

Cybersecurity Scenario

Objective: Is to protect the organizations data from internal and external threats

Context

Buffalo Network is a small medium IT company specializing in software development, Networking and other IT services. This team is tasked to provide and safeguard sensitive data, including client information, proprietary code, and financial records, against internal and external threats. This team already have some measures that are implemented to safeguard this information. The implemented measures include access control, intrusion detection, data encryption etc.

Relevance to learning objective

This scenario is relevant as it provides hands on experience with real world cybersecurity challenges, It aligns with the learning objective of understanding cybersecurity measures, incident response, data protection, and employee training. We will gain practical knowledge of implementing security protocols, conducting security audits, monitoring network traffic, and developing comprehensive response plan for data breaches.

Key Challenges

- The key challenged may be Identifying and Mitigating Vulnerabilities, conducting security audits to identify vulnerabilities requires a plenty of time while taking into consideration priorities.
- Monitoring network traffic, the challenge may be continuously monitoring network traffic for suspicious activity and potential breaches.
- Employee training and awareness, ensuring all employees are aware of cybersecurity best practices and their roles.

Task No 1

1. Conducting a security audit and identifying vulnerabilities.

Date of audit: 23/01/2024

Conducted by: Buffalo Networks

Overview of Recent security audit results

Scope of Audit

- Network Infrastructure
- Webserver
- Database server
- Desktop and multi user systems
- Web applications
- Data storage systems
- Access controls and authentication mechanisms

Audit Methodology

Vulnerability tools used to scan the network system.

Nmap report

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets, with the following details visible:

No.	Time	Source	Destination	Protocol	Length	Info
16992	146.108703	4.154.131.236	192.168.0.113	TCP	1466	443 → 49759 [ACK] Seq=48439 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
16993	146.108703	4.154.131.236	192.168.0.113	TCP	1466	443 → 49759 [ACK] Seq=49851 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
16994	146.108703	4.154.131.236	192.168.0.113	TCP	1466	443 → 49759 [ACK] Seq=51263 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
16995	146.108703	4.154.131.236	192.168.0.113	TLSv1.2	1466	Application Data
16996	146.108817	192.168.0.113	4.154.131.236	TCP	54	49759 → 443 [ACK] Seq=14200 Ack=54087 Win=131072 Len=0
16997	146.306222	192.168.0.113	192.178.54.42	QUIC	71	Protected Payload (KP0)
16998	146.310694	192.178.54.42	192.168.0.113	QUIC	74	Protected Payload (KP0)
16999	146.373792	192.168.100.23	239.255.255.250	SSDP	308	NOTIFY * HTTP/1.1
17000	146.414330	4.154.131.236	192.168.0.113	TCP	1466	443 → 49759 [ACK] Seq=54087 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
17001	146.414330	4.154.131.236	192.168.0.113	TCP	263	[TCP Previous segment not captured] 443 → 49759 [PSH, ACK] Seq=66795 Ack=14200 Win=4194816 Len=209 [TCP segment of a reassembled PDU]
17002	146.414521	192.168.0.113	4.154.131.236	TCP	66	49759 → 443 [ACK] Seq=14200 Ack=55499 Win=131072 Len=0 SLE=66795 SRE=67004
17003	146.415140	4.154.131.236	192.168.0.113	TCP	1466	[TCP Out-Of-Order] 443 → 49759 [ACK] Seq=55499 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
17004	146.415140	4.154.131.236	192.168.0.113	TCP	1466	[TCP Out-Of-Order] 443 → 49759 [ACK] Seq=56911 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
17005	146.415140	4.154.131.236	192.168.0.113	TCP	1466	[TCP Out-Of-Order] 443 → 49759 [ACK] Seq=58323 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
17006	146.415140	4.154.131.236	192.168.0.113	TCP	1466	[TCP Out-Of-Order] 443 → 49759 [ACK] Seq=59735 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
17007	146.415140	4.154.131.236	192.168.0.113	TCP	1466	[TCP Out-Of-Order] 443 → 49759 [ACK] Seq=61147 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
17008	146.415278	192.168.0.113	4.154.131.236	TCP	66	49759 → 443 [ACK] Seq=14200 Ack=56911 Win=131072 Len=0 SLE=66795 SRE=67004
17009	146.415355	192.168.0.113	4.154.131.236	TCP	66	49759 → 443 [ACK] Seq=14200 Ack=58323 Win=131072 Len=0 SLE=66795 SRE=67004
17010	146.415392	192.168.0.113	4.154.131.236	TCP	66	49759 → 443 [ACK] Seq=14200 Ack=59735 Win=131072 Len=0 SLE=66795 SRE=67004
17011	146.415427	192.168.0.113	4.154.131.236	TCP	66	49759 → 443 [ACK] Seq=14200 Ack=61147 Win=131072 Len=0 SLE=66795 SRE=67004
17012	146.415463	192.168.0.113	4.154.131.236	TCP	66	49759 → 443 [ACK] Seq=14200 Ack=62559 Win=131072 Len=0 SLE=66795 SRE=67004
17013	146.415945	4.154.131.236	192.168.0.113	TCP	1466	[TCP Out-Of-Order] 443 → 49759 [ACK] Seq=62559 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
17014	146.415945	4.154.131.236	192.168.0.113	TCP	1466	[TCP Out-Of-Order] 443 → 49759 [ACK] Seq=63971 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
17015	146.415945	4.154.131.236	192.168.0.113	TCP	1466	[TCP Out-Of-Order] 443 → 49759 [ACK] Seq=65383 Ack=14200 Win=4194816 Len=1412 [TCP segment of a reassembled PDU]
17016	146.416053	192.168.0.113	4.154.131.236	TCP	66	49759 → 443 [ACK] Seq=14200 Ack=63971 Win=131072 Len=0 SLE=66795 SRE=67004
17017	146.416122	192.168.0.113	4.154.131.236	TCP	66	49759 → 443 [ACK] Seq=14200 Ack=65383 Win=131072 Len=0 SLE=66795 SRE=67004
17018	146.416234	192.168.0.113	4.154.131.236	TCP	54	49759 → 443 [ACK] Seq=14200 Ack=67004 Win=131072 Len=0

The bottom pane shows the packet details for the selected packet (No. 17003). The details are as follows:

> Frame 17003: 303 bytes on wire (2424 bits), 303 bytes captured (2424 bits) on interface Device0
> Ethernet II, Src: AzureWaveTec_96:e1:5d (78:66:55:96:e1:5d), Dst: TplinkTechno_b6:58:96 (70:44:17:00:00:00)
> Internet Protocol Version 4, Src: 192.168.0.113, Dst: 199.232.210.172
> Transmission Control Protocol, Src Port: 49760, Dst Port: 80, Seq: 499, Ack: 15337, Len: 249
> Hypertext Transfer Protocol

The packet bytes pane shows the raw data of the packet, including the TLS handshake and application data segments.

Identified vulnerabilities

Identify weaknesses in the systems, processes, or practices that could be exploited by threats.

	Threats	Vulnerabilities	Priority
Webserver	SQL injection Cross-Site Scripting Denial of Service	Outdated software Misconfigured Services	2
Database Server	Unauthorized Access Data Breaches Malware infections	Weak password Unpatched security flaws	1
Employee workstations	Malware infections Phishing attacks	Lack of antivirus software Outdated operating systems	3
WIFI Networks	Eavesdropping Rogue access points	Weak encryption Default credentials	4

2. Implementing security measures for Desktop and Multi- User systems

Date of Review: 10/01/2024

Conducted by: Buffalo Networks

Scope of review:

Desktop workstations

Multi-user systems (shared systems, servers, etc)

Software and application used across these systems

Current Security Measures

User access controls- Role based access controls are implemented to ensure users have minimum necessary permissions. They are managed through Active Directory and group policies

Data Encryption- Sensitive data on desktops and multi user systems is encrypted. Bitlocker and file vault are used for both windows and macOS systems.

Endpoint Detection and Response(EDR)- EDR solutions are deployed to monitor and respond to security incidents on endpoints.

Proposed New Measures

(a) Antivirus and anti-malware software

- All desktops and multi user systems must have antivirus and anti-malware software installed.
- Example of anti-virus and anti-malware software: TotalAV, Bitdefender, Intego, McAfee.
- With these regular scans and real time protection are always active.

(b) Operating System Updates and Patching

- All systems must be configured to receive automatic updates for operating systems
- They must be managed through a centralized IT management Tools.
- These are effective but some may encounter certain delays due to user interventions and configuration issues.

(c) Firewall protection

- Built in firewalls must be enabled on all systems to prevent unauthorized access
- They must be configured through group policies and local system settings
- Effective in blocking unauthorized access and correct configurations must be ensured

Deployment timelines and responsibilities to be assigned:

3. Monitor Network Traffic for Suspicious Activity

Current Network Monitoring practices and tools that were reviewed

Zenmap

Scan Tools Profile Help

Target: 192.168.0.1/24 Profile: Quick traceroute

Command: nmap -sn --traceroute 192.168.0.1/24

Hosts		Services		Nmap Output		Ports / Hosts		Topology		Host Details		Scans	
OS	Host	Port	Protocol	State	Service	Version							
	192.168.0.1	22	tcp	open	ssh	Dropbear sshd 2012.55 (protocol 2.0)							
	192.168.0.100	23	tcp	open	telnet	BusyBox telnetd 1.14.0 or later (TP-LINK ADSL2+ router telnetd)							
	192.168.0.104	80	tcp	open	http	TP-LINK TD-W8968 http admin							
	192.168.0.113	1900	tcp	open	upnp	Portable SDK for UPnP devices 1.6.19 (Linux 2.6.36; UPnP 1.0)							
	192.168.0.118												

2nd

***Wi-Fi**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
35	0.215827	192.168.0.113	23.50.192.251	TLSv1.3	423	Application Data
36	0.216059	192.168.0.113	23.50.192.251	TCP	1466	61428 → 443 [ACK] Seq=1043 Ack=271 Win=66048 Len=1412 [TCP segment of a reassembled PDU]
37	0.216301	192.168.0.113	23.50.192.251	TLSv1.3	438	Application Data
38	0.253533	192.168.100.23	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
39	0.256983	192.168.100.23	239.255.255.250	SSDP	364	NOTIFY * HTTP/1.1
40	0.380553	23.50.192.251	192.168.0.113	TCP	54	[TCP Previous segment not captured] 443 → 61428 [FIN, ACK] Seq=1325 Ack=2839 Win=64128 Len=0
41	0.380978	23.50.192.251	192.168.0.113	TCP	54	443 → 61428 [ACK] Seq=271 Ack=674 Win=64128 Len=0
42	0.380978	23.50.192.251	192.168.0.113	TCP	54	443 → 61428 [ACK] Seq=271 Ack=1043 Win=64128 Len=0
43	0.380978	23.50.192.251	192.168.0.113	TCP	341	[TCP Out-Of-Order] 443 → 61428 [PSH, ACK] Seq=271 Ack=1043 Win=64128 Len=287
44	0.380978	23.50.192.251	192.168.0.113	TCP	66	443 → 61428 [ACK] Seq=558 Ack=1043 Win=64128 Len=0 SLE=2455 SRE=2839
45	0.380978	23.50.192.251	192.168.0.113	TCP	54	443 → 61428 [ACK] Seq=558 Ack=2839 Win=64128 Len=0
46	0.380978	23.50.192.251	192.168.0.113	TCP	797	[TCP Out-Of-Order] 443 → 61428 [PSH, ACK] Seq=558 Ack=2839 Win=64128 Len=743
47	0.380978	23.50.192.251	192.168.0.113	TCP	78	[TCP Out-Of-Order] 443 → 61428 [PSH, ACK] Seq=1301 Ack=2839 Win=64128 Len=24
48	0.380978	23.50.192.251	192.168.0.113	TCP	54	[TCP Retransmission] 443 → 61428 [FIN, ACK] Seq=1325 Ack=2839 Win=64128 Len=0
49	0.395424	192.168.0.113	23.50.192.251	TCP	54	[TCP Dup ACK 34#1] 61428 → 443 [ACK] Seq=2839 Ack=271 Win=66048 Len=0
50	0.395600	192.168.0.113	23.50.192.251	TCP	54	61428 → 443 [ACK] Seq=2839 Ack=1326 Win=65024 Len=0
51	0.396327	192.168.0.113	23.50.192.251	TCP	54	[TCP Dup ACK 50#1] 61428 → 443 [ACK] Seq=2839 Ack=1326 Win=65024 Len=0
52	0.401736	192.168.0.113	23.50.192.251	TLSv1.3	78	Application Data
53	0.401931	192.168.0.113	23.50.192.251	TCP	54	61428 → 443 [FIN, ACK] Seq=2863 Ack=1326 Win=65024 Len=0
54	0.424126	23.50.192.251	192.168.0.113	TCP	54	443 → 61428 [ACK] Seq=1326 Ack=2863 Win=64128 Len=0
55	0.424126	23.50.192.251	192.168.0.113	TCP	54	443 → 61428 [RST] Seq=1326 Win=0 Len=0
56	0.439805	192.168.0.113	23.50.192.251	TCP	66	61429 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
57	0.455241	192.168.100.23	239.255.255.250	SSDP	372	NOTIFY * HTTP/1.1
58	0.463278	23.50.192.251	192.168.0.113	TCP	66	443 → 61429 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128
59	0.466822	192.168.0.113	23.50.192.251	TCP	54	61429 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
60	0.469157	192.168.0.113	23.50.192.251	TLSv1.3	647	Client Hello (SNI=go.microsoft.com)

> Frame 56: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF...
> Ethernet II, Src: AzureWaveTec_96:e1:5d (70:66:55:96:e1:5d), Dst: TplinkTechno_b6:58:96 (70:44:17:b6:58:96)
> Internet Protocol Version 4, Src: 192.168.0.113, Dst: 23.50.192.251
> Transmission Control Protocol, Src Port: 61429, Dst Port: 443, Seq: 0, Len: 0

0000 70 4f 57 b6 58 96 70 66 55 96 e1 5d 08 00 45 00 pOW-X [f l . . .] : E
0010 00 34 26 bc 40 00 7e 06 3c c1 c0 a8 00 71 17 32 -48 @ . . . < . . . q : 2
0020 c0 fb ef f5 01 bb 41 ef 7b 20 00 00 00 00 02 A {
0030 fa f0 2c 18 00 00 02 04 05 b4 01 03 03 08 01 01
0040 04 02

wireshark_Wi-FiC8B2P2.pcapng Packets: 17097 · Displayed: 17097 (100.0%) · Dropped: 0 (0.0%) Profile: Default

✓ Port 22 (SSH using Dropbear sshd 2012)

Risks

Brute Force Attacks- Attackers may try to guess login credentials through repeated attempts.

Exploits in Dropbear SSHD 2012- Older versions of Dropbear may have known vulnerabilities that could be exploited.

Weak Authentication Methods- Using password-based authentication instead of key-based authentication increases risk.

Strategies for improving monitoring

Use Strong Authentication- Implement key-based authentication instead of password-based.

Update and Patch Software- Ensure Dropbear SSHD is updated to the latest version.

Limit Access- Use firewalls to restrict access to port 22 to known IP addresses.

Enable Intrusion Detection- Monitor for unusual login attempts and implement rate limiting or fail2ban.

✓ Port 23 (Telnet on TP-Link ADSL2)

Risks

Unencrypted Communication- Telnet transmits data, including credentials, in plaintext, making it susceptible to eavesdropping.

Legacy Protocol- Telnet is considered outdated and insecure compared to modern alternatives like SSH.

Potential Router Exploits- Routers may have vulnerabilities that can be exploited via Telnet.

Strategies for improving monitoring

Disable Telnet- If possible, disable Telnet and use SSH instead for secure remote management.

Use Strong Authentication- Ensure strong, unique passwords are used.

Update Router Firmware- Keep the router firmware up-to-date to mitigate known vulnerabilities.

Restrict Access- Use a firewall to restrict access to port 23 to known, trusted IP addresses.

✓ **Port 80 (HTTP for Admin Access)**

Risks

Unencrypted Communication- HTTP traffic is unencrypted, making it susceptible to interception and man-in-the-middle attacks.

Web Application Vulnerabilities- The admin interface may have vulnerabilities such as cross-site scripting (XSS), SQL injection, etc.

Default Credentials- Admin interfaces often have default credentials that may not have been changed.

Strategies for improving monitoring

Use HTTPS- Implement HTTPS to encrypt communication.

Secure Admin Interface- Ensure the admin interface is not exposed to the internet or is accessible only from a secure network.

Change Default Credentials- Use strong, unique credentials for the admin interface.

Regular Updates and Patching- Keep the web server and any associated software updated.

Implement Web Application Firewall (WAF)- Use a WAF to protect against common web vulnerabilities.

✓ **Port 1900 (UPnP Services on Portable SDK)**

Risks

UPnP Exploits- UPnP has known vulnerabilities that can be exploited to gain unauthorized access or cause denial of service.

Exposure to Internal Network- UPnP can expose internal devices and services to potential attackers if not properly secured.

Strategies for improving monitoring

Disable UPnP- If UPnP is not required, disable it on the device.

Restrict Access- Use firewall rules to limit access to port 1900 from trusted internal networks only.

Update Firmware- Ensure that the device firmware is up-to-date to mitigate known UPnP vulnerabilities.

Monitor Traffic- Regularly monitor network traffic for unusual activities related to UPnP services.

4. Develop a Response Plan for the Potential Data Breaches

Date of Review: 15/01/ 2024

Existing Data Breach Response Plan

Purpose: The data breach response plan aims to provide a structured and effective approach to handling data breaches, minimizing damage, and ensuring a swift recovery. It outlines the steps to identify, respond to, mitigate, and report data breaches.

Key Components of the Existing Plan

1. Preparation:

- **Incident Response Team (IRT):** A dedicated team responsible for handling data breaches, comprising members from IT, legal, public relations, and management.
- **Training and Drills:** Regular training sessions and simulated breach scenarios to prepare the IRT and relevant staff for real incidents.
- **Contact List:** A comprehensive list of internal and external contacts, including IRT members, legal advisors, law enforcement, and third-party security experts.

2. Identification:

- **Monitoring and Detection:** Continuous monitoring of systems and networks using security information and event management (SIEM) tools and intrusion detection systems (IDS).
- **Reporting Mechanism:** Clear procedures for employees to report suspected data breaches promptly.

3. Containment:

- **Immediate Actions:** Steps to contain the breach, such as isolating affected systems, revoking access, and stopping data exfiltration.
- **Short-Term Containment:** Temporary fixes to prevent further damage while a thorough investigation is conducted.
- **Long-Term Containment:** Implementation of permanent solutions to address vulnerabilities and prevent recurrence.

4. Eradication:

- **Root Cause Analysis:** Identifying the cause of the breach and removing all traces of the threat from the systems.
- **System Cleaning:** Ensuring affected systems are clean and secure before resuming normal operations.

5. **Recovery:**

- **Restoration:** Restoring systems and data from backups, ensuring they are free from vulnerabilities.
- **Monitoring:** Increased monitoring of affected systems to detect any signs of residual or new threats.

6. **Communication:**

- **Internal Communication:** Informing relevant internal stakeholders, including management and employees, about the breach and response actions.
- **External Communication:** Notifying affected parties, regulators, and the public as required by law and company policy.
- **Media Management:** Coordinating with public relations to manage media inquiries and protect the company's reputation.

7. **Post-Incident Review:**

- **Debriefing:** Conducting a thorough review of the incident, response actions, and outcomes.
- **Lessons Learned:** Identifying strengths and weaknesses in the response plan and making necessary adjustments.
- **Documentation:** Documenting the breach, response actions, and lessons learned for future reference and compliance purposes.

2. **Updates and improvements to the response plan.**

(a) **Enhanced Monitoring and Detection:**

- Implement advanced SIEM and IDS tools to improve breach detection capabilities.
- Regularly update and fine-tune monitoring tools to adapt to evolving threats.

(b) **Regular Training and Simulations:**

- Increase the frequency of training sessions and simulated breach scenarios for the IRT and relevant staff.
- Include cross-departmental drills to ensure comprehensive preparedness.

© **Clear Reporting Mechanism:**

- Simplify and streamline the reporting process for suspected breaches.
- Ensure all employees are aware of the reporting procedures.

(c) **Improved Communication Protocols:**

- Develop clear guidelines for internal and external communication during a breach.
- Regularly update the contact list and communication templates.

(d) **Post-Incident Review Enhancements:**

- Establish a more structured debriefing process to ensure thorough analysis and documentation of each incident.
- Implement a continuous improvement process based on lessons learned.

Assigning roles and responsibilities

Person	Responsibility	Task

5. Educating Staff on best Practices for Data security

Date of the awareness: 24/01/2024

Reviewed the Effectiveness of Current Training Programs

Summary: The effectiveness of current training programs was evaluated based on feedback from employees, the number of security incidents reported, and the overall improvement in data security practices.

Findings

Positive Outcomes: Increased awareness of phishing threats and improved password hygiene among staff.

Areas for Improvement: Continued occurrences of minor security breaches due to human error, indicating a need for more comprehensive training.

New Training Initiatives Introduced

Initiative 1: Interactive Workshops

- **Description:** Monthly interactive workshops where employees engage in hands-on activities related to data security, such as recognizing phishing emails, secure password creation, and understanding the importance of encryption.
- **Benefits:** Enhances practical understanding and application of security practices.

Initiative 2: E-Learning Modules

- **Description:** Introduction of e-learning modules covering various aspects of data security, including safe internet browsing, handling sensitive information, and identifying social engineering attacks. These modules will be mandatory for all employees and include quizzes to reinforce learning.
- **Benefits:** Allows employees to learn at their own pace and ensures consistent training across the organization.

Scheduled Regular Training and Awareness Sessions

Frequency: Quarterly training and awareness sessions to keep all staff updated on the latest data security practices and emerging threats.

Next Training Session:

- **Date:** 23/07/2024
- **Agenda:**
 - Overview of recent security incidents and lessons learned.
 - Introduction to new data security tools and practices.
 - Interactive workshop on recognizing and responding to phishing attempts.
 - Q&A session to address any concerns or questions from staff.