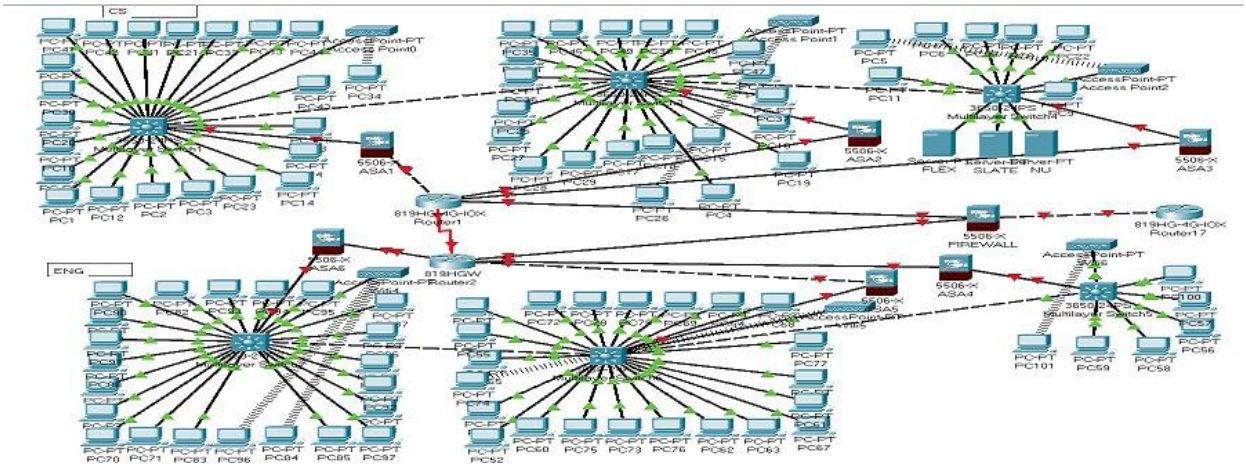
Network Security

Project Scope

- Secure Network Design
- CVE Vulnerabilitites, Exploit and Patches
- Project Hardware and Software Requirements
- Justification
- Conclusion

Secure Network Design



CVE Vulnerabilities,Exploits, and Patches

Without security measures following are the security threats:

1. **Vulnerbility: IBM solidDB 6.5.0.3 - Denial of Service**

Exploit: The solid.exe service listening on port 1315 can be crashed by an external attacker through a malformed type of packet.
The bugged function is located at address 0063dc60 which is called recursively if the packet contains a particular value between the range of values 15001 and 15100 (switch 9).

The effects of the problem can be:
- stack exaustion by using over 14000 of these values so that all the memory of the stack gets consumed by these recursive callings
- NULL pointer due to the usage of only one of these values where an unused pointer (set to zero) is used in a comparison operation
- invalid memory access by using also another type of value after those

- **Patch:** No Fix

2. **Vulnerbility: Trustwave SWG 11.8.0.27 - SSH Unauthorized Access**

Exploit: Trustwave SWG allows remote attackers to send to the SWG product a SSH key that will be used by the SWG product as the SSH key to logon to the device.
This allows unauthenticated user to send a POST request to /sendKey Which will add the supplied ssh key to Trustwave SWG, which we can use it to login to the device.

- **Patch:** Trustwave Secure Web Gateway (SWG) "provides distributed enterprises effective real-time protection against dynamic new malware, strong policy enforcement, and a unique Zero-Malware Guarantee when managed for you by our experts."

3. **Vulnerbility: Python smtplib 2.7.11 / 3.4.4 / 3.5.1 - Man In The Middle StartTLS Stripping**

Exploit: python smtplib does not seem to raise an exception when the remote end (smtp server) is capable of negotiating starttls (as seen in the response to ehlo) but fails to respond with 220 (ok) to an explicit call of `SMTP.starttls()`. This may allow a malicious mitm to perform a starttls stripping attack if the client code does not explicitly check the response code for starttls, which is rarely done as one might expect that it raises an exception when starttls negotiation fails (like when calling starttls on a server that does not support it or when it fails to negotiate tls due to an ssl exception/cipher mismatch/auth fail).

- **Patch:** raise an exception if the server replies with an unexpected return-code to an explicit call for `smtplib.starttls()`.

4. **Vulnerbility: HP System Event Utility - Local Privilege Escalation**

Exploit: The HP System Event service "HPMSGSVC.exe" will load an arbitrary EXE and execute it with SYSTEM integrity.
HPMSGSVC.exe runs a background process that delivers push notifications.

The problem is that HP Message Service will load and execute any arbitrary executable named "Program.exe"
if found in the users c:\ drive.

- **Patch:** Update HP System Event Utility to latest version.

5. **Vulnerbility: Complete Authentication Bypass In Tenda N3 Wireless N150 Routers**

Exploit: The router (AP) is using very poor authentication mechanism . It uses a static cookie to verify the incoming authentication. After careful inspection it was found that the cookie used were same for any number of authentication by the Admin .

Thus the cookie can be easily forged and the admin account could be compromised without supplying the credentials .

- **Patch:** Use a secure authentication mechanism consisting of random , complex Cookies.

Project Hardware and Software Requirements

- 3 TP-Link AC1900 Smart WiFi Router (Archer A8) -High Speed MU-MIMO Wireless Router, Dual Band Router for Wireless Internet, Gigabit, Supports Guest WiFi TP-Link

Connectivity Technology	Wi-Fi, Ethernet
Frequency Band Class	Dual-Band
Data Transfer Rate	1900 Megabits Per Second
Wireless Type	802.11n, 802.11b, 802.11a, 802.11ac, 802.11g
Number of Ports	5
Security Protocol	WEP, WPA2-Enterprise, WPA2-PSK
LAN Port Bandwidth	Gigabit
Voltage	100240 Volts
Antenna Type	Fixed

- 2 Cisco Meraki MX67 Cloud-Managed Security Appliance | MX67-HW | 450 Mbps throughput | Firewall and DHCP Device

Connectivity Technology	Wired
Data Transfer Rate	450 Megabits Per Second
Brand	CISCO DESIGNED
Number of Ports	5
LAN Port Bandwidth	10/100/1000 megabits_per_second
Operating System	Cisco IOS

- 3 BUFFALO LinkStation SoHo 220 2-Bay Desktop 8TB Home Office Private Cloud Data Storage with Hard Drives Included

Free personal cloud for access to from any PC & Mac computer tablet and smartphone

Direct Copy-ready NAS lets you save data directly from USB devices

8 TB – 2 drives included - ships in RAID 1 = 4 TB usable capacity

Bundled with Novastor's novaBACKUP PC backup software (5 licenses)

Optimized performance for 1 - 10 concurrent users

Private Cloud for security & convenience, Qualifies for Buffalo Data Recovery Service

- 4 CISCO DESIGNED Business CBS350-24P-4G Managed Switch | 24 Port GE | PoE | 4x1G SFP | Limited Lifetime Protection (CBS350-24P-4G) (CBS350-24P-4G-NA)

SWITCH PORTS: 24-Port 10/100/1000 + 4 x 1GE SFP
SIMPLE: Intuitive Cisco Business Dashboard or on-box U/I simplifies network operations and automates lifecycle management
POWER-OVER-ETHERNET: 24 PoE ports with 195W total power budget, PoE, PoE+
ENHANCED SECURITY: IP-MAC port biding detects and blocks deliberate network attacks. IPv6 First Hop Security provides unparalleled protection against a vast range of address spoofing and man-in-the-middle attacks on IPv6 networks
INNOVATIVE DESIGN: Elegant and compact design, ideal for installation outside of wiring closet such as retail stores, open plan offices, and classrooms

- 1 NETGEAR 8-Port Fast Ethernet Switch (FS608)

- Vertical option saves space on your desk
- 100 Mbps access/200 Mbps in full-duplex
- It auto-detects speed and duplex
- It is Plug and Play installation, no configuration
- Auto Uplink makes the right connection
- Plug and Play installation, no configuration
- Auto-detects speed and duplex

- Auto Uplink makes the right connection
- 100 Mbps access/200 Mbps in full-duplex
- Vertical option saves space on your desk

- 1 NETGEAR 10-Port Ultra60 PoE Gigabit Ethernet Smart Switch (GS110TUP) - 8 x 1G, Managed, Optional Insight Cloud Management, 4 x PoE+ and 4 x PoE++ @240W, 2 x 1G Uplinks, Desktop, Wall, or Rackmount

4 PoE+ (30W) and 4 Ultra60 PoE++ (60W) ports with a 240W total power budget
1 x 1G copper and 1 x 1G SFP ports
Smart software with easy-to-use interface offers managed control for secure setup, access, and SNMP (NMS 300) management. Includes NETGEAR Insight to remotely manage your networks from anywhere.
Supports desktop, wall or rackmount placement, and includes all the necessary mounting hardware in the box
Lifetime Limited Hardware Warranty, Next Business Day Replacement, and 24/7 chat with a NETGEAR expert
Energy efficient design compliant with IEEE802.3az
Silent operation ideal for noise sensitive environment

- 100 ASUS ExpertCenter D500SA Small Form Factor Desktop PC, Intel Core i5-10400, 12GB DDR4 RAM, 512GB PCIe SSD, Wi-Fi 6, TPM, Windows 10 Professional, Black, D500SA-AB501

- 10th Gen Intel Core i5-10400 Six-Core Processor (12M Cache, up to 4.3 GHz)
- Windows 10 Professional and 1 month trial of Microsoft 365 for new customers - ASUS recommends Windows 10 Pro for business
- 512GB PCIe NVMe M.2 SSD and 12GB 2666 MHz DDR4 RAM (expandable up to 64GB)
- TPM 2.0 Security
- Small Form Factor - weighs 11 lbs
- Seamless connectivity with Gig+ Dual-Band Wi-Fi 6 (802.11ax) and Bluetooth 5.0
- Front I/O: 1x DVD Writer, 1x Headphone jack, 1x 3.5mm combo audio jack, 4x USB 3.2 Type-A (Gen 1), Smartcard Reader, SD Card Reader

- Rear I/O: 1x RJ45 Gigabit LAN, 1x HDMI 1.4, 1x DisplayPort, 1x DVI-D, 2x PS2, 4x USB 2.0 Type-A (Gen1), 3x Audio jacks (*USB Transfer speed may vary. Learn more at ASUS website)
- Expansion slots include 1x PCIe 3.0 x16, 1x PCI, 2x PCIe 3.0 x1, 1x M.2 connector for Wi-Fi (occupied), 2x M.2 connector for storage (1x occupied), 2x DDR4 U-DIMM slot (2x occupied)
- Keyboard and mouse included

- Amazon Basics Snagless RJ45 Cat-6 Ethernet Patch Internet Cable - 7-Foot, White, 5-Pack

  Set of five 7 foot Cat6 ethernet cables for connecting networked devices such as computers, printers, routers, and more
  Performs at a bandwidth up to 250MHz
  Low signal loss with a transmission speed up to 10 gigabit per second and 100 meter distance
  Snagless plug design helps prevent damage when plugging/unplugging cable
  Gold-plated contacts and bare copper conductors improve signal integrity and resist corrosion
  Featuring flexible protective PVC jackets, 5.0mm cable diameter, and 26 AWG conductor gauge

- Tripp Lite T1 Shielded RJ48C Cross-over Cable (RJ45 M/M), 7-ft. (N266-007)

  ANSI certified T1 cable, Levels 1, 1A, and 1C
  Complies with ANSI T1.403 Carrier-to-Customer Installation-DS1 Metallic Interface
  Cross-over T1 wiring configuration
  Available in 3ft, 5ft, 7ft, and 10ft stocked lengths
  Custom length cables available
  NEC (UL) Type CMR
  Available also in Straight-through wiring configurations
  22AWG Solid Tinned Copper

- Cable Sourcing - 100ft (30m) CAT5e Cable, External (Outdoor use) & Internal, 100% Solid Copper, Ethernet, CCTV, 10/100/1000mb, RJ45 Plugs, Networking & Patch Cable

Compatible Devices	Laptop, TV, PC, Router, Modem
Brand	Cable Sourcing
Cable Type	Ethernet
Color	Black
Connector Type	RJ45

Justification

CIA - Confidentiality, Integrity and Availability.

The CIA Triad is actually a security model that has been developed to help people think about various parts of IT security.

Confidentiality

Protecting confidentiality is dependent on being able to define and enforce certain access levels for information. In some cases, doing this involves separating information into various collections that are organized by who needs access to the information and how sensitive that information actually is - i.e. the amount of damage suffered if the confidentiality was breached.

Integrity

This is an essential component of the CIA Triad and designed to protect data from deletion or modification from any unauthorized party, and it ensures that when an authorized person makes a change that should not have been made the damage can be reversed.

Availability

Authentication mechanisms, access channels and systems all have to work properly for the information they protect and ensure it's available when it is needed.

Here in our network design all three aspect is fullfilled, By assigning a role-based access control for each department that if a person no more of in that role then he/she cannot access it, servers are there for data backup which allow data to be restored if changes are made inadvertently or rescinded later. Data flow on network either wired or wireless both are secure by software and hardware configuration that only they can access their own data by blocking others to access it also web-based filtering is in place that only those website will be accessble which were related to their business. Don’t allow unwanted traffic with check and balance.

Conclusion

In above network design we have two buildings one is CS and second is ENG.

Both have 50 workstations, total 100 combine. There combine connection is connected with firewall and then router.

In buildings There is one main router which is connected with three different firewalls behind which three different swithes are there and first two are identical switches in term of devices connected and third router is different in number of devices connected .

CS and ENG building are connected through subnetting and both building have same network except one thing that CS building have server but ENG not.

We have done web-base filtering via extended ACL(Access Control List) in Router so that specific website cannot be accessible, Role Based Access Control (RBAC) Configuration in Router Switch Parser View.

Reference

www.amazon.com
https://cve.mitre.org/data/refs/refmap/source-EXPLOIT-DB.html
https://cve.mitre.org/data/downloads/index.html
https://www.exploit-db.com/