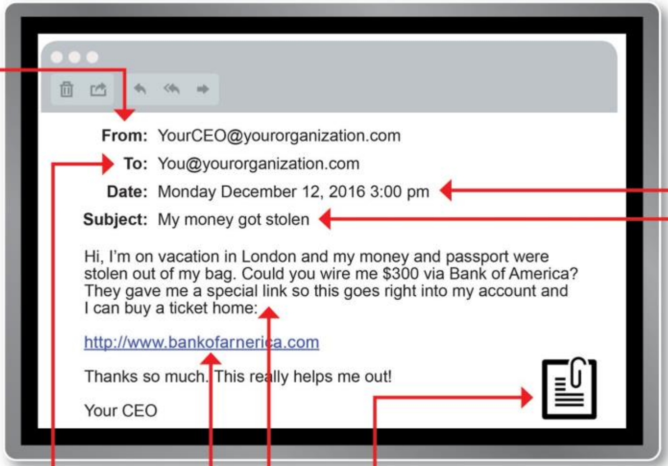
- Has become a successful technique:
  - System exploits have become more difficult
  - Now easier to exploit human weakness
- Use of deception to obtain information or convince to install malware:
  - Prey upon human “willingness to be helpful”
  - Persuasive tactics
  - Psychological manipulation
- Tactics based upon principals of influence: (Robert Cialdini - behavioral psychologist)
  - Reciprocity
  - Commitment
  - Social Proof
  - Authority
  - Liking
  - Scarcity
- Popular tactics:
  - Phishing (everyone - wide audience appeal)
  - Spear phishing (specific target audience – individual, group, organization)
  - Whaling (c suite focused audience – “executive” phishing)
  - Smishing / vishing (SMS & VM based)

knowbe4

Ongoing user training to understand and recognize social engineering tactics is the best defense.

CISA.gov

Social Engineering Red Flags



FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

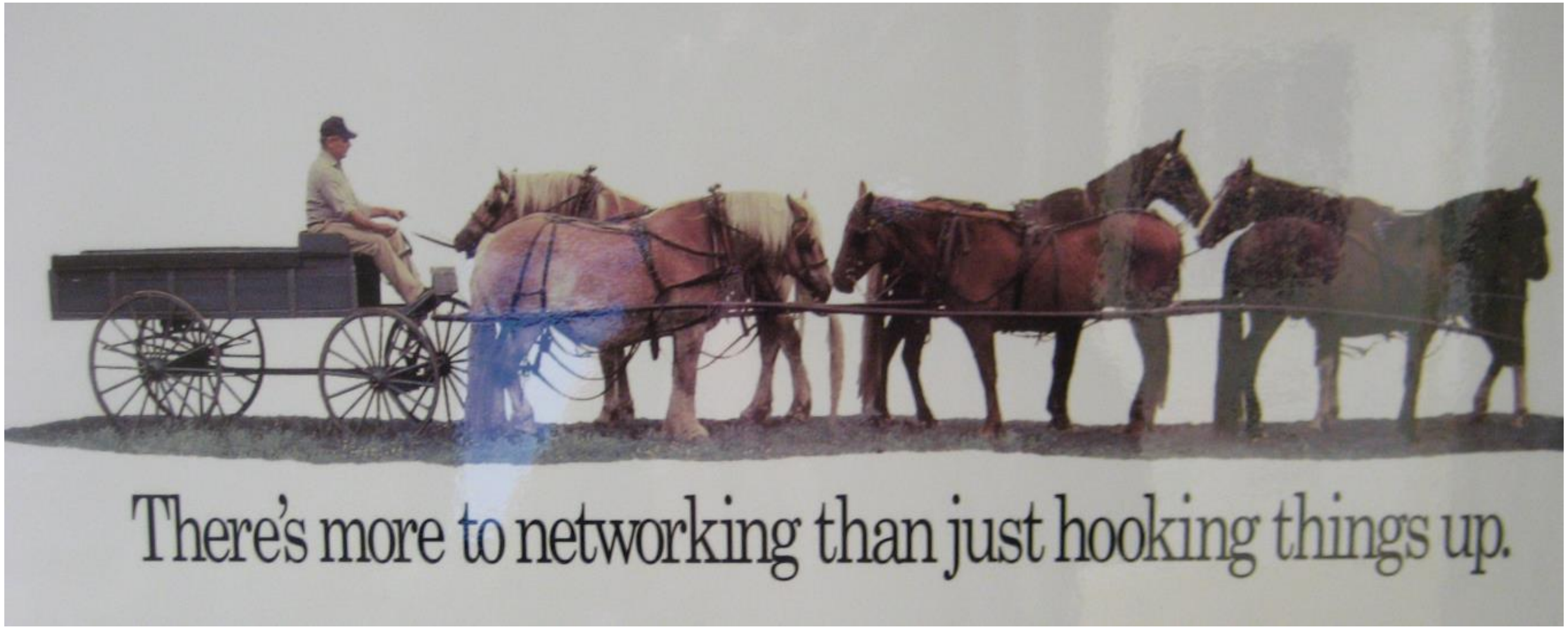
https://blog.knowbe4.com/red-flags-warn-of-social-engineering

Cybersecurity Resources

- CISA "Shields-Up" Program:
  - www.cisa.gov/shields-up
- CISA Known Exploited Vulnerabilities "KEV" Catalog:
  - www.cisa.gov/known-exploited-vulnerabilities-catalog
- NIST Cybersecurity Framework:
  - www.nist.gov/cyberframework/framework
- NIST Incident Response:
  - nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- nmap:
  - nmap.org
- Metasploit:
  - www.metasploit.com
- Shodan:
  - www.shodan.io
- IT Asset Inventory Manager:
  - www.spiceworks.com/
- Monitoring (open-source):
  - www.zabbix.com/
  - www.paessler.com/
- Phishing Training Resource:
  - www.knowbe4.com

Questions & Discussion

Presentation Handout



Wayne M. Pecena CPBE, AMD, ATSC3, DRB, 8VSB, CBNE
Texas A&M University
w-pecena@tamu.edu
wpecena@sbe.org
979.845.5662