ENHANCING CYBERSECURITY WITH ADVANCED NETWORK SECURITY

by Boluwarin Oladipo

I. EXECUTIVE SUMMARY

Cybersecurity firm CrowdStrike defines an attack vector as a method or combination of methods in which an unauthorized person or cybercriminal gains access to a network or system[1]. This paper seeks to explore three attack vectors relating to recent vulnerabilities that may affect a modern individual or corporate network topology.

A network setup will be defined with network devices released between April 2023 and April 2024 with the purpose of the network being explained in context. A network setup diagram will be drawn to give a visual representation of the network. Vulnerabilities relating to devices on the network will be explored to determine the level of access each attack vector will give to a malicious attacker and the impact of the compromise.

Finally, mitigation solutions will be discussed for each attack vector based on the vulnerabilities and for the network in general in line with industry standard regulations and guidelines. The rest of the paper is organized as follows:

- Section II: Network setup
- Section III: Attack vectors
- Section IV: Mitigation solutions
- Section V: Conclusions
- References

II. NETWORK SETUP

A. *Defining the network*

To define the network, multiple authoritative sources on network topologies were consulted to ensure the network setup was as realistic as possible. A three-tier network [2] was selected as the topology due to the advantages it holds over other network designs in context of a corporate network distributed across multiple locations. Two of the major advantages are the scalability of the topology and the efficiency of traffic flow from the edge of the network to the endpoints[2].

Requirements:

The typical network devices and needs of a fictional animation company named Dexacorp Studios with 150 employees across three office locations within the same country were also considered to ensure the network topology was as realistic as possible.

- Dexacorp Studios works as a sub-contractor for several high-level animation studios on animated feature films and television shows.
- Their major requirements are highly available, fast digital storage media and local network connections with high throughput for effective collaboration amongst their Animation and Graphic Design departments.
- They also require the ability to work from anywhere in the world as securely as possible and accessing the network services as they need.

The National Vulnerability Database [3] was consulted for vulnerabilities within the last 6 months to determine what devices will be on the network. The websites and datasheets of networking equipment manufacturers Grandstream Networks was also consulted to obtain the Layer 2 and Layer 3 network switch specifications and determine their suitability for the network setup[4].

B. *Network Characteristics and Complexity*

The network topology is a three-tier network designed with redundancy and single responsibility in each layer of the network. Each branch office is connected to the headquarters via the Wide Area Network (WAN). There is a router present to enable WAN connectivity. Users of the network that are not present in any of the branch offices may connect to the network and access the resources present via the Virtual Private Network provided by the Palo Alto firewall present at the WAN edge. The main goal of the network's design is to enable efficient flow of north to south traffic (i.e. traffic coming in from outside the network to the required endpoint) and enable redundancy at each layer through the presence of two core switches and two distribution switches at each physical segment of the network. The three-tier network design addresses the major requirement of providing fast, reliable access to data on the Network Attached Storage device by making traffic only three physical hops from the network resource on the local network[2]. The network is configured so only company issued devices can connect to the network whether remotely or on-site at the headquarters or branch office. This design Table 1 shows the devices present on the network, their release date, hardware and software details.

C. *Assumptions*

- Only company devices are allowed to access the network.
- Two separate Internet Service Providers are present on the network to provide redundancy.
- WAN connectivity service and internet connectivity are provided by the same provider.

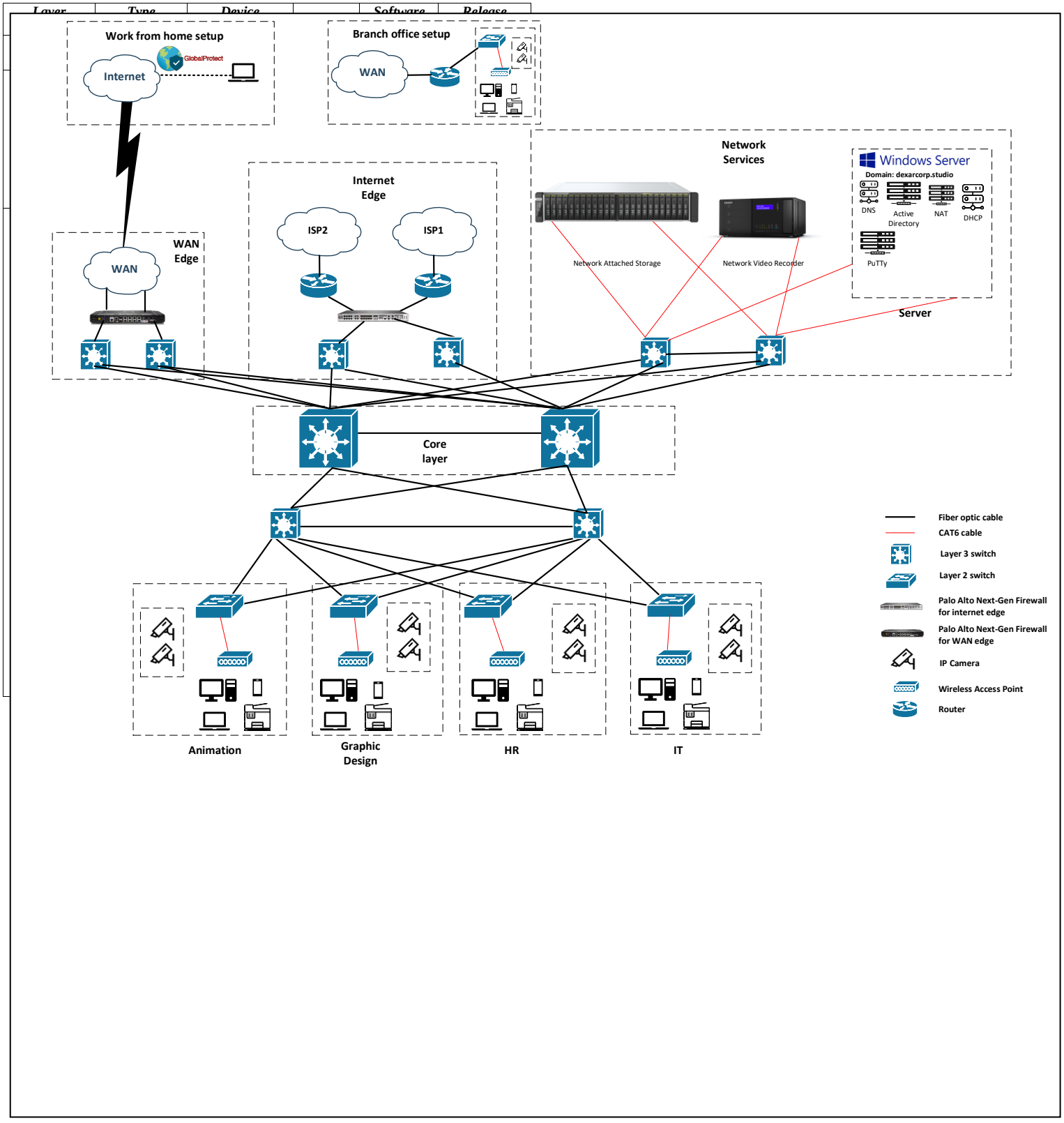

Fig. 1. Network diagram

TABLE I. NETWORK DEVICES

III. ATTACK VECTORS

Each attack vector targets a different layer of the Open Systems Interconnection model with the aim of compromising each or all of the confidentiality, integrity and availability of data and information present on the network is compromised when each or all these vectors are used. The Remote Code Injection vulnerability is present in the network on the Palo Alto edge next generation firewalls that allows a remote malicious attacker create and execute arbitrary code with root privileges [5], the man in the middle attack vector targets sensitive user traffic and seeks to manipulate requests and responses on the network through compromise of the vulnerabilities present in the Bitvise Secure Shell (SSH) client and server applications [10] and the Denial of service attack vector aims to disrupt the availability of the QNAP network attached storage devices present on the network [11]. Table II summarizes the attack vectors that will be discussed in detail in this section:

TABLE II. ATTACK VECTORS

Attack Vector	***Type***	***CVE***	***Brief Description***	***Exploit***	***Date***
Command Injection	Application	CVE-2024-3400 [12]	Inputting malicious code that is executed by the application	Arbitrary file creation resulting in command injection.	April 2024
Man in the Middle	Transport	CVE-2023-48795 [13]	Interception and manipulation of legitimate user traffic by a malicious actor	Removal of sequence numbers during SSH handshake bypassing connection security measures.	December 2023
Denial of Service	Network	CVE-2023-39296 [14]	Interruption in access to resources of authorized users with malicious intent.	Overriding existing attributes within the code with incompatibly typed attributes leading to a system crash	January 2024

A. Command Injection

Command injection according to the Open Web Application Security Program is the execution of arbitrary commands on a host's operating system that is executed by the targeted application [15]. This attack takes advantage of poor coding and flaws within applications to execute commands on the host with the privileges of the user the attacks are launched with. Version 11.1 of the PAN-OS operating system on Palo Alto firewall is susceptible to this attack vector through an arbitrary file creation vulnerability leading to command injection. The attacker may be unauthenticated and can execute commands with root privileges by creating scripts [5], [16].

Motive: The possible motives of this attack are to gain unauthorized persistent access to the network to perform reconnaissance operations on the network or exfiltrate sensitive information contained on the host operating system.

Techniques: SQL injection and cross site scripting are some techniques utilized to exploit this attack vector. They involve finding input fields where user input is not checked for illegal characters, keywords or strings that could lead to command injection [15].

Target devices: The target devices on the network where this attack vector can be exploited are the Palo Alto Next Generation firewalls present at the network borders due to a vulnerability within its PAN-OS operating system.

Vulnerabilities: The vulnerability CVE-2024-3400 published in April 2024 is a command injection vulnerability resulting from the creation of arbitrary files. These files could carry malicious payloads to execute scripts that enable the attacker achieve control over parts of or the whole network. This vulnerability has a CVSS 3.1 score of 10 on a scale of 10 [12] indicating a critical level due to the level of compromise that it could cause for information contained on the network .

Exploit: According to cybersecurity firm Volexity [17], a malicious actor they were tracking was able to create a reverse shell and gain access to a Palo Alto firewall device through the GlobalProtect feature. Proof of concept scripts have been disclosed by 3rd parties on public platforms[18].

Impact: The exploits detailed by security researchers tracking this vulnerability allowed access to the firewall, enabling the attacker remotely execute commands on the firewall device as a root user [17]. This gives the attacker total control over the network edge security measures and potentially compromises the entire network due to the high privileges obtained and relative low complexity of the exploitation of the attack vector.

The cybersecurity firm Volexity on April 10 and 11 2024 discovered compromise on the Palo Alto firewall device of two of its customers where it had deployed a network security monitoring service on successive days by the same threat actor[17]. This threat actor then deployed a reverse shell to download tools onto the device to exfiltrate data that will be useful for initiating lateral movement across the networks that were compromised. Volexity then broadened the scope of its investigation and discovered compromise on some of its other network security monitoring customer networks through the same attack vector dating back to March 2024. Fig. 2 below shows a timeline of events from the discovery of the exploitation of the vulnerability and publishing of the findings.

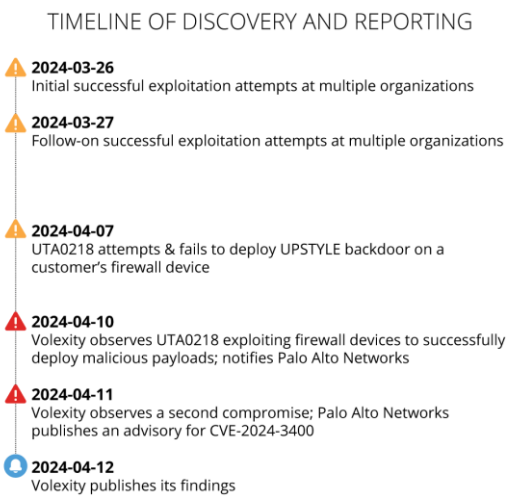

Fig. 2. Timeline of events of the investigation of CVE-2024-3400 [17].

B. *Man in the Middle*

A Man in the Middle attack is the interception and manipulation of communication between two parties by an unauthorized third party. This attack occurs at the network and transport layers of the Open Systems Interconnection model by interception of network packets exchanged between clients and servers by an unauthorized third party[19]. This attack requires the attacker to be on the same network as the server and the client. Due to a configuration flaw with the SSH protocol when used with certain OpenSSH extensions, a remote attacker is able to bypass integrity checks consequently downgrading the security of the connection and allowing an attacker to intercept and decode traffic [10].

Motive: The possible motives of this attack are to read privileged information passed over a connection between client and server.

Techniques: This attack can be performed by spoofing the IP or MAC address of the legitimate server in order to capture network packets and manipulate them.

Target technology: The target technology on the network where this attack vector can be exploited is the Bitvise Secure Shell (SSH) client and server applications installed on the individual workstations and network server.

Vulnerabilities: The vulnerability CVE-2023-48795 published in December 2023 [13] details a method whereby an attacker may omit some network packets, bypassing integrity checks used in completing the handshake for the establishment of a Secure Shell connection.

Exploit: Cybersecurity researchers Baumer, Brinkman and Schwenk provide a proof of concept of how the attack could be carried out in practice [10], [20]. They perform an extension downgrade attack where the packet EXT_INFO for negotiation of certain OpenSSH protocols is dropped but is not noticed by the client or the server because the attacker replaces the missing packet to counter the re-transmission of missing packets feature of the Binary Packet Protocol used in place of the Transport Control Protocol in implementation of Secure Shell connections when it detects a break of packet sequencing.

Impact: The exploit enables a remote attacker on the network intercept an SSH connection request and compromise its integrity by deletion of a sequence of number in the message required to complete its handshake and force the connection to use less secure encryption. This potentially allows the attacker snoop on the session and steal valuable and privileged information.

Cybersecurity researchers Fabian Bäumer, Marcus Brinkmann and Jörg Schwenk of the Ruhr University Bochum published a paper on 19th December 2023 named "Terrapin Attack: Breaking SSH Channel Integrity By Sequence Number Manipulation" [10] detailing the abuse of sequencing numbers on the Binary Packet Protocol to compromise SSH connections. The researcher claimed in the paper that 77% of SSH servers [10] on the public internet are vulnerable to this attack due to their configuration. This vulnerability was assigned CVE number CVE-2023-48795 [13]. The researchers proposed mitigation strategies as well as affected versions of programs that implement the SSH protocol in a configuration vulnerable to the Terrapin attack. While there have not been any reports of this vulnerability being exploited as part of any data breach or cyber-attack, it is not unlikely that it can be exploited on the network setup detailed in Section II especially when exploited along with the PAN-OS vulnerability (CVE-2024-3400) discussed in sub-section A of section III of this paper.

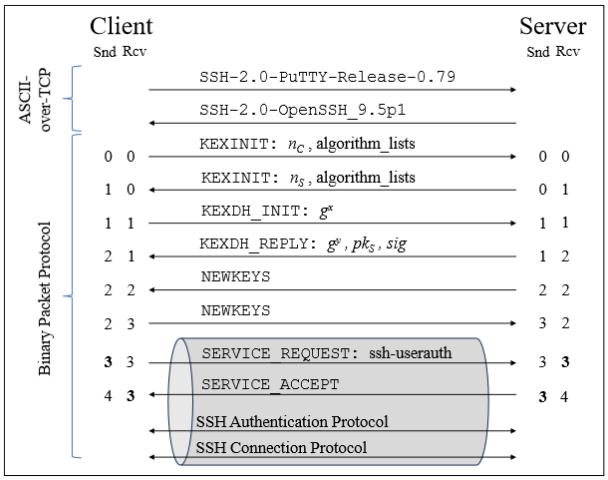

Fig. 3. Visual representation of the Secure Shell client-server handshake [10].

In Fig. 3 above, the client machine is running version 0.79 of the PuTTY SSH client program with the server is running version 9.5p1 of the OpenSSH server program. The *Snd* and *Rcv* values represent the sequence numbering on packets exchanged in the negotiation of the connection.

The exchange of packets is unencrypted until the exchange of the NEWKEYS message as is common with the connection-oriented Binary Packet Protocol. The authentication keys and encryption are then used to form a secure channel with the intention of protecting the confidentiality of further communication and the integrity of the ordering of the packets that will carry further information. There are two separate cipher streams for each direction of the connection and the order of the arrival of messages is guaranteed in one direction only.

Fig. 4 below is a visual representation of where the sequencing vulnerability exists [10]:

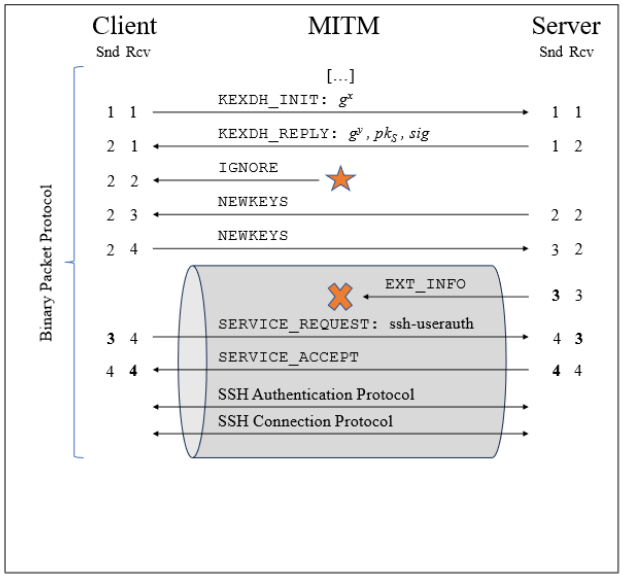

Fig. 4. Extension Downgrade Attack for ChaCha20-Poly1305 [10].

In the exploit represented above, the Man in the Middle injects an IGNORE message before the handshake concludes. The change in sequence numbers allows the MitM to strip the EXTINFO message from within the secure channel, directly downgrading the security of the connection by making the more secure extensions unusable.

Fig. 5 below is a chart of the trend of critically vulnerable servers discovered across North America, South America, Europe, Asia and Oceania between the 30th of March 2024 to the 27th of April 2024:

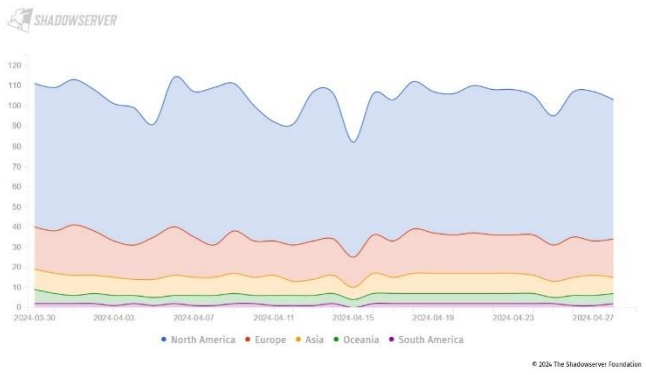

Fig. 5. Time-series chart showing the number of servers critically vulnerable to the Terrapin attack [21].

C. Denial of Service

A denial of service is the interruption of a legitimate client's access to a particular resource or service on a server by overloading the server with requests so it crashes and is unavailable. Fig. 6 below shows a visual representation of a denial of service attack.

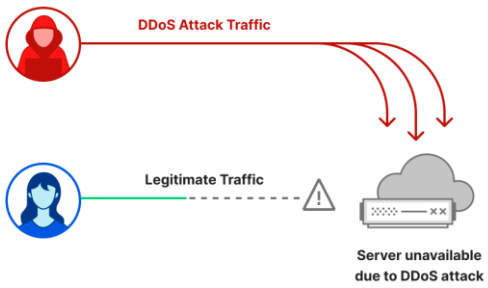

Fig. 6. Denial of service attack [22].

Motive: The aim of this attack is to disrupt operations that are facilitated by a particular service in order to either demand a ransom for stopping the attacks or distract the responsible network security team from another attack on the network.

Techniques: SYN flooding is a common techniques used to conduct denial of service attacks. Synchronize-Acknowledgment packets are used for the establishment of communication under the Transport Control Protocol. These packets are part of a 3-way handshake that is required to establish a session. According to Cloudflare's Distributed Denial of Service(DoS) report for the 4th quarter of 2023, SYN flood attacks were the second most common network layer attack recorded on their network for the year 2023 behind DNS flooding attacks [22].

Target devices: The target device on the network where this attack vector can be exploited is the QNAP Network Attached Storage devices due to the vulnerability that exists within its QTS and QuTS Hero operating systems [11].

Vulnerabilities: The vulnerability CVE-2023-39296 published in January 2024 is a prototype pollution vulnerability which allows remote attackers override existing attributes within the operating system code with unsuitable types via the network leading to unexpected behavior and crashing the program [14].

Exploit: The vulnerability is exploited by using specifically crafted Javascript Object Notation (JSON) object processed by the QTS and QuTS operating systems running on the Network Attached Storage devices. This exploits the failure of the parsing library present within the operating systems to verify each attribute is correctly typed, potentially leading to unhandled errors within the program and a subsequent crash[23].

Impact: The CVSS 3.1 base score of this vulnerability is 7.7 out of 10 [14] indicative of a high risk to networks with the affected devices running the vulnerable operating systems. Within organizations utilizing their Network Attached Storage systems to run periodical backups or store critical data of workstations and servers, this vulnerability will impair their ability to restore normal operations in the event of a disaster leading to further undesired consequences. A blog post by security researcher Do Son, [23] details a simple one-line command using cURL, a command line tool used to transfer data to and from servers [24] to exploit this vulnerability via the network and potentially cause an operating system crash of the Network Attached Storage devices. The ease of this attack with the privileges already obtained by exploiting other vulnerabilities discussed earlier in this paper pose a threat to the entire network.

According to Cloudflare [25], a Content Delivery Network (CDN) company that offers protection against denial of service attacks, the largest denial of service attacks recorded on their network increased from 26 million requests per second in 2022 to 201 million requests per second in 2023 [22]. This reflects the growing threat of denial of service attacks in the modern cybersecurity landscape.

While there have not been any public reports of this particular vulnerability being exploited as part of any data breach or cyber-attack, it is not unlikely that it can be exploited on the network setup detailed in section II especially when exploited along with the PAN-OS vulnerability (CVE-2024-3400) discussed in sub-section A of section III of this paper.

IV. MITIGATION SOLUTIONS

Generally, due to the vulnerabilities present on the network being zero-day vulnerabilities, updates to versions where the vulnerabilities have been fixed will be sufficient for mitigation of all the attack vectors discussed in this paper. Specific mitigations and guidelines will be discussed for each attack vector and the particular in the sections below.

A. Command Injection

Given the implications of a command injection attack on a network being severe due to how much undetected damage can be done on the network, the Open Web Application Security Project (OWASP) recommends some defenses against command injection attacks namely:

- Avoiding calling operating systems commands directly by utilizing Application Programming Interface (API) calls to robust libraries [26].
- Escaping values passed to operating system command calls within application code[26] e.g. converting all user input to a string data type before passing to the operating system command call negates the processing of any keywords that can be processed by the operating systems and defends against the attack.
- Annex A9 of the International Standards Organization 27001:2022 details guidelines on granting the least privilege necessary to individuals and programs to execute their tasks [27].

Due to the reliance on third party software to perform operations at the fictional company Dexacorp Studios, a comprehensive patch management schedule can be adopted to ensure mission-critical software is kept up to date. Patches were released for versions affected by the vulnerability within the PAN-OS operating system within four days [5] of the publishing of the proof of concept exploits by Volexity [17]. The fix completely prevented the initial attacks and any further attempt at persistence. Palo Alto Networks also released a threat detection identifier for its Threat Prevention customers to alert them if an attack was attempted on their firewall appliance.

This is in line with the guidelines set in the fourth revision of the National Institute of Standards and Technology special publication NIST SP 800-40r4 [28]. Applying the guidelines in securing the network may lead to more and frequent planned downtimes of the systems which may impact the productivity of the users. This can however be reduced by scheduling downtimes during off-peak hours.

B. Man in the middle

The security researchers credited with uncovering the Terrapin attack have stated there is no simple fix for the vulnerability due to the difference in implementations across different Secure Shell (SSH) server and client programs. [10] Updates were released for the Bitvise SSH client and server programs used on the workstations and server were released two days after public disclosure of the vulnerability with instructions on how to enable workarounds for managing the vulnerability [8], [9].

The consequence of this to users may be subject to longer connection times due to the use of stronger encryption algorithms and non-interoperability to servers and clients that do not have the patches applied on their respective SSH clients and servers and are therefore not able to establish connections [10].

C. Denial of service

Given the severity of a denial-of-service attack on operations of an organization, the best recommended mitigation solutions are outlined below:

- Recognition of denial-of-service network attempts is crucial to prevention of attacks. Organizations should invest in monitoring solutions and personnel to ensure threats are adequately prevented.
- Identification of potential targets is also crucial to prevention of attacks. These targets should be equipped with adequate protections to ensure they are well protected against any attacks.
- A well-defined response plan to any denial-of-service attacks.
- A well-designed network with that can absorb any attacks launched against it. The Layer 3 switches present at the network core and distribution layers provide 128Gbps of total switching capacity [ref. datasheet].
- Logical and physical segmentation of the network on as many layers as possible.

For Dexacorp Studios specifically, a denial-of-service attack on their network attached storage devices could completely disrupt their operations and their ability to recover from a disaster. The mitigation solutions for this attack vector should be a priority for implementation.

CONCLUSIONS

At the beginning of this paper, a realistic network was set up to meet the requirements of the fictional Dexacorp Studios by with network devices released between April 2023 and April 2024. Attack vectors targeting the specific vulnerabilities present on the network devices hardware and software were then researched using the National Vulnerability Database and the Common Vulnerabilities and Exposures database for vulnerabilities reported in the last 6 months.

Three attack vectors targeting three different layers of the Open Systems Interconnection reference model were explored and the accompanying vulnerabilities relating to the network. The attack vectors were discussed in detail with the motive, techniques, exploits and real-world security incidents all being critically analyzed for each attack vector. The man in the middle attack vector proved to be the most severe because of the depth of the flaws being at the protocol level and the impact of the widespread nature on interoperability of different SSH client and server implementations.

Mitigation solutions and general recommendations were proposed for each attack vector to properly mitigate risks in line with the ISO 27001 and NIST SP 800-40r4 guidelines[27], [28]. The consequences of implementing the mitigation solutions proposed for each attack vector on users on the network were also detailed and a comparison of the trade-offs.

The proposed next steps for this report are:

- A practical analysis of the best ways to implement the mitigation solutions proposed, either through technology, user education or policies using the fictional company Dexacorp Studios as a case study.
- Exploration of modern attacks at lower levels of the Open Systems Interconnection model than were discussed in the paper.

REFERENCES

[1] B. Lenaerts-Bergmans, "What are Attack Vectors: Definition & Vulnerabilities - CrowdStrike." Accessed: Apr. 30, 2024. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/attack-vector/

[2] Leslie, "What is Three Tier Architecture in Switch Networking?" Accessed: Apr. 17, 2024. [Online]. Available: https://www.qsfptek.com/qt-news/what-is-three-tier-architecture-in-switch-networking

[3] National Institute of Standards and Technology, "NVD - Home." Accessed: Apr. 30, 2024. [Online]. Available: https://nvd.nist.gov/

[4] Grandstream Networks, "Grandstream Releases New Layer 3 Aggregation Switches." Accessed: Apr. 18, 2024. [Online]. Available: https://blog.grandstream.com/press-releases/grandstream-releases-new-layer-3-aggregation-switches

[5] Palo Alto Networks, "CVE-2024-3400 PAN-OS: OS Command Injection Vulnerability in GlobalProtect." Accessed: Apr. 18, 2024. [Online]. Available: https://security.paloaltonetworks.com/CVE-2024-3400

[6] QNAP, "QuTS hero h5.1.2.2534 build 20230927 | Release Notes | QNAP." Accessed: Apr. 24, 2024. [Online]. Available: https://www.qnap.com/en/release-notes/quts_hero/h5.1.2.2534/20230927

[7] QNAP, "QTS 5.1 Series | Release Notes | QNAP." Accessed: Apr. 30, 2024. [Online]. Available: https://www.qnap.com/en/release-notes/qts/overview/5.1.0

[8] Bitvise, "Bitvise SSH Client Version History | Bitvise." Accessed: Apr. 30, 2024. [Online]. Available: https://www.bitvise.com/ssh-client-version-history

[9] Bitvise, "Bitvise SSH Server Version History | Bitvise." Accessed: Apr. 30, 2024. [Online]. Available: https://www.bitvise.com/ssh-server-version-history

[10] F. Bäumer, M. Brinkmann, and J. Schwenk, "Terrapin Attack: Breaking SSH Channel Integrity By Sequence Number Manipulation." arXiv, Dec. 19, 2023. Accessed: Apr. 27, 2024. [Online]. Available: http://arxiv.org/abs/2312.12422

[11] "Multiple Vulnerabilities in QTS, QuTS hero, QuTScloud, and myQNAPcloud - Security Advisory | QNAP." Accessed: Apr. 21, 2024. [Online]. Available: https://www.qnap.com/en/security-advisory/qsa-24-09

[12] Palo Alto Networks Inc., "NVD - CVE-2024-3400." Accessed: Apr. 30, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2024-3400

[13] MITRE, "NVD - CVE-2023-48795." Accessed: Apr. 30, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-48795

[14] "NVD - CVE-2023-39296." Accessed: Apr. 30, 2024. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-39296

[15] "Command Injection | OWASP Foundation." Accessed: Apr. 26, 2024. [Online]. Available: https://owasp.org/www-community/attacks/Command_Injection

[16] B. N. Chandan, "More on the PAN-OS CVE-2024-3400." Accessed: Apr. 21, 2024. [Online]. Available: https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/

[17] Volexity, "Zero-Day Exploitation of Unauthenticated Remote Code Execution Vulnerability in GlobalProtect (CVE-2024-3400)," Volexity. Accessed: Apr. 16, 2024. [Online]. Available: https://www.volexity.com/blog/2024/04/12/zero-day-exploitation-of-unauthenticated-remote-code-execution-vulnerability-in-globalprotect-cve-2024-3400/

[18] MiawOren, "0x0d3ad/CVE-2024-3400." Apr. 24, 2024. Accessed: Apr. 28, 2024. [Online]. Available: https://github.com/0x0d3ad/CVE-2024-3400

[19] Rapid7, "Man in the Middle (MITM) Attacks - Definition & Prevention | Rapid7." Accessed: Apr. 30, 2024. [Online]. Available: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

[20] "RUB-NDS/Terrapin-Artifacts." Ruhr University Bochum - Chair for Network and Data Security, Apr. 15, 2024. Accessed: Apr. 30, 2024. [Online]. Available: https://github.com/RUB-NDS/Terrapin-Artifacts

[21] The Shadowserver Foundation, "Time series · General statistics · The Shadowserver Foundation." Accessed: Apr. 29, 2024. [Online]. Available: https://dashboard.shadowserver.org/statistics/combined/time-series/?date_range=30&source=ssh&source=ssh6&severity=critical&tag=cve-2023-48795%2B&group_by=geo&style=stacked

[22] "DDoS threat report for 2023 Q4." Accessed: May 01, 2024. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-2023-q4

[23] D. Son, "Decoding the CVE-2023-39296 Vulnerability: A Technical and PoC Analysis." Accessed: Apr. 29, 2024. [Online]. Available: https://securityonline.info/decoding-the-cve-2023-39296-vulnerability-a-technical-and-poc-analysis/?expand_article=1

[24] D. Stenberg, "curl - How To Use." Accessed: Apr. 30, 2024. [Online]. Available: https://curl.se/docs/manpage.html

[25] Cloudflare, "What is Cloudflare? | Cloudflare." Accessed: May 01, 2024. [Online]. Available: https://www.cloudflare.com/learning/what-is-cloudflare/

[26] Open Web Application Security Project, "OS Command Injection Defense - OWASP Cheat Sheet Series." Accessed: Apr. 30, 2024. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/OS_Command_Injection_Defense_Cheat_Sheet.html

[27] M. Edwards, "ISO 27001 – Annex A.9: Access Control | ISMS.online." Accessed: Apr. 30, 2024. [Online]. Available: https://www.isms.online/iso-27001/annex-a-9-access-control/

[28] M. Souppaya and K. Scarfone, "Guide to enterprise patch management planning : preventive maintenance for technology," National Institute of Standards and Technology (U.S.), Gaithersburg, MD, NIST SP 800-40r4, Apr. 2022. doi: 10.6028/NIST.SP.800-40r4.