MR SIM XIANGYUAN, IT3552-01

Practical Assignment: Exploitation Discovery

It3552 – Cybersecurity project

Dennis Ng Han jie, 204461H

# Enterprise Security Solutions

## IPS & IDS

One of the enterprise security solutions that can be used to mitigate CVE-2019-1388 (Privilege Vulnerability), and CVE-2019-0708 (BlueKeep) is by implementing an intrusion detection system (IDS) and an intrusion prevention system (IPS), preferably together in one to reduce latency. It would also be advisable to have both host-based IPS & IDS, and network-based IPS & IDS in the security architecture.

By having an IPS & IDS such as Suricata or Snort, it would be able to constantly monitor the system or network depending on where it is implemented, for any malicious activities due to the rules that are implemented into these tools. By matching the traffic against the conditions of the rules, the IDS will be able to detect attempts of an attack on the network or the computer and notify the respective personnel immediately, however by itself it would not be able to prevent attacks. Therefore, together with an IPS is needed, as only an IPS can stop it. Thus, it is preferable if it is implemented together into one tool to help reduce the latency of needing to send the alert from the IDS to the IPS to tell it to stop the attack.

Hence, by implementing a network-based and a host-based IDS, it will also be able to detect and log the attacks, for instance it would log the remote desktop connection used for CVE-2019-0708 or log the privilege escalation attempt for CVE-2019-1388. This allows incident responders to track their IP address and create an audit trail of what the attacker did during the attack, and know which computers were affected. Additionally, the network-based and host-based IPS will also be able to stop the attacker from continuing its attack by blocking remote desktop connections or any data exfiltration attempts.

## Vulnerability Scanner

Vulnerability scanners can also help in mitigating CVE-2019-1388, and CVE-2019-0708.

A vulnerability scanner such as Nessus, will be able to scan through all systems on the network. It will scan for any vulnerabilities such as misconfigurations, default passwords, missing patches, or open ports. After scanning, it will generate a report for the administrator to view, the vulnerabilities will also be organized into the severity level of the vulnerability, Critical, High, Medium, Low, and Info (Tenable, Nessus 10.4.x User Guide, n.d.), allowing the administrator to know which vulnerabilities needs to be resolved first.

Thus, it would be able to detect that port 3389, which is used for Remote Desktop Protocol (RDP), is enabled, allowing for the exploitation of CVE-2019-1388. It would also therefore be able to detect that the patches to resolve the vulnerabilities for both CVE-2019-1388, and CVE-2019-0708 are missing.

However, it will only notify the administrator about these issues, and will not be able to fix them on its own. Thus, a patch management tool should be accompanied with a vulnerability scanner.

## Patch Management

Instead of updating the systems one by one manually, a patch management tool should be implemented into the enterprise security architecture to handle the updating. A patch management tool such as Symantec Altiris Patch Management will be able to apply patches to computers remotely, schedule the patches, and automate these updates. They are also able to detect which patches are missing, and list out the vulnerabilities that the patches fix, such that the administrator would know immediately which updates should be applied while also letting them know about the vulnerabilities that the patch is fixing. By doing so, they can update the machines as soon as possible.

Microsoft have already provided updates to mitigate the CVE-2019-1388 (Tenable, KB4525232: Windows 10 November 2019 Security Update, 2019), and CVE-2019-0708 (Cimpanu, 2019) exploitations, thus by applying these patches, these vulnerabilities will be removed.

Furthermore, Nessus (Tenable, Nessus 10.4.x User Guide, n.d.) can integrate with Symantec Altiris Patch Management. Thus, Nessus can be used to scan for vulnerabilities that the IT infrastructure is vulnerable to, and then make use of Symantec Altiris Patch Management to apply the patches to fix these discovered vulnerabilities, making it easier for administrator to manage.

## File Integrity Monitoring

One other solution would be to implement a tool that is able to do File Integrity Monitoring (FIM). With FIM, it will be to detect if there any files that are modified, deleted, or added in the system. This is done by verifying the integrity against a baseline that was set beforehand, and if any changes were to be detected, it would send an alert to the respective administrator to notify them immediately.

Since CVE-2019-1388 is an exploit that allows attacker to establish a remote connection to their target, allowing them to have remote access to the system, and CVE 2019-0708 being an exploit that grants the user administrative privileges, they can then modify the files on the system as they wish. They could also upload a file onto the system to maintain access to it. However, these modifications or files uploaded in the system will immediately be detected by the FIM, sending alerts to the administrator. Thus, the victims will be able to easily remove the malicious files, and know which files were affected so that they can recover them promptly, and hence they would not be greatly affected by the attack.

The malicious files that were uploaded and detected by the FIM can also be sent for further analysis to gain more information about the attacker as well, as some attackers tend to use the same malicious files for their attacks, thus the incident response team may be able to determine who was the attacker.

Therefore, FIM tools such as Wazuh are extremely useful in minimizing the impact of cyberattacks due to giving the users the ability to detect the malicious files that were uploaded, and determining which files were affected by the attack, allowing a swift recovery of the system.

## Firewall

Another solution would be the implementation of Firewalls. Firewalls such as pfSense or Sophos, will be able to prevent attacks that make use of network connections such as CVE-2019-1388. This is due to having the ability to implement rules that block ports, and filtering IP addresses. Thus, by blocking the port 3389, CVE-2019-1388 will be prevented as port 3389 is used for the Remote Desktop Protocol, which is needed for the exploitation to work. However, if port 3389 is needed, Firewalls also provide the ability to filter out IP addresses such that we can make a whitelist of allowed IP addresses to be able to use that port. Thus, preventing outsiders from being able to attack the network.

Next Generation Firewalls also provide the ability to monitor the packets that are going in and out of the network through Deep Packet Inspection. This allows the firewall to determine if the traffic is malicious or not, and if it is malicious, the packets will be dropped. They also provide the ability to filter packets based on the application, for instance, it can block traffic going to or comes from Facebook.com.

Thus, even if CVE-2019-0708 were to be exploited, by implementing a whitelist of sites the network can access, and using Deep Packet Inspection, the attackers would not be able to download malicious files, or exfiltrate data out from the systems, helping to minimize the impact of the CVE-2019-0708 vulnerability.

# Enterprise Security Architecture & Implementation Plan

Diagram

Description automatically generated

Figure Enterprise Security Architecture

Diagram, schematic

Description automatically generated

Figure Network Architecture

In reference to Figure 2, for the implementation plan, firstly, servers that should be accessible to the public such as DNS servers, web servers, or file servers should be placed outside the network, and surrounded by two firewalls, namely PfSense firewall and Sophos firewall. By doing so, it ensures that even if those servers were to be compromised, the internal network will not be affected. Furthermore, by having two firewalls, the attacker must bypass both firewalls rather than just one, hindering the attacker. Rules such as blocking of unused ports and services should also be configured, doing so will minimize the attack surface of the network. For instance, by blocking port 3389, which is used for Remote Desktop Protocol, it will be able to mitigate CVE-2019-1388. Additionally, by using firewalls of different brands, it will minimize the chances of an attacker using the same exploit to bypass both firewalls.

Secondly, the Suricata network IPS & IDS should be placed right after the Sophos firewall, this enables it to be able to monitor all traffic that are to go in and out of the network as it is placed on the border. Thus, it will detect any malicious traffic and immediately stop it before it can even traverse in or out of the internal network.

Thirdly, the Symantec Altiris Patch Management, along with Nessus Manager should be installed on the Windows Server. Nessus Manager can integrate with Symantec Altiris by configuring the patch management options in the Credentials section, allowing it to perform patch auditing (Tenable. (n.d.). *Nessus 10.4.x User Guide*). Thus, any missing updates will be detected by Nessus Manager, and the Patch Management can be immediately used to deploy them, helping to patch vulnerabilities such as CVE-2019-1388, and CVE-2019-0708. Nessus agents should also be installed on all hosts to allow Nessus to scan for vulnerabilities on all hosts, preventing any misconfigurations or vulnerabilities on the hosts which can be used to the attacker’s advantage.

Fourthly, the Wazuh Indexer and Server should be installed on a machine that has Ubuntu OS or any Linux distribution as it is only compatible with them. After installation, File Integrity Monitoring should be enabled, integrate with VirusTotal, and configure the Active Response and Alerts. This allows Wazuh to monitor for any files that were added, modified, or deleted, and upload them to VirusTotal to check if it is malicious, and react accordingly. By doing so, it will detect any changes made to files, ensuring integrity. It is also able to detect malicious files by uploading the hashes of any files that were added to VirusTotal such as those that make use of the CVE-2019-0708 exploit. Wazuh will then be able to remove the file immediately if configured to do so, while also alerting the administrator about the event. Wazuh agents should also be installed on all the other hosts as well and connect them to the server, allowing the administrator to monitor the logs on the Wazuh server rather than checking them manually. Furthermore, there should be a backup Wazuh system in case the first one was to go down, ensuring resilience.

Lastly, Snort host IPS & IDS should be installed on all client machines. In addition to the network IPS & IDS, Snort will monitor malicious activity that happen on the host machines instead. This is to prevent attacks that do not occur through the network, for instance, insider attacks. Thus, there will be another layer of defense in the event of an attack.

With this implementation, defense-in-depth will be assured as there are multiple tools protecting the same attack vector, so even if one tool is unable to prevent the attack or were to go down, another tool will be in place to prevent it and helping to ensure the confidentiality, integrity, and availability of the whole system.

# References

Cimpanu, C. (14 May, 2019). *Microsoft May 2019 Patch Tuesday arrives with fix for Windows zero-day, MDS attacks*. Retrieved from Zdnet: https://www.zdnet.com/article/microsoft-may-2019-patch-tuesday-arrives-with-fix-for-windows-zero-day-mds-attacks/

Tenable. (12 November, 2019). *KB4525232: Windows 10 November 2019 Security Update*. Retrieved from Tenable: https://www.tenable.com/plugins/nessus/130903

Tenable. (n.d.). *Nessus 10.4.x User Guide*. Retrieved from Tenable: https://docs.tenable.com/nessus/Content/RiskMetrics.htm

Tenable. (n.d.). *Nessus 10.4.x User Guide*. Retrieved from Tenable: https://docs.tenable.com/nessus/Content/PatchManagement.htm