**UNIVERSITY OF WESTMINSTER**

**College of Design, Creative and Digital Industries**

**School of Computer Science and Engineering**

**6NTCM004W - Security Testing and Implementation**

**Coursework:**

**Security Appliances and Wireless Security**

Vulnerability Scanning and Penetration Testing

**Student**

**Dragomir Alexandru Mihai w164298**

**Professor**

**Imtiaz Sandia**

Contents – ***CTRL + CLICK to navigate***

[Large enterprise network 2](#_Toc100039392)

[Security Appliances - Cisco ASA 5585-X with FirePOWER SSP-60 2](#_Toc100039393)

[Firewall: 2](#_Toc100039394)

[IDPS 4](#_Toc100039395)

[VPN 5](#_Toc100039396)

[Wireless Security 5](#_Toc100039397)

[Small Enterprise Network 7](#_Toc100039398)

[Security Appliance - Cisco Firepower 1150 with ASA 7](#_Toc100039399)

[Firewall 7](#_Toc100039400)

[Technical specifications 8](#_Toc100039401)

[Access Control 8](#_Toc100039402)

[Intrusion Detection and Prevention 8](#_Toc100039403)

[Advanced Malware Protection and File Control 8](#_Toc100039404)

[BYOD Security 9](#_Toc100039405)

[Application Control 9](#_Toc100039406)

[Containerization 9](#_Toc100039407)

[Encrypting Data at Rest and in Transit 9](#_Toc100039408)

[Small business network. 10](#_Toc100039409)

[Security appliances – Cisco Meraki MX64 10](#_Toc100039410)

[Firewall: 11](#_Toc100039411)

[IDPS: 12](#_Toc100039412)

[VPN: 12](#_Toc100039413)

[Wireless Security 13](#_Toc100039414)

[Changing the default SSID 13](#_Toc100039415)

[Enabling Encryption 13](#_Toc100039416)

[Disabling SSID Broadcast 13](#_Toc100039417)

[Adjust Radio Power Levels 13](#_Toc100039418)

[Assign Static IP addresses 14](#_Toc100039419)

[MAC address filtering 14](#_Toc100039420)

[Vulnerability assessment 15](#_Toc100039421)

[Scan Results: 15](#_Toc100039422)

[Penetration Testing 18](#_Toc100039423)

[Discovery: 18](#_Toc100039424)

[Scoring – Outdate Python version 21](#_Toc100039425)

[Vulnerability exploited: Cross Site Scripting (XSS) 21](#_Toc100039426)

[References and bibliography: 23](#_Toc100039427)

Task 1 (Security Appliances and Wireless Security)

**Large enterprise network**

Graphical user interface, diagram

Description automatically generated*Figure 1: Tier 3 topology, demonstrating placement of security appliances, author: Alexandru-Mihai Dragomir*

Security Appliances - Cisco ASA 5585-X with FirePOWER SSP-60

Firewall:

A close-up of a computer

Description automatically generated with low confidence*Figure 2 – Cisco ASA 5585-X with FirePOWER SSP-60[1]*

Specifications that are of interest in our case, given the 10 Gbps bandwidth, we need a firewall that can maximise the bandwidth performance and not bottleneck it. Therefore, the ASA 5585X can provide the following throughputs:

* 15 Gbps for application visibility and control[1]
* 40 Gbps stateful inspection [1]

In terms of handling large amounts of traffic and users, the numbers are:

* 1024 VLANs [1]
* 7500 Cisco Cloud Web Security users [1]
* 160000 new connections per second [1]
* 4000000 concurrent sessions [1]
* 10000 site-to-site and IPsec IKEv1 client VPN user sessions [1]

Cisco ASA with FirePOWER Services augments the Cisco ASA 5585-X Adaptive Security Appliance firewall systems with specific threat-focused next-generation security services. It offers full protection against known and advanced threats, including targeted and persistent malware attacks. The Cisco ASA with FirePOWER Services includes the following full capabilities:

* stateful firewall with remote access VPN and intelligent clustering for highly secure, high-performance access and high availability to ensure business continuity. [1]
* Reputation and category-based URL filtering that can provide full alerting and control over malicious online traffic, enforcing standards over millions of URLs in over 80 categories. [1]

Practical configurations that I recommend implementing:

1. Permitting or Denying Traffic with Access Rules

Used to restrict traffic both outbound and inbound traffic.

1. Applying NAT

NAT is used to hide local addresses from other networks, making it harder for attackers to discover the real address of the device

1. Protecting from IP Fragments

The ASA protects against IP fragmentation. This capability completes full reassembly of all ICMP error signals as well as virtual reassembly of the remaining IP fragments routed through the ASA. When a fragment fails the security check, it is being dropped and logged.

1. Applying HTTP, HTTPS, or FTP Filtering

Although access lists can be used to block outbound access to specific websites or FTP servers, due to the breadth and dynamic nature of the Internet, controlling and managing web usage in this manner is impractical.

Cloud Web Security should be configured on the ASA, or an ASA module that provides URL and other filtering services, in this case the ASA FirePOWER, can be installed. The ASA can also be used in conjunction with a third-party product, such as the Cisco Web Security Appliance (WSA).

1. Applying Connection Limits and TCP Normalization

TCP and UDP connections, as well as embryonic connections, can be restricted. A DDoS attack is mitigated by limiting the number of connections and embryonic connections.

The embryonic limit is used by the ASA to activate TCP Intercept, which protects internal systems from a DDoS attack conducted by flooding an interface with TCP SYN packets.

Ultimately, the ASA firewall can run in two modes: router and transparent.

The difference being that in the routed mode, the firewall is considered a router hop in the network, whereas the transparent mode the firewall is stealthier and does not count as a router hop.

In terms of which mode should the network administrator decide to operate the firewall, I recommend the transparent mode, as it can cloak the firewall from attackers, making it harder to locate and identify and also helps simplifying the network configuration. However, it will not support integrated routing and bridging, so if the network relies on this, the firewall should be configured in the routed mode.

IDPS

The Adaptive Security Algorithm inspects all traffic passing through the ASA and determines whether it should be permitted through or dropped. A simple packet filter can check for the correct source address, destination address, and ports, but it cannot check for the correct packet sequence or flags. A filter also checks each packet against the filter, which can be a time-consuming procedure.

A single ASA can be divided into many virtual devices known as security contexts. Each context is a self-contained device with its own security policies, interfaces, and administrators. Having several contexts is analogous to having multiple separate devices. Many functions, including as routing tables, firewall features, intrusion prevention systems, and management, are offered in multiple context modes.

The ASA FirePower module can be configured either to inline or monitor-only deployment. For which I recommend configuring the FirePower module as inline deployment.

Traffic in inline mode is routed through the firewall before being forwarded to the ASA FirePOWER module. When you choose traffic for ASA FirePOWER inspection on the ASA, it passes as follows through the ASA and the module:

Diagram

Description automatically generated *Figure 3: ASA FirePower deployment demonstration [2]*

VPN

Tunnelling protocols are used by the ASA to negotiate security parameters, establish, and manage tunnels, encapsulate packets, transmit or receive them via the tunnel, and unencapsulated them. The ASA acts as a bidirectional tunnel endpoint, receiving plain packets, encapsulating them, and sending them to the other end of the tunnel, where they are unencapsulated and routed to their destination. It can also receive encapsulated packets, decapsulate them, and deliver them to their intended destination.

ASA support the following functions[]:

* Establishes tunnels
* Negotiates tunnel parameters
* Authenticates users
* Assigns user addresses
* Encrypts and decrypts data
* Manages security keys
* Manages data transfer across the tunnel
* Manages data transfer inbound and outbound as a tunnel endpoint or router

Wireless Security

A few steps that can be taken in order to ensure or at least fortify wireless security are:

* Change default passwords - because default passwords are easily obtained online, employing complicated passwords can make it more difficult for attackers to access a device.
* Restrict access - by filtering MAC addresses, you can restrict access to your network to just authorised users.
* Encryption – best would be WPA3 to secure information being transmitted over the network.
* Change default SSID - the default SSID may allow attackers to determine the type of router and potentially exploit any known vulnerabilities.
* Disable fire sharing: - When not needed, file sharing should be disabled, and never open a whole hard drive for file sharing or allow file sharing on public networks.
* Security patches - Check the manufacturer's website for any updates or patches for your device on a regular basis.

**Small Enterprise Network**

Diagram

Description automatically generated*Figure 4: Tier 2 topology, demonstrating placement of security appliances, author: Alexandru-Mihai Dragomir*

Security Appliance - Cisco Firepower 1150 with ASA

A picture containing text, electronics, projector

Description automatically generated*Figure 5: Cisco Firepower 1150 with ASA[3]*

Firewall

A tier 2 network topology resume of users accessing the database directly from the client system, without a mediator application server in between. Therefore, visibility and control of applications are a must. The BYOD policy requires a more detailed inspection and prevention mechanism, also, being a small enterprise network – the firewall solution must be bandwidth effective and being able to deal with a large number of requests.

Given the above, I recommend the Cisco Firepower 1150 with the ASA module.

Technical specifications

Throughput speeds[4]:

* Firewall (FW) + Application Visibility and Control 5.3 Gbps
* FW + AVC + Intrusion Prevention System 4.9 Gbps
* Transport Layer Security (TLS) 1.5 Gbps
* IPSec VPN throughput (1024B TCP w/Fastpath) 2.4 Gbps

Connections[4]:

* Maximum concurrent sessions, with AVC 600000
* Maximum VPN Peers 800

Access Control

Access control policies need to be configured to leverage Security Intelligence data to blacklist traffic, and access control rules should be used to exercise granular control over network traffic logging and handling. These rules can be basic or complicated, matching and inspecting traffic based on many parameters; for example, you can control traffic by security zone, network or geographical location, port, application, requested URL, and user.

Each access control rule also contains an action, which defines whether matching traffic is monitored, trusted, blocked, or allowed. When you accept traffic, you can instruct the system to first scan it with intrusion or file policies to detect and block any exploits, malware, or forbidden files before they reach your assets or leave your network.

Intrusion Detection and Prevention

These policies examine traffic for security violations and, in inline implementations, can block or alter hostile traffic using intrusion rules and other parameters.

If the system-provided policies do not fully suit your organization's security needs, custom policies can improve system performance in your environment and give a concentrated view of hostile traffic and policy violations on your network. You may define how the system analyses and inspects network traffic for intrusions at a very granular level by developing and adjusting custom policies.

Advanced Malware Protection and File Control

Network-based advanced malware protection (AMP) enables the system to scan network traffic for malware in various file types.

You can submit a discovered file to the Collective Security Intelligence Cloud for a basic known-disposition lookup using the file's SHA-256 hash value, regardless of whether you store it. You can set the system to prohibit or allow specific files based on this contextual information.

As part of your overall access control setup, you configure malware protection; file policies connected with access control rules inspect network traffic that fulfils rule requirements.

File control allows devices to identify and prevent your users from uploading (sending) or downloading (receiving) specified types of files over specific application protocols. As part of your overall access control setup, you define file control; file policies linked with access control rules inspect network traffic that fulfils rule requirements

BYOD Security

Application Control

* iOS devices have the ability to restrict access to the Apple App Store.
* Android Enterprise allows you to configure Google Play to display only approved applications.

Drawbacks: limiting access to applications on a user's personal device is impractical, as employees are likely to oppose such limitations because they believe they should be able to use their own device freely when not at work.

Containerization

Containerization is a method of separating each component of a device into its own secure environment, each with its own password, security settings, programmes, and data. This allows employees to use the gadget freely while still preventing security hazards to the business network.

Cyber criminals who penetrate the general workplace are entirely contained within it and are unable to migrate laterally to the other protected environment. They can't get to the host or privileged OS, and they can't even tell it's there.

Encrypting Data at Rest and in Transit

BYOD causes sensitive data to be retrieved and seen on systems that are not under the control of a company.

Encryption protects the content of important files even in the worst-case scenario of device theft or compromise.

Encrypting all data delivered to staff devices can be difficult in practise. All scenarios in which a user downloads or saves a file on the local computer, such as downloading email attachments or obtaining data from corporate cloud storage, must be considered by security and operations teams. In all of these circumstances, the BYOD device's software must verify that the data is secured.

Drawback: encryption can stifle day-to-day operations, reduce productivity, and irritate users. Furthermore, any flaw in the encryption procedure can prevent users from accessing crucial files required for their employment.

**Small business network.**

*Diagram

Description automatically generatedFigure 6: SOHO topology, demonstrating placement of security appliances, author: Alexandru-Mihai Dragomir*

Security appliances – Cisco Meraki MX64

A grey stapler on a white surface

Description automatically generated with medium confidence*Figure 7: Cisco Meraki MX64[5]*

For the SOHO network, the recommended solution would be the security appliance of the Cisco Meraki MX64, that features traffic shaping with application management, malware protection and intrusion detection and prevention.

Firewall:

The MX64 firewall settings provide layer 3 stateful rules support and layer 7 stateless rules.

Layer 3 configurations available that should be implemented to achieve network security:

*Outbound and Inbound rules*

ACL statements can be configured to govern whether to allow or deny traffic between subnets or out or from the network to the Internet and vice-versa. The MX allows configuration of ACL based on protocol, source IP and port or destination IP and port.

*Cellular Failover Rules*

When the appliance switches to using a cellular modem as its uplink, these firewall rules are added to the existing outgoing rules. This can be beneficial for restricting cellular traffic to only business-critical applications in order to avoid excessive cellular overages.

Layer 7 configurations available that should be implemented to achieve network security:

*Traffic shaping and application management:*

Without specifying IP addresses or port ranges, firewall rules can be created to ban specific web-based services, websites, or types of websites. This is especially beneficial when programmes or websites use several IP addresses, or when their IP addresses or port ranges change.

Applications could also be blocked by category (for example, 'All video & music sites') or by application type within a category (for example, only iTunes within the 'Video & music' category).

In addition to that, traffic can be restricted also based on the HTTP hostname, destination port, remote IP rand and combination between Destination IP and port.

*Geo-IP based rules*

Can be used to filter traffic depending on the origin of inbound traffic or the destination of outbound traffic. You can choose to restrict all traffic to or from a certain group of countries or all traffic that is not to or from a specific set of countries.

*Port forwarding*

Should be used to forward traffic destined for the WAN IP of the MX on a specific port to any IP within a local subnet.

*Forwarding rules for NAT server*

Since there are 8 devices in the network, I made the assumption that all of the would have to access the NAT server, therefore the recommended forwarding profile here should be 1:Many NAT, which allows you to specify one public IP that has multiple forwarding rules for different ports and LAN IP addresses.

IDPS:

The intrusion detection mechanism is analysing the flow of packets between both LAN and internet interfaces, and subnets, logging all the triggered alerts to the Syslog.

From there, the intrusion prevention component blocks the malicious packets and also subsequent packets from the same flow. Although this solution is a great first layer of defence, it should not be used alone, and I recommend consolidating it with a host-based security solution to fortify the defence strategy.

The IDPS can be configured based on three different detection rulesets based on CVSS score.

1. Connectivity

Cisco’s vulnerability database composed of rules from the current year and past to years for threats with a CVSS score of 10.

1. Balanced

Category based rules with a CVSS score of 9 from, Malware-CNC, Blacklist, SQL Injection and Exploit Kit.

For example, rules for known malicious commands such as call home, force download dropped files, exfiltration of data and other control activity for identified botnet traffic. Rules for known URLs, user agents, DNS hostnames or IP address that have been reported as malicious. Lastly, rules that can detect SQL injection and exploit kit activity.

1. Security

Rules regarding above mentioned categories but targeting slightly lowered scored vulnerabilities (CVSS score of 8), plus rules that can look for and control certain applications that could generate network activity.

The MX64 has built in Advanced Malware Protection, which comes in the form of a license add on.

The key functionality of this feature is that once enabled, it will constantly look through all the files that are being downloaded and asses based on three defined dispositions whether the contents are clean, malicious, or unknown to the software’s database, and acts against the findings, by isolating and blocking the malicious files.

VPN:

In terms of virtual private network capabilities, the MX offers client VPN service through the L2TP tunnelling protocol and does not require any additional software.

Encryption methods available are: 3DES and hashing SHA1 for Phase1 and AEX128/3DES and SHA1 for Phase2.

For authentication, the MX provides three options: Meraki Cloud, Radius or Active Directory.

To transmit and authenticate credentials, Meraki client VPN use the password authentication protocol (PAP). PAP authentication is always sent using strong encryption inside an IPsec tunnel between the client device and the MX security appliance. User credentials are never sent in clear text over a WAN or LAN. Because PAP is the inner authentication mechanism used inside the encrypted IPsec tunnel, an attacker sniffing the network will never access the user credentials.

In terms of the authentication, I would recommend using the Meraki Cloud platform, as it offers network administrators to later integrate with the Sentry VPN Security from Cisco, which can be configured to deploy the necessary configuration needed to connect through the Client VPN via the System Manager profile of the device.

Wireless Security

Changing the default SSID

By default, network access devices use the manufacturer’s name or model number of the device as the network service set identifier.

If the wireless network broadcasts the default SSID, an attacker could research the documentation for that specific device to determine default IP address range, default administrator credentials and other details that could help compromising the network easily.

This method will not stop the attacker from trying to obtain that information through other means, it will just make it a little more challenging to do so.

Enabling Encryption

At least WPA2, ideally WPA3 if supported. If encryption is not enabled, the network will be open for anyone to connect, putting at risk the confidentiality and integrity of the data and business applications, as attackers could join and see the network traffic and operations. Secondly, anyone could connect to the network and consume bandwidth, resulting in a slower internet speed.

The drawback of this method is that it relies heavily on the complexity of the password, thus, heaving a weak password would result in an attacker being able to quickly crack the password and gain access to the network. On the opposite side of the coin, heaving a complex password, would only make it more time consuming to crack, but not impossible.

Disabling SSID Broadcast

By disabling the SSID broadcast option, the router will stop advertising the SSID. Meaning that casual users looking up Wi-Fi networks will not be able to discover the SOHO network, while this option will not stop an attacker from discovering the network, because network analyser tools can still see disabled SSIDs, it will however, make it less probable to be targeted by random people trying to connect to available Wi-Fis.

Adjust Radio Power Levels

The radio power level of a wireless router is adjustable. By default, the power level might be set too high, meaning that the wireless signal could be emitted outside the perimeter of the office – which could result in an attacker standing at the edge of that perimeter to pick up on the signal and try to gain access on the network. Therefore, the radio power level should be adjusted in a way that will not go beyond the perimeter of the office.

There are two drawbacks to this method: if the power levels are set too low, the signal could not cover the whole perimeter of the office, resulting in the office having spots in which the signal is not available; this method will not stop an attacker from gaining access to the network, it will just limit the physical distance that an attacker would need to able to discover and reach the network.

Assign Static IP addresses

In order to restrict certain devices from obtaining an IP address from the router, the DHCP should be disabled. Meaning that the network administrator, will manually have to assign IP addresses to devices that are trying to join the network, therefore restricting access for unwanted devices.

MAC address filtering

MAC addresses are uniquely assigned to each network card and are being used to determine access to a network. MAC address filtering is a method in which a blacklist and a whitelist are defined and used in order to either permit or deny network access to specific devices. Therefore, similar to the above-mentioned method, by creating a whitelist with the known devices in the office, you can deny access to any other devices trying to connect.

However, there are limitations with this option. MAC address filtering can be circumvented by an attacker. Since MAC addresses are not encrypted, an attacker using a packet analyser tool could discover the MAC address that belongs to a network whitelisted device, and then using MAC spoofing software, can masquerade the MAC address of the whitelisted device to gain access to the network.

Task 2 (Vulnerability Scanning and Penetration Testing)

**Vulnerability assessment**

Tools used for the exercise – Nessus, Skipfish, Nmap, Pentest-Tools, Lighthouse, Bull-Attack, Netcraft and Kali-Linux.

Nessus, Pentest-Tools, Lighthouse vulnerability scanning, Skipfish – fingerprint scanning/directory crawler, Nmap, Netcraft – network discovery, Bull-Attack – geolocation IP tracer.

Scan Results:

1. Nessus

Nessus was able to find one Critical vulnerability with a score of 10 according to the CVSS V3.0, that vulnerability being an unsupported Python version being used on the website, which coincided with the findings from Pentest-Tools, however, not flagged by Lighthouse or Skipfish.

The other 19 findings, Nessus labelled them as noise (info), however, some of them are returning valuable information such as: Device type, OS Identification, protocols available ICMP, TCP etc, all which can be used to identify the target device.

1. Lighthouse

Lighthouse only flagged two security issues: using HTTP instead of HTTPS and a XSS vulnerability due to the usage of a vulnerable jQuery package.

1. Skipfish

With Skipfish I have run a different kind of analysis, it was a vulnerability scan, but also a crawl scan – or could also be interpreted as a fingerprint directory-based attack, as I was able to retrieve paths of files, hidden files, scripts etc, which played a vital role in helping me understand the software that was used to compose the webpage.

1. Pentest-tools

Provided the most insight into the vulnerabilities of the webpage, being able to not only flag the critical python outdated version, but also broke down every single known vulnerability that comes with existing python versions, providing rich information on where the issue is and how it can be exploited. In addition to that, it was also able to identify the XSS vulnerabilities cause by the jQuery package.

Graphical user interface

Description automatically generated*Figure 8: Nessus scan results* Chart, waterfall chart

Description automatically generated*Figure 9: Pentest-Tools results*

*Table

Description automatically generated with medium confidenceFigure 10: Pentest-Tools results continued* A screenshot of a computer

Description automatically generated*Figure 11: Lighthouse scan resultsGraphical user interface, text, application

Description automatically generatedFigure 12: Skipfish Crawl resultsGraphical user interface, text, application

Description automatically generatedFigure 13: Skipfish files found*

**Penetration Testing**

Discovery:

1. Operating System - Linux

Text

Description automatically generated*Figure 14: Nmap os interrogation results*

1. Server software found:

Graphical user interface, text, application

Description automatically generated*Figure 15: Netcraft search results*

1. Services running on the web server:

Text

Description automatically generated*Figure 16: Nmap services running results*

1. Network information:

Graphical user interface, text, application, email

Description automatically generated*Figure 17: Netcraft lookup results*Graphical user interface, text, application

Description automatically generated*Figure 18: Netcraft IP delegation results*

1. Geolocation tags:

A screenshot of a computer

Description automatically generated with medium confidence *Figure 19: Bull-Attack geolocation information*

Scoring – Outdate Python version

Graphical user interface, text, application, chat or text message

Description automatically generated*Figure 20: CVSS V3.1 online calculator*

Vulnerability exploited: Cross Site Scripting (XSS)

Cross-Site Scripting (XSS) attacks are a sort of injection in which malicious scripts are injected into otherwise trustworthy websites. XSS attacks occur when an attacker utilises a web application to transmit malicious code to a separate end user, typically in the form of a browser side script. The flaws that allow these attacks to succeed are extremely common, and they occur whenever a web application includes user input inside the output it generates without verifying or encoding it.

eval() is a hazardous function that executes the code provided to it with the caller's privileges. If you use eval() on a string that could be manipulated by a malicious entity, you could end up running malicious code on the user's machine with the rights of your webpage / extension. More crucially, a third-party code can know the scope in which eval() was used, which can lead to assaults in ways that the equivalent Function is not vulnerable to.

The code I wrote leverages eval() to successfully execute arbitrary code from the console of the webpage.

Graphical user interface, application

Description automatically generated*Figure 21: XSS injection demonstration*A screenshot of a computer

Description automatically generated*Figure 22: XSS injection console script [6]*

**References and bibliography:**

1. Support, P., Services, C. and Guides, I., 2022. *Cisco ASA FirePOWER Module Quick Start Guide*. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/td/docs/security/asa/quick\_start/sfr/firepower-qsg.html> [Accessed 5 April 2022].
2. Support, P. and Services, C., 2022. *Cisco ASA 5585-X with FirePOWER SSP-60*. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/support/security/asa-5585-x-firepower-ssp-60/model.html#DataSheetsandProductInformation> [Accessed 5 April 2022].
3. Services, P., Series, C. and Sheets, D., 2022. *Cisco Firepower 1000 Series Data Sheet*. [online] Cisco. Available at: <https://www.cisco.com/c/en/us/products/collateral/security/firepower-1000-series/datasheet-c78-742469.html> [Accessed 5 April 2022].
4. Network Warehouse. 2022. *Cisco Firepower 1150 Security Appliance | FPR1150-ASA-K9*. [online] Available at: <https://networkwarehouse.co.uk/products/cisco-fpr1150-asa-k9?variant=35815444742298> [Accessed 5 April 2022].
5. Cisco Meraki. 2022. *Meraki MX64W | Security & SD-WAN | Enterprise WAN*. [online] Available at: <https://meraki.cisco.com/en-uk/product/security-sd-wan/small-branch/mx64/> [Accessed 5 April 2022].
6. Dragomir, A., 2022. *xss-injection*. [online] Available at: <https://github.com/dragomir-am/xss-injection.git> [Accessed 5 April 2022].
7. Cisco Meraki. 2022. *SD-WAN and Traffic Shaping*. [online] Available at: <https://documentation.meraki.com/MX/Firewall\_and\_Traffic\_Shaping/SD-WAN\_and\_Traffic\_Shaping> [Accessed 5 April 2022].
8. Cisco Meraki. 2022. *Client VPN Overview*. [online] Available at: <https://documentation.meraki.com/MX/Client\_VPN/Client\_VPN\_Overview> [Accessed 5 April 2022].
9. 2022. [online] Available at: <https://community.cisco.com/kxiwq67737/attachments/kxiwq67737/4561-docs-security/5098/1/Cisco%20ASA%20with%20FirePOWER%20Services%20data%20sheet.pdf> [Accessed 5 April 2022].