LAB 09 – Networking II

By :- Faraz Ahmed

1. MEMO

To: CEO David Murray

From: Faraz Ahmed, Security Engineer

Date: October 30th, 2024

Subject: Proposal for two new cybersecurity measures for UBNetDef Wiki

Dear CEO Murray,

As part of our security team which helps to secure UBNetDef's data and integrity of our UBNetDef Wiki which is our personal website, I am submitting two essential proposals for consideration and implementation in the upcoming budget evaluation for the UBNetDEf Wiki to enhance our defence mechanisms against potential threats and to detect threats and response. These proposals leverage honeypots, honeynets and intrusion detection/prevention systems to improve our overall security system and provide a robust protection against different types of threats. This will help by making Wiki website always functional to use (always available) and provides protection to the data inside that website.

Table of Contents

2. Executive Summary

a. Proposal 1- Use or Implementation of Honeypots and Honeynets

UBNetDef finds that implementing or deploying honeypots and honeynets will significantly enhance our overall security capabilities making it more robust system to break and intrude. These are a type of decoy systems will not only help to divert initial threats but also provide time to the security teams to correctly study and analyse the pattern of attack and gather valuable information to mitigate that issue. So, honeypots and honeynets will provide an extra and effective layer of security by diverting attackers away from our sensitive assets and data. It will lure all attackers away from our actual network assets, providing us better insights and intelligence into attack techniques and patterns to mitigate it. By analysing the attacks, we can develop better defence strategies and improve our threat response protocols. The estimated cost for this implementation is approximately $20,000 which includes hardware, software and some setup costs.

b. Proposal 2- Deployment of Intrusion Detection and Prevention Systems (IDPS)

UBNetDef finds that implementing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) will improve our ability to monitor and logging network traffic for some suspicious activities and anomalies. This system will automatically alert administrators by detecting certain unusual and suspicious activities such as malicious logins or network anomalies and automatically take action to block potential threats or can also mitigate them. So, the IDPS basically will get the basic baselines of that system and then it compares the threat network activity with those baselines, IDPS will help to prevent significant breaches in that network system. The projected cost for this proposal is around $30,000 covering all of the official software licenses, hardware and implementation services.

3. Technical Findings

a. Proposal 1- Honeypots and Honeynets

- Findings: Research shows that organizations using honeypot have seen a 40% decrease in successful intrusions in the system. Implementing honeypots and honeynets into the system serves as a proactive measure against cyber threats. These decoys attract malicious actors and thus allowing our security team to study and analyse their behaviours without risking our actual data and assets in that system. Honeypots can give you reliable information about how threats are evolving and pattern. They deliver information about attack vectors, exploit, and malware - and in the case of email traps about spammers and phishing attacks. Hackers continually upgrade their intrusion techniques with time because of which, a cybersecurity honeypot helps to spot newly emerging threats and intrusions. A good use of honeypots helps to eradicate blind spots and also a great training tools for technical security staff.
- Consequences of Non-Implementation: Failure to implement this measure could result in all of the risks of being unprepared for upcoming threats, which could lead to certain data breaches and significant financial losses and also to suffer missed opportunities to gather intelligence, potentially exposing UBNetDef to sophisticated attacks that could disrupt operations or compromise sensitive information.
- Cost Methodology: Costs were estimated based on various hardware expenses such as servers and virtual machines and also licenses of software such as Anti-malware tools and security monitoring tools. And also researching about different historical reports from venders on these types of attacks.

b. Proposal 2- Intrusion Detection and Prevention Systems (IDPS)

- Findings: An IDPS is crucial for maintaining the security and integrity of our network. By continuously monitoring for malicious and suspicious activities and automating responding to the detected threats, we can mitigate the risk and reduce the breaches. So, implementing IDS/IPS can reduce the time taken to detect breaches drastically and so can help the system security team to study and analyse the threat on time and try to find proper method to mitigate the threat before it hinders the assists and integrity of the system.
- Consequences of Non-Implementation: Failure to adopt IDS/IPS could leave UBNetDef vulnerable to certain malicious attacks and ransomware attacks similar to incidents experienced in major Target Data Breach which happened in 2013 where Target's IDPS system detected some malicious activity on its network after hackers gained access via third-party vendor. However, these alerts were ignored which the attackers took advantage of and were able to install malware on the company's sensitive systems, compromising 40 million credit and debit card accounts. That's why the absence of such a system could leave us vulnerable to attacks that can go undetected, leading to financial losses and also some reputational damage.
- Cost Methodology: Cost estimates were derived from market analysis, discussing with venders and licensing fees for IDPS software and the necessary hardware to support its implementation.

4. References

a. Network Security Best Practices
Netwrix. (n.d.). *Network security best practices.* Retrieved from https://www.netwrix.com/network_security_best_practices.html

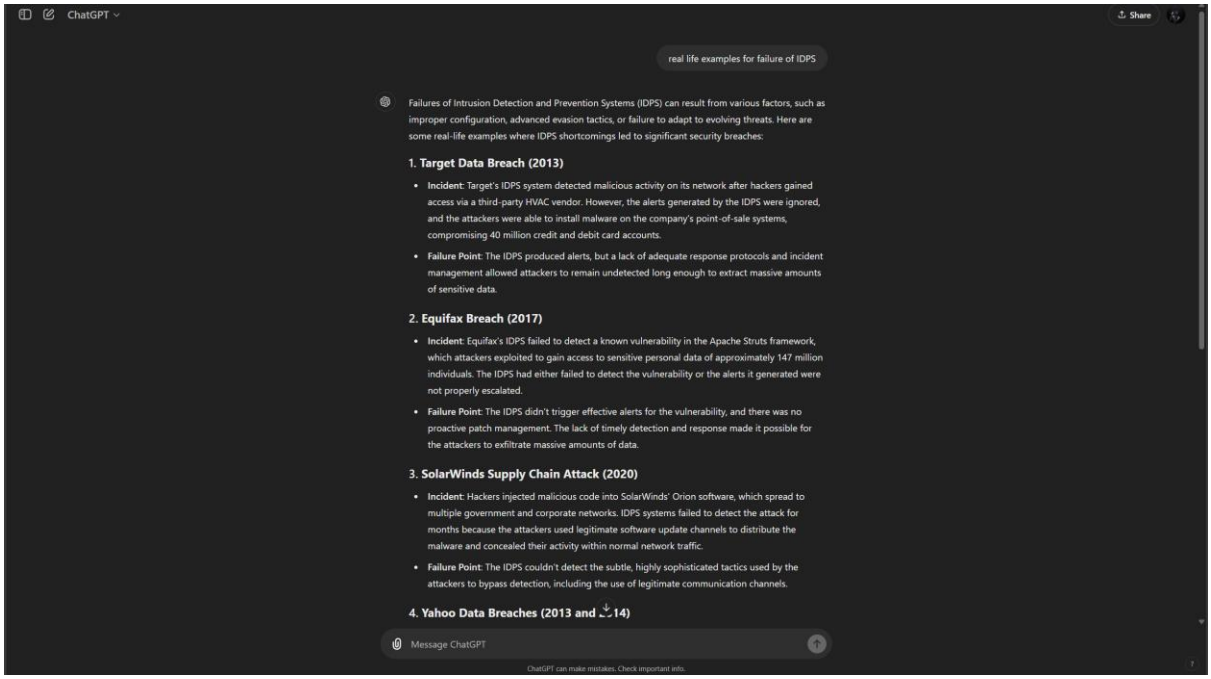
b. What is a honeypot? How honeypots help security
Kaspersky. (n.d.). *What is a honeypot? Definition and meaning.* Retrieved from https://usa.kaspersky.com/resource-center/threats/what-is-a-honeypot

c. What is a honeypot? How it protects against cyber attacks
TechTarget. (n.d.). *Honeypot.* Retrieved from https://www.techtarget.com/searchsecurity/definition/honey-pot

d. What Are Intrusion Detection and Prevention Systems?
Kiteworks. (n.d.). *What are intrusion detection and prevention systems?* Retrieved from https://www.kiteworks.com/risk-compliance-glossary/intrusion-detection-prevention-systems/

e. What is an Intrusion Detection and Prevention System? | **Swimlane**
Swimlane. (n.d.). *The power of IDPS in cybersecurity.* Retrieved from https://swimlane.com/blog/power-of-idps-in-cybersecurity/

f.


ChatGPT
Share
real life examples for failure of IDPS
Failures of Intrusion Detection and Prevention Systems (IDPS) can result from various factors, such as improper configuration, advanced evasion tactics, or failure to adapt to evolving threats. Here are some real-life examples where IDPS shortcomings led to significant security breaches:
1. Target Data Breach (2013)
Incident: Target's IDPS system detected malicious activity on its network after hackers gained access via a third-party HVAC vendor. However, the alerts generated by the IDPS were ignored, and the attackers were able to install malware on the company's point-of-sale systems, compromising 40 million credit and debit card accounts.
Failure Point: The IDPS produced alerts, but a lack of adequate response protocols and incident management allowed attackers to remain undetected long enough to extract massive amounts of sensitive data.
2. Equifax Breach (2017)
Incident: Equifax's IDPS failed to detect a known vulnerability in the Apache Struts framework, which attackers exploited to gain access to sensitive personal data of approximately 147 million individuals. The IDPS had either failed to detect the vulnerability or the alerts it generated were not properly escalated.
Failure Point: The IDPS didn't trigger effective alerts for the vulnerability, and there was no proactive patch management. The lack of timely detection and response made it possible for the attackers to exfiltrate massive amounts of data.
3. SolarWinds Supply Chain Attack (2020)
Incident: Hackers injected malicious code into SolarWinds' Orion software, which spread to multiple government and corporate networks. IDPS systems failed to detect the attack for months because the attackers used legitimate software update channels to distribute the malware and concealed their activity within normal network traffic.
Failure Point: The IDPS couldn't detect the subtle, highly sophisticated tactics used by the attackers to bypass detection, including the use of legitimate communication channels.
4. Yahoo Data Breaches (2013 and 2014)
Message ChatGPT
ChatGPT can make mistakes. Check important info.

5. Appendix A: Hardware/Software Inventory

a. 10.42.32.0/24 Network Segment

Device label	MAC Address	IP Address (CIDR)	Default Gateway	DNS Server	Operating System	Software Providing Services
Win10Client	00-50-56-86-85-12	10.42.32.12/24	10.42.32.1	10.42.32.98	Windows 10	Windows Services
UbuntuClient	00:50:56:86:e2:74	10.42.32.7/24	10.42.32.1	8.8.8.8	Linux	Linux Services
IISServer	00-50-56-86-5F-F8	10.42.32.90/24	10.42.32.1	10.42.32.98	Windows Server	IIS Web Services
ADServer	00-50-56-86-0E-94	10.42.32.98/24	10.42.32.1	8.8.8.8	Windows Server	Active Directory Services
AdminNet Interface		10.42.32.1/24	10.42.32.1	-	-	-

b. 10.43.32.0/24 Network Segment

Device label	MAC Address	IP Address (CIDR)	Default Gateway	DNS Server	Operating System	Software Providing Services
UbuntuWebServer	00:50:56:86:fc:53	10.43.32.7/24	10.43.32.1	8.8.8.8	Linux	Apache Web Server
RockyDBServer	00:50:56:86:4e:7b	10.43.32.30/24	10.43.32.1	8.8.8.8	Linux	Database Services
ServerNet Interface		10.43.32.1/24	10.43.32.1	-	-	-

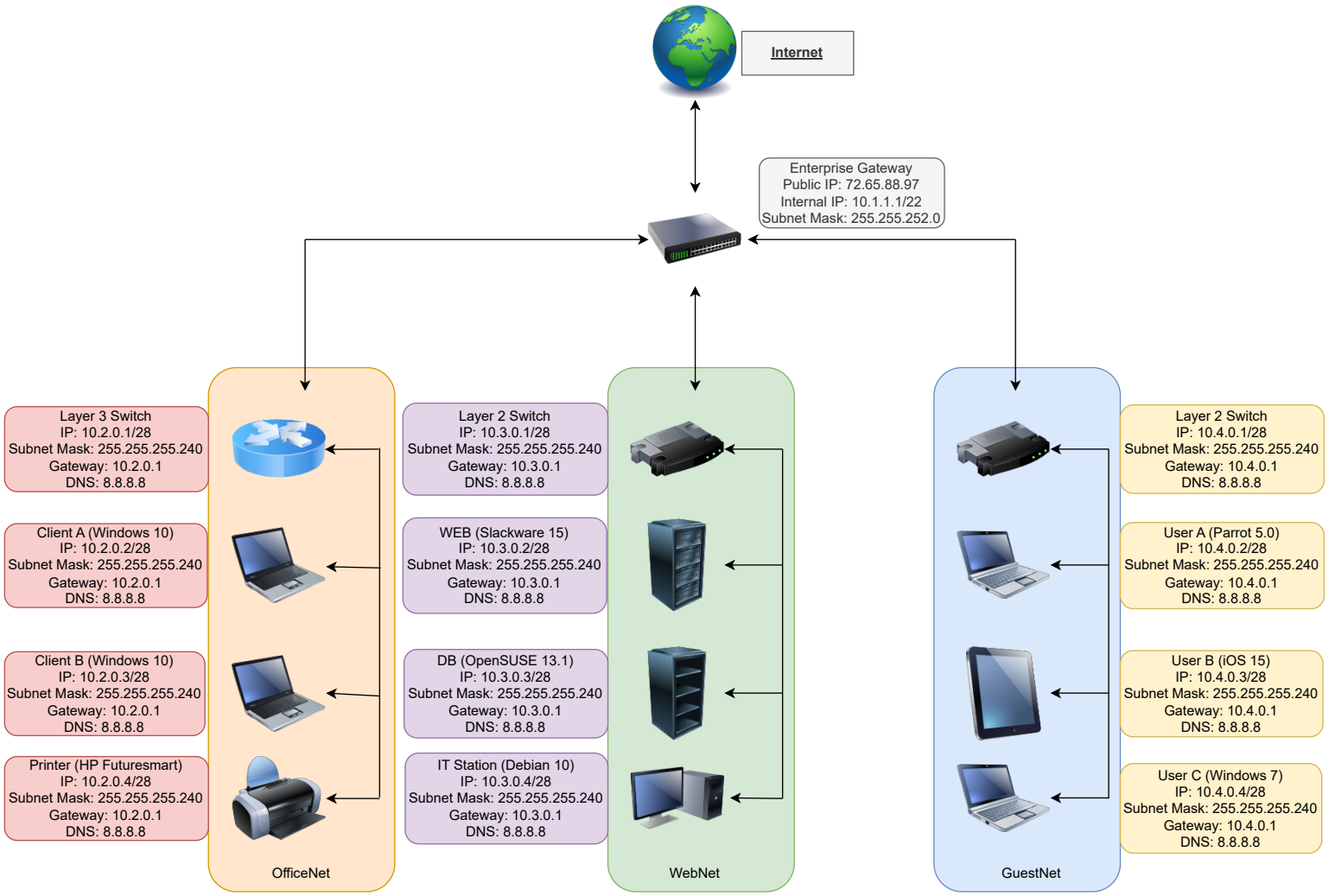
Thanks for taking your time and reading the whole proposals properly to stop any further vulnerabilities in the system.

Best Regards,

Faraz Ahmed

Security Engineer

UBNetDef.



HW09- TOPOLOGY