# Assignment 2: Coursework

Systems Security

# Index

## 1. Detecting reconnaissance

First, I need to have an inventory with all the organisation assets to identify the risks analysing all the network critical points to mitigate found ones. The exposure level will be calculated multiplying the probability of exploitation with the potential company's lost.

I will collect flows and logs. Flows are a sequence of network packets from a source computer to a destination, for example when we establish a session between two hosts. Logs are events in a computer, firewall, web proxy, server and can be originated by processes and actions.

Relatively to flows, we must collect data from network traffic on the core gateway that is facing the internet (1). This is the entry point, it is always a must to capture the inbound and the outbound data. Capturing data in this node we can detect data exfiltration, connections to C&C servers, access to malicious sites, brute force attacks, DDoS, SQL injections, XSS, etc. We collect data on node 7 because we pretend to analyse if there are non authorized access to servers from clients' nodes (10 and 11). On node 2 because we have a lot of servers connected to this router and we are going to analyse the traffic reaching those servers, specifically, the traffic that is going to node 7, 5, 4 and 3. Node 3 is also relevant because is connected to servers through node 4 and receive flows from node 8 where are connected the majority of clients' nodes. Node 8 will give high visibility over the clients' nodes and detect lateral movements. The downside is that host to host connections in the same network segment will not be analysed. 9 is the Wi-Fi AP that will enable the client to have his employees connecting their own devices to the internal network (BYOD), this creates a lot of variables that increase the attack surface so it must be watched closely. This will detect the exposure for example of a man-in-the-middle attack to an IT administrator that is accessing the servers.

Relatively to logs, I want to collect mainly from Servers and Domain Controllers (DC). A deep investigation on all servers: web servers, database servers, proxy server, file servers, etc. Their logs, system information, open ports, software, a full reconnaissance that enable to calculate their exposure levels. The logs from DC will give a detailed overview of the node since they are responsible for the backbone of any Windows Domain. I want to collect important information about account actions, privileges escalation, unauthorized authentications, etc.

If an intruder collects this data (i.e spyware or tapping the network traffic) they can understand how the security infrastructure works and easily commit malicious behaviours without being noticed or even tempering that data to incriminate another identity.

To collect the network data (flows) from the referenced nodes I would implement TAP and SPAN. I would advise the client to keep collecting flows described above and sending it to the security information event management (SIEM) platform. The implementation of a firewall that controls all inbound and outbound traffic and it must have the capability of IPS, AntiVirus, AntiBot, URL filtering, content filtering, application control, etc. All logs from this firewall will go to a SIEM platform, this could be configured directly in the firewall. The servers and endpoints also should have an AntiVirus server with IPS capabilities. The client should also have a WAF (reverse proxy server and load balancer) for which all outbound connections are centralized with anti-malware, URL filtering and content filtering capabilities. For the portals that are exposed to the internet a web application firewall (L7) to protect the application from XSS, DDoS, SQL injection should be implemented. The last advised at the network level is the implementation of 2FA solution to prevent access from compromised accounts to servers.
To collect servers and DC data I would install an agent collector that automatically will send the needed for further analysis, using an agent collector which will send data to a SIEM server with

automatic tools to analyse all generated alerts. For both DC and servers, it would be ideal to keep track only specific events. If the client wants to collect them he would need to install a collector agent and a central server. Encrypt of files mainly on servers and disks in case of data stolen which will make harder to access the plain text data. Data lost prevention (DLP) software should also be installed on the servers, it will be essential to detect inside threats such as data exfiltration.
For the central server/SIEM, I would advise the ELK stack to aggregate and analyse data of all hosts. This SIEM will receive a massive amount of logs so it would be better to split it in three servers, one with the Elasticsearch to search and analyse, other with Logstash that processes the ingested data coming from all the network and Kibana to visualize the data easily with charts and graphs. Backing to the logs collection, the ELK agent collector is Beats that would be installed in every DC and server accordingly with the host specifications. This means that the DCs will have Winlogbeat (windows event logs), AuditBeat (audit data), Filebeat (server logs) and Packetbeat (server network data) and the servers will also have all of them except the Winlogbet.

There are two ways to implement network sensors to get flows, through Test Access Point (TAP), that are hardware devices that are placed in the middle of a network segment accessing and monitoring the network traffic. This method is more appropriated to high-density traffic, this would be ideal to place in gateway 1 since through it will pass all traffic between the network and the internet. I would place it in getaway 9 since this is one of the most dangerous nodes and TAP offers better suspicious traffic detection. The other method is Switch Port Analyser (SPAN) consists in copying network packets from a gateway to the SIEM. (Garland Technology, n.d.) Since the gateway will have to process the tasks for this additional port it will decrease its performance, however, is more appropriate to monitor multiple stations at once ideal for gateways 2,3,7 and 8. These sensors placement will be made in low pick hours and the packets will also be filtered taking in account ethical/legal concerns and accordingly to certain situations, i.e full packet for forensic investigations, session and statistical for normal monitoring operations.

## 2. Statistical Data collection

Session data will contain header information that is used to established the connection between two hosts. This will containmainly information from session layer such as the source and destination IP, which ports were used, what protocols were used (TCP or UDP), the timestamps and the amount of data exchanged in a session. This data must be collected in clients nodes since they give a more detail information of the connections being made between them. Since it has communication information between hosts in a specific protocol we can detect for instance the number of connections from the same source IP to a DC increasing in a substantial way indicating that we could be under a brute force password attack. (Bejtlich, 2008)
Statistical data will contain a lot information of the application layer. This means that information such as and not limited to DNS, FTP and HTTP will be collected. This is more suitable to be used in nodes where the servers are installed. Through this we will for example monitor the number of connections being made to a web server in a given time. If an abnormal amount of connections is detected the server might be under a DDoS attack or volume indicating an exfiltration.

Three locations that would be ideal to collect statistical data is in nodes 4,5 and 6 because they are the server farm nodes. This will enable a statistical analysis of the servers' traffic for instance database connections, web servers, DNS queries, file server downloads, etc.
I would recommend SolarWinds NTA to collect statistical data. This tool enables customization of reports for current and historical network traffic data, detecting high peak bandwidth usage and permits policies adaptation for better management. It can detect bandwidth top talkers across large and busy networks enumerating which endpoints are generating more network traffic causing a

network congestion. The most important functionality is the packet metrics analyse, it enables admins to monitor relevant applications across their IT environments such as SQL servers and web servers using metavalues from the packets rather than the full packet data. This program also enables to create groups based on IP ranges to monitor for instance the DNS traffic of the respective.
The Orion Database and NTA Flow Storage database are advised to be installed on the same SQL server. I would recommend a dedicated server for having these platforms. The servers and router from the above mentioned nodes will have to enable Simple Network Manage Protocol (SNMP) and if they are Windows devices the Windows Management Instrumentation (WMI). The second step is determining IP ranges or individual IP addresses with respective subnets of the devices and their login credentials. After all these steps are done accessing the Orion Web Console we perform a network discovery and add those discovered devices to SolarWinds Network Performance Monitor (NMP). At this point, we can start the monitoring process since everything should be well configured. (SolarWinds, 2020)

## 3. Snort or Suricata

The Suricata engine was released in 2010 as a low-cost multi-threaded tool that is used as an IDS, intrusion prevention system (IPS), network security monitoring (NSM) and offline pcap processing. It detects protocols to perform properly detection and logging logic. Its rulesets are from Emerging Threats Suricata ruleset from Proofpoint and the VRT ruleset from Snort/Talos.

Snort can be used as IPS and NIDS and like Suricata it uses signature detection. It was released in 1998 and was considered one of the “greatest open source software of all time (Dineley, 2009)”. Its rules are from “Community Ruleset” and “Snort Subscriber Ruleset” from Cisco Talos and CrowdStrikes which provide expertise rulesets. It looks at traffic matching its rules and takes actions upon matches however additional software (OpenAppID) needs to be installed to understand its application context using Layer 7 Detectors. (Siemons, 2019)

Snort 3.0 is a multi-thread software, the downside is still on Beta which means it is not fully stable and few bugs may be encountered.

Going a deep further, Suricata can detect automatically the protocols being used in the application layers: dcerpc, dnp3, DNS, HTTP, IMAP, FTP, Modbus, SMB, SMB2, SSH and TLS. This detection is port agnostic Snort also has this capability has mentioned before in their new technology OpenAppID introduced in Snort 3.0. Snort uses whitelist and blacklist to filtrate network traffic while Suricata categorizes them with a reputation score. Suricata for the same packet/stream can set and check flowbits, Snort checks flowbits in the order they appear in the rule, from left to right losing some efficacy in tracking rule states during a transport protocol session<>. Suricata can match files from FTP, HTTP and SMTP streams and log them to disk, Snort also has this functionality. Suricata can invoke Lua scripts to access packets, payloads, HTTP buffers, etc. Snort can set a limit on the number of generated alerts while Suricata cannot, he is limited to 15 alerts per packet/stream. Suricata can store certificates to verify their validity calculating the fingerprints on certain TLS/SSL certificates.

(Suricata.readthedocs.io, n.d.)

Suricata uses payload keywords to inspect the packets' content. The user can make its own payload so that Suricata find similar signatures. The signature check can be configured to detect in all packet or only on specific parts. It is possible to match all printable and non-printable characters. By default it uses case-sensitive matching but can be configured with a modifier to not distinction between uppercase and lowercase characters. There are other multiple modifiers that the user can modify accordingly to its needs: "*depth*" specify how many bytes from the beginning of the payload will be checked, "o*ffset*" which byte in the payload will be checked to find a match , "*distance*" will determine the byte in the payload from which will be checked for a match relative to the previous match, "*within*" will make sure there will only be a match if the content matches with the payload within the set amount of bytes, "*isdataat*" it will look if there is still data at a specific part of the payload, "*dsize*" it will match on the size of the packet payload, "*rpc*" that can be used to match in the SUNRPC CALL on the RPC procedure numbers and the RPC version, "*replace*" can be used in IPs to adjust to network traffic, "*pcre*" and "*fast_pattern*".

(Suricata, n.d.)

Summing up Snort is a well known and recommended tool by network administrators. The disadvantage is its age, however, the recent updates gave to Snort the functionalities needed to keep up with the technology evolution from recent years. Suricata accordingly with its documentation is a more recent IDS having more functionalities such as hardware acceleration (using GPU), file extraction, Lua scripting and log packet context.

**The rest of the business**

ITIL 4 defines a service as: "A means of enabling *value* co-creation by facilitating *outcomes* that customers want to achieve, without the customer having to manage specific *costs* and *risks*.". The integration of this framework in both systems will be summarized. Some associated changes will also be outlined. (Rance, 2019)

So when a SIEM is built accordingly with this framework it will have a cyclic adaptation system to comply with the following constant company changes: compliance requirements, processes, procedures, threats, vulnerabilities, people and personnel, client expectations and service-level agreements (SLAs), creating a self-propelling and self-maturing system. (The State of Security , 2016)

This framework outlines four important concepts and the importance of their delivery services. The first one is *value* defined as "(…) the perceived benefits, usefulness and importance of something.", adding the advised security layers will improve the client's services and their *co-creation* (second concept) with his consumers. This concept will be met since the client's consumers will be more tempted to use their solutions knowing that their provider is a secure company which is concerned in providing high-quality products, services and communication. (ITSM Zone, n.d.) The third is *outcome*, if the value and co-creation are improved consequently this will also be. The fourth one is *managing specific costs and risks*, the changes will have a considerable impact in the company costs since it will require hardware, software, staff training, etc, having some risks associated with such as improper configuration. This last frame seems that only brings disadvantages but the impact suffered from an attack is higher than the cost of securing the network.

The following ITL4 company's practices/processes will be impacted by the implementation of my system:

General management practices

- Architecture management: this practice needs to be revaluated since the network scheme will suffer some changes.
- Information Security Management: CIA triad and other aspects of information security such as authentication and non-repudiation will be much more secure with the introduction of the new system. This will be specifically affected by anti-virus, malware protection and supplier access.
- Change control: this guidance will be modified since the new system will provide help in decision making in IT changes and ensures that risks were assessed properly.

Service management practices

- Incident management to mainly maintain services levels using risk mitigation strategies, meeting service availability requirements for critical services, increase staff efficiency and productivity through the usage of automated tools and improving user satisfaction ensuring that client's consumers are not affected by an incident. https://blog.logsign.com/what-is-itil-incident-management/
- Monitoring and Event Management: the implementation of my system will provide guidance to systematically observe services and service components, and record and report changes of state.

Technical management practices

- Infrastructure and platform management: it will also have an impact in the way of overviewing all infrastructure and platforms used by an organization and its external service providers.

(Knowledge Apple, n.d.)

Given this information, we can see that using ITIL framework to guide the company system and my suggested system implementation we can improve the overall service value system (SVS). These benefits will have an impact in the already established ITIL on the company but they will be more refined.

## 4. Advanced persistent threats (APTs)

I would recommend the conduction of password spraying on network endpoints, DCs, servers and applications. The difference between this attack and brute force is the usage of multiple usernames, avoiding password lockouts, the different platforms being testes will generate alerts by the security tools. This is also used to detect weak login credentials when attackers attempt lateral movements. The second test would be privilege escalation attacks, on endpoints, DCs and servers.

(Pham, 2020) For windows OSs a PowerShell dropper and for Linux a Sudo escalation. It is very important to detect these events since this post-exploitation is the main goal of the attackers. For the applications, firewall and IPS I would test SQL injections and XSS. Social engineering tests should also be conducted to check if filters are detecting for instance phishing emails and if the employees are preceding accordingly with the new policies. These tests can be conducted using the following methods:

- Black Box: limited network knowledge with no extra information,
- Gray Box: some network knowledge such as diagrams and login credentials,
- White Box: network information with some inside accesses such as to server, database and source code.
  (Smith, 2020)

These tests should be performed by certified ethical hackers. It should be performed from the outside of the network to the inside and only part of the security team should know when the penetration test will happen so that the incident response team can be evaluated as well.

One of the most known certification within the ethical hackers is the CEH certification, it is globally recognized as a standard for ethical hackers including the latest hacking and malware tactics. Other good certifications are the following: GPEN, CPT and OSCP. He must be a computer system expert, with very strong programming and computer networking skills capable of performing password guessing and cracking, session hijacking and spoofing, network traffic sniffing, Denial of Service attacks, exploit buffer overflow vulnerabilities and SQL injection. (Tutorialspoint, n.d.) His toolset may include Nmap, Metasploit, John the Ripper, Wireshark, OpenVas, etc.

The first layer of protection will be the firewall which is capable of malware detection. If it managed to avoid being detected the endpoints and servers will also have IPS and anti-virus to detect it via signature-based detection. If successfully are hidden in the host through UEBA abnormal behaviours will be detected and alerts are fired principally if exfiltration, modification of data, lateral and expand access, DDoS attacks, AC bypass attempts and other. (Maayan, n.d.)

## 5. Cost effectiveness

I would recommend two physical servers to increment the virtualization capacity. They will have both 512GB RAM, 800GB SAS 15k (OS, w/Raid1) and 1.2TB SAS 10k (data storage w/Raid 5). It is necessary two 15k disks and six 10k storage disks, costing in total 7120£. (Senetic, n.d.)
ELK servers are virtualized and the software is open-source so no additional cost in its acquisition. This is essential to have real-time visibility across the organization's information security systems.
For the AntiVirus the software that is going to be used is Symantec (10£/user), chosen based on Gartner. This is more directed to the inside of the network detecting and removing malicious software from endpoints with IPS capabilities.
For the SolarWinds NTA with the SL200 plan (2000£). This software is going to collect and analyse the statistical data.
The WAF is going to be applied virtually in the infrastructure. The chosen software will be f5 networks (18000£/y). (Shi, n.d.) WAF protects from third-party software bugs and zero-day vulnerabilities.
(See appendix, Table 1)
The training resources are essential to provide to some employees the knowledge needed to work with the new software. They also need to assist in the products' workshops to keep up with the new updates and industry evolution. The installation and configuration will be almost all made by the software sellers' with a fixed cost.

The human resources that will be needed to monitor and work with these platforms. It is essential to have these analysts to perform triage, incident response and threat hunting. They should also prepare sensibility campaigns to alert from phishing emails, suspicious links, etc. These systems only provide the tools needed to professionals perform their work, so the security of the company will almost depend on their performance.

The installation of these systems will disrupt mainly network traffic. It is important to do a study of the hours which have the lowest network connectivity to minimise as possible the company's operations interruption.

## 6. References


Garlandtechnology.com. n.d. *TAP Vs SPAN | Garland Technology*. [online] Available at: <https://www.garlandtechnology.com/tap-vs-span> [Accessed 29 November 2020].

Redmine.openinfosecfoundation.org. n.d. *Payload Keywords - Suricata - Open Information Security Foundation*. [online] Available at: <https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Payload_keywords> [Accessed 7 December 2020].

Bejtlich, R., 2008. *Network Session Data Analysis With Snort And Argus*. [online] ComputerWeekly.com. Available at: <https://www.computerweekly.com/news/2240100102/Network-session-data-analysis-with-Snort-and-Argus> [Accessed 29 November 2020].

Documentation.solarwinds.com. 2020. [online] Available at: <https://documentation.solarwinds.com/archive/pdf/npm/NPM_Getting_Started_Guide_1_Get_Started.pdf#%5B%7B%22num%22%3A9%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C36%2C741%2C0%5D> [Accessed 29 November 2020].

Dineley, D., 2009. *The Greatest Open Source Software Of All Time*. [online] InfoWorld. Available at: <https://www.infoworld.com/article/2631146/the-greatest-open-source-software-of-all-time.html> [Accessed 29 November 2020].

Siemons, F., 2019. *Open Source IDS: Snort Or Suricata? [Updated 2019] - Infosec Resources*. [online] Infosec Resources. Available at: <https://resources.infosecinstitute.com/topic/open-source-ids-snort-suricata/> [Accessed 29 November 2020].

Suricata.readthedocs.io. n.d. *6.35. Differences From Snort — Suricata 6.0.0 Documentation*. [online] Available at: <https://suricata.readthedocs.io/en/suricata-6.0.0/rules/differences-from-snort.html> [Accessed 29 November 2020].

Rance, S., 2019. *Everything You Officially Need To Know About ITIL 4 | Sysaid Blog*. [online] SysAid Blog. Available at: <https://www.sysaid.com/blog/entry/everything-you-officially-need-to-know-about-itil-4> [Accessed 29 November 2020].

The State of Security. 2016. *Why Do I Need A SIEM (Security Information And Event Management)?*. [online] Available at: <https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/why-do-i-need-a-siem/> [Accessed 29 November 2020].

Knowledge Apple. n.d. *ITIL V4 Management Practices - Knowledge Apple*. [online] Available at: <https://www.knowledgeapple.com/itil-v4-practices/> [Accessed 29 November 2020].

Smith, A., 2020. *Difference Between Black-Box, White-Box, And Grey-Box Testing - Dzone Performance*. [online] dzone.com. Available at: <https://dzone.com/articles/difference-between-black-box-white-box-and-grey-bo> [Accessed 29 November 2020].

Maayan, G., n.d. *How To Prevent And Detect APT Attacks By Gilad David Maayan*. [online] Hakin9 - IT Security Magazine. Available at: <https://hakin9.org/how-to-prevent-and-detect-apt-attacks/> [Accessed 29 November 2020].
Senetic. n.d. *HPE P02464-B21 Agora O Desconto 35% DL380 Gen10 4210 1P 32G 8SFF Svr*. [online] Available at: <https://www.senetic.pt/product/P02464-B21> [Accessed 29 November 2020].

Shi. n.d. *BIG-IP Add-On Advanced Web Application Firewall (WAF) | Www.Shi.Com*. [online] Available at: <https://www.shi.com/product/35122510/BIG-IP-Add-On-Advanced-Web-Application-Firewall-(WAF> [Accessed 30 November 2020].

## 7. Appendix

| Server | CPU Cores | RAM (Gb) | Partition 1 OS (Gb) | Partition 2 Software (Gb) | Partition 3 Data Storage (Logs) (Tb) |
|---|---|---|---|---|---|
| Elasticsearch | 4 | 16 | 100 | 100 | - |
| Logstach | 8 | 32 | 100 | 100 | 3 |
| Kibana | 4 | 16 | 100 | 100 | - |
| AntiVirus | 8 | 32 | 100 | 250 | 0.5 |
| SolarWinds | 8 | 16 | 100 | 150 | 0.5 |

Table 1 – *Virtual Server Resources*