**0421-EH-Assignment-Team-Project Document**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No. | Team Name | Team Member (Full name)  Put a (-L) to indicate Team Leader | Class  (ISF01/02/03) | Private Phone Contact | Project Title | Outline | Tutor’s Feedback and Endorsement |
| 1 | wat name | Ewen Keck | CSF 01 |  |  | **Case Scenario**  It is 2077, a startup video vendoring company known as CoolHipBTSBlackPinkOneDirectionTameImpala Video. They typically sell shows about frogs that can fly and a dolphin with a dream to have his own space program powered by whale farts. Given that streaming services require large amounts of storage for file server capabilities to store the large amounts of video and user information. In these trying times of Covid-19, another streaming platform known as Deuche Bjåg was jealous about the success that CoolHipBTSBlackPinkOneDirectionTameImpala was having and wanted to foil their reputation by performing Corporate Espionage and bribed an insider to carry out their misdeeds.        **Summary of Attacks**   1. Hack internal WinServer 2012 using:    1. MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution 2. Create stagefright\_mp4\_tx3g\_64bit APK and reverse\_tcp shell apk 3. Using chromium exploit to spoof malicious apk 4. Remote into windows 7 using bluekeep vulnerability   **Pen-Test Environment Setup**  Victim  1 Windows Server 2016  1 Windows 7  1 Android 8.1.0  Whisk thoroughly    Attacker  1 Kali Linux Virtual Machine      **Network Diagram**  [tmr]        **Post Exploitation Activities**   1. Access the web Hosting aspect of Windows Server 2012 and place a malicious spoofed html page 2. Extract user information via APK(s) 3. Obtain and leak user's information via a hacked windows 7 pc belonging to the CEO to frame CEO | What is AWDL? Outline too brief. See previous year sample. |
| Lucas -L |  |
|  |  |  |
| 2 | Team Shampoo | Tan Wen Hao | CSF01 |  |  | **Case Scenario** Conan has been a Security Analyst at JP Sachs for the past 10 years until he was recently retrenched during the pandemic. Unhappy that he was made to leave immediately and unable to keep copies of his work for his portfolio, he contacted Team Shampoo to access the company’s file server and retrieve confidential documents for him. Conan gave Team Shampoo some basic information about the company’s network layout and software versions of the File Server and Workstations. From there, Team Shampoo researched online for vulnerabilities affecting the software and exploited them to help Conan retrieve the files. **Setup**  Attacker machine   * Kali Linux 2021.1 VM   Victim machines   * Windows 7 * Windows Server 2003 (Company’s File server)  **Network Diagram**   **Exploited Vulnerabilities**  * *Remote Access*   + *CVE-2019-0708*     - [*https://www.cvedetails.com/cve/CVE-2019-0708/*](https://www.cvedetails.com/cve/CVE-2019-0708/)   + *CVE-2017-0144(EternalBLue Exploit)*     - Could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server.     - [*https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf*](https://www.cisecurity.org/wp-content/uploads/2019/01/Security-Primer-EternalBlue.pdf)     - [*https://www.cvedetails.com/cve/CVE-2017-0143/#:~:text=CVE%2D2017%2D0143%20%3A%20The,7%20SP1%3B%20Windows%208.1%3B%20Windows*](https://www.cvedetails.com/cve/CVE-2017-0143/#:~:text=CVE%2D2017%2D0143%20%3A%20The,7%20SP1%3B%20Windows%208.1%3B%20Windows)   + [CVE-2019-0708](https://www.cvedetails.com/cve/CVE-2019-0708/)     - <https://www.cvedetails.com/cve/CVE-2019-0708/>     - Windows Server 2003 Vulnerability     - A remote code execution vulnerability exists in Remote Desktop Services: when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'. * *Escalation of Privileges*   + [CVE-2021-31956](https://www.cvedetails.com/cve/CVE-2021-31956/)     - [*https://www.cvedetails.com/cve/CVE-2021-31956/*](https://www.cvedetails.com/cve/CVE-2021-31956/)     - Windows NTFS Elevation of Privilege Vulnerability     - Exploitation for Windows 7  **Post-Exploitation Activities**  1. Escalation of Privileges 2. Disabling Security Software (firewall or anti-virus) 3. Data Exfiltration of the server/workstation 4. Screenshare 5. Obtain user and server credentials 6. Clear log files |  |
| Seah Le | CSF01 |  |
| Kervin Ong Guan Cheng | CSF01 |  |
| Matthias Gan | CSF03 |  |
| 3 | Team UTee | Lee Wei Jie -L | CSF02 |  | Exploiting Microsoft Exchange Server RCE and Zerologon | Case Scenario Jordan Schlansky is a disgruntled employee that worked tirelessly at a dead-end job for 10 years. He decided that finally he had enough. He confronted his boss and demanded for a promotion and pay-raise but was instead laid off. In disbelief and resentment for his boss, he went into a raged-filled conquest to seek revenge for his wrongful dismissal. Jordan snuck out his Windows 10 workstation (company-owned laptop) before leaving the company building. The network administrator has not removed Jordan’s credentials and he is still able to log into the company network when in close proximity to the building. Jordan also has his own workstation at home that runs Kali-Linux. Pen-Test Environment SetupSetup Attacker Machines  Kali Linux 2021.1 VM  Windows 10 VM (Company-Owned)  Victim Machines  Windows Server 2019 VM  Microsoft Exchange Server 2019 VM Network Diagram  Tasks OutlineExploited Vulnerabilities  * CVE-2020-1742 (Zerologon)   + <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472>   + <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472> * CVE-2020-0688 (Microsoft Exchange Validation Key Remote Code Execution Vulnerability)   + <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0688>   + <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-0688>  Post-Exploitation Activities  1. Data exfiltration (credential dumping) 2. Command and control (PowerShell Empire) 3. Establishing persistence 4. Privilege Escalation 5. Uploading of malicious files into server |  |
| Bradley Goh | CSF02 |  |
|  |  |  |
| 4 | Team H@cks4Lyfe | Aloysius Goh Guan Teng | CSF02 | 90090439 | Exploiting Apache Tomcat | **Case scenario**  Naas and Brothers, a banking firm, operates its network through the use of a Apple AirPort Time Capsule Wireless Access Point and a pfSense Router. It has recently been found to be underpaying and mistreating staff. As a result, its CISO has been replaced recently who, prior to that, has been making many poor security decisions. Unhappy with being sacked, the CISO contacted us, Team H@cks4Lyfe to hack Naas and Brothers as an act of revenge.  Using Evil-Twin attack on the WAP, we gain access to the network. From there, we try to exploit the router which can be used to access the internal network. Afterwards, we should be able to discover servers in the network such as the web server - TomCat version 8.5, which we are able to exploit as well.  **Setup**   * Windows Server 2019 as the Web Server running on Version 8.5 of Apache Tomcat * Windows Server 2008 as the File Server * Router * Kali Linux 2021.1 (Attacker machine) * Apple AirPort Time Capsule as the Wireless Access Point   **Exploitation**   * Evil-Twin on Access Point * CVE-2017-12617 (TomCat - v8.5)   + <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12617> * CVE-2016-10709 (pfSense - v2.3) - Subject to Change   + <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10709> * CVE-2018-14847 (MicroTik Router) - Also Subject to Change. Either this or the above.   + <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14847> * MS09-050   + <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-050>   **Network Diagram**    **Post-Exploitation Activities:**   1. Command & Control (PoshC2) 2. Data Exfiltration 3. Keylogging 4. Disruption of Web-Hosting (Delete Web-related Files, Replace with Phishing, etc) 5. Malware Infection of File Server/Upload of Malware into File Server 6. Packet Interception/Sniffing | 1) Please be careful not to cross over into WAPT. Pentest web server itself is OK but not the web application.   2) Do plan early on demo on Wireless hack as it can be tricky if done through online. Same for your video deliverables. Points to think about. |
| Teo Shi Jie | CSF02 | 97571304 |
| Preamraj S/O Subramaniyam -L | CSF02 | 96302415 |
| 5 | Team Sushi | Gerron Lee Yan Fong | CSF02 |  | Exploitation of Remote Desktop Protocol (RDP) on Windows 7 and Windows Server 2003 | **Case Scenario** James is a system administrator at ABC company. One day, he received an email from Tom, an intern assigned to him, saying that he had to reset his workstation due to some error and he disconnected from the company’s Wi-Fi password, thus he needed the password to do his work. In reality, this email was from an attacker, Zack, that had hacked into Tom’s email account. James, thinking that the email was from Tom, then sent the password to him. Therefore, Zack now had access to the company’s internal network.  Using this information, Zack will be able to gain access to the Wi-Fi and conduct various scans to figure out the IP address of James’s workstation and the company’s server. From there, he would be able to gain unauthorized access using vulnerabilities found in “Remote Desktop Protocol” and proceed to escalate his current privileges. This would enable him to conduct various malicious activities, such as disabling security software, injection of malicious files and data exfiltration. **Setup**   * Kali Linux (Attacker machine) * Windows 7 (Victim machine) * Windows Server 2003 (Company’s File server)  **Network Diagram**   **Exploited Vulnerabilities**  * Remote Access   + CVE-2019-0708 (For Windows 7 and Windows server 2003)     - <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708>     - <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2019-0708> * Escalation of Privileges   + CVE-2015-2365     - <https://www.cvedetails.com/cve/CVE-2015-2365/>     - <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-073>   + CVE-2020-17087 (For Windows 7)     - <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17087>  **Post-Exploitation Activities**  1. Escalation of Privileges 2. Disabling Security Software (firewall or anti-virus) 3. Injecting malicious files into the server    1. Usage of EICAR Test Files 4. Data Exfiltration of the server/workstation |  |
| Jewel Jace Lim | CSF02 |  |
|  |  |  |
| 6 | Team Cyberskulls | Mansoor Siraj Bin Osman | CSF 02 |  | Insider Threats in Corporate Network | **Case Scenario:**  Xiao Boh Boh is an employee currently under A&M Technologies Pte Ltd. While he is employed in the company as an Administrative Assistant, Xiao Boh Boh is also an adept hacker. As an experienced member of the working team, Xiao Boh Boh has tried multiple times to negotiate for a pay raise. However, these requests were revoked, citing his horrible work attitude as the main reason.  This angered Xiao Boh Boh greatly. After negotiations for a pay raise fell through for a fifth time, Xiao Boh Boh made the decision to launch a variety of attacks on the company’s internal network. He wishes to target his boss, Mr Anas in hopes of stealing as much information as possible and crippling his business. As an employee of A&M Technologies, Xiao Boh Boh is well aware of the internal network topology and the company’s security posture. Using this information, he will be launching attacks from a remote location (his home) as well as from his workstation on-site of A&M Technologies.  **Network Diagram:**    Devices Used:  1) WAP  2) Workstation (Ubuntu VM) (Windows 10)  3) FTP Server (Ubuntu VM)  Exploits Used:  1) WAP   * Evil Twin using Evil-Twin-Tool.py   2) Workstation   * LibreOffice RCE (CVE-2019-9848) * MSWord Buffer Overflow (CVE-2017-11882) * MiTM using Ettercap * Local Privilege Escalation via Polkit (CVE-2021-3560)   3) FTP Server   * Buffer Overflow * Brute-Forcing FTP Credentials * *ProFTPD Mod\_Copy* Command Execution (CVE-2015-3306)   Post-exploitation:  1) Establishing a persistent C2 Server  2) Credential Harvesting  3) Clearing Tracks and Logs  4) Pivoting to other devices in the internal network  5) Setting up Phishing sites |  |
| Aidil Farhan Bin Amran |  |  |
|  |  |  |
| 7 | Team “Re-Exec” | Rifa Achrinza | CSF02 |  | Insider threat with ZeroLogon vulnerability. | **Case Scenario:**  John Doe is a disgruntled ex-employee at ACME Corporation. He has been recently dismissed from the corporation and has had all his credentials recently revoked. John Doe was part of the I.T. department and hence has some additional knowledge on the company’s internal infrastructure and patching schedules. As such, he leverages this knowledge to discover 2 CVEs that the organisation is vulnerable to, thereby enabling him to create a kill chain as a persistent threat actor (PTA) to exfoliate data and perform a ransomware attack on the organisation.  John decides to leverage his general knowledge on I.T. to craft a special OpenDocument file with a Python script that would trigger an arbitrary remote code execution (RCE) vulnerability in the vulnerable LibreOffice version and send it via a spoofed email of which its FROM header will not be validated. The spoofed email is sent to Sam, one of his ex-colleagues. Sam worked in the same department as John and held similar access privileges. He will then utilize the ZeroLogon vulnerability to spoof his identity as other users to evade detection, and gain privilege escalation to internal and external services used by the organisation and linked via SSO or stored in the Bitwarden password manager server. The FSMO Master Controller is discovered via the Read-Only Controller with the privileged credentials. Additional credentials of external services are harvested from the Bitwarden password manager. Data exfiltration from the email and NextCloud server, and persistent, lateral movement is achieved with GPO.  **Network Diagram:**    **Environment Setup (Devices Used):**   * Windows Server 2019 * Windows 10 * LibreOffice 6.2.4 (<https://downloadarchive.documentfoundation.org/libreoffice/old/6.2.4.2/>)   **Exploits used:**  **LibreOffice RCE** – CVE-2019-9848   * An exploitation of the LibreOffice feature where documents can specify that pre-installed scripts can be executed on various document events such as mouse over, etc. This vulnerability exists due to LibreLogo, which is typically bundled with LibreOffice, a programmable turtle vector graphics script, which can be manipulated into executing arbitrary python commands.   **ZeroLogon** – CVE-2020-1472   * An elevation of privilege vulnerability where an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC).   **Inherent Vulnerabilities Used:**   * Many organisations do not leverage an *enforced DMARC policy* with *SPF* and *DKIM* on their domains. This means that email clients do not have a method to cryptographically verify the authenticity of the email origins and content authenticity. Hence, threat actors can leverage this weakness to spoof an internal email address for the email’s FROM header, thereby creating implicit trust with the victim. * Many services used by an organisation leverage SSO; This means identical credentials are used for the same user, thereby allowing compromised credentials to be leveraged for identity spoofing and gaining elevated privileges.   **Post Exploitation:**   * Credential harvesting via Bitwarden password manager * Persistence command and control (C2) scripting through WMI (Windows Management Instrumentation) * Data exfiltration & encryption * Horizontal movement via GPO deployment |  |
| Lim Jun Hao | CSF02 |  |
|  |  |  |
| 8 | Team Laksa | Bryan Lee Yixian | CSF02 |  | CVE-2019-0708  CVE-2017-0143 | Case Scenario:    Mike is an employee of a small company, XYZ Technology Pte Ltd. One day in the morning, he found out the network in the system had some connections issues and the company could not solve it. The boss then asked Mike to find for a cheap network repair company fix it. Mike contacted the cheapest one he could find online and arranged for him to come down in the afternoon.  The repairman, Ben, came down and got down to work. However, he was actually a black hat hacker and is installing a program to install onto the system. After Ben was able to fix the problem and install the malware, he now establishes a remote connection into the network. He can use this connection to harvest the company’s confidential data, track their activity on their devices, and escalate their privileges to gain admin rights.  Network Diagram:    Devices used:   1. Windows 7 Machine 2. Windows Server 2016 Machine 3. Kali Linux Machine 4. Windows 10 Machine   Exploits used:   1. CVE-2019-0708 (Remote Code Execution, Windows 7)    1. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708> 2. CVE-2017-0143 (Remote Code Execution, Windows Server 2016)    1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0143> 3. CVE-2019-0796 (Remote Code Execution, Windows 10)    1. <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2020-0796>   Post-Exploitation Activities:   1. Data Exfiltration 2. Privileges Escalation   BadBlue Passthru Exploit   * 1. Windows 7- <https://54m4ri74n.medium.com/windows-7-privilege-escalation-using-uac-bypass-b08f5523b7de>   CVE-2019-1458   * 1. Windows 10 - <https://www.cvedetails.com/cve-details.php?t=1&cve_id=cve-2019-1458>  1. Disabling Security Software 2. Key Logging 3. Ensuring Persistence |  |
| Ng Tianyu Jerric |  |  |
| Neo Say Ping |  |  |
| 9 | Team Bread | Dainel Koh Chye Lek | CSF01 |  | Android & Windows Exploitation | **Case Scenario**  Ken is a cybersecurity student. His father, Mr Lim, owns a small company. Ken decided to test his pen-testing skills on his father’s company computer system. To save money, Mr Lim did not upgrade the server and computer systems. He also did not hire professional IT personnel to ensure that the server and computer systems are patched and configured securely.  Ken managed to obtain the company’s network from the administrator personnel during his visit there. He also found out that there is a company’s phone used to contact their clients.  Zerologon (CVE 2020-1472)  **Workstations**   1. Kali Linux (Attacker machine) 2. Windows Server 2012 R2 3. Windows 7 4. Android Oreo   **Network Diagram**    **Post-Exploitation Activities**   1. Pivoting 2. Establishing Persistence 3. Keylogging 4. Spy on victim machines 5. Stealing credentials |  |
| Ng Shu Hyan | CSF01 |  |
|  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | Team Ananas | Muhd Anas | CSF02 | 91090291 | Diving into Remote Code Execution Attacks and Android Device Exploits | **Case Scenario:**  Mdm Da BoBo, CEO of Royal Maggie Silks, has contracted Mdm Sangeetha as a spy to infiltrate into her rival’s company, Rupini’s Textiles’ network. Mdm Sangeetha is a skilled ethical hacker with a certificate from Bombay University. To accomplish her task, Mdm Sangeetha managed to be hired as an employee of Rupini’s Textiles and thus has access to their network.  In her short time in Rupini’s, she realizes that Rupini’s has poor implementations of IT Security. The boss is known to be stubborn, refusing to invest in her IT infrastructure. With her experience in Ethical Hacking, she carries out both passive and active reconnaissance to gather information regarding the IT habits of the employees at Rupini’s, types of operating systems and security solutions used in their network. With this knowledge, she uncovers each of her target’s vulnerabilities and uses the necessary exploits to gain unauthorized access to the machines that she uncovers from the reconnaissance stage.  Our assignment will cover how Mdm Sangeetha manages to uncover sensitive information for her boss, Da BoBo, from the company’s systems.  **Parties Involved**  Mdm Sangeetha → Attacker  Rupini’s Textiles (Rupini’s) → Target Company  Rupini’s Boss → Main Target  **Project Outline:**  The following section will cover all exploits and post exploits covered by our team to gain information on Rupini’s systems.  **First Phase (Reconnaissance):**  Conduct Passive Recon on Rupini’s  Mdm Sangeetha has to find out:  Rupini’s IT culture  Rupini’s Boss Working Hours  Rupini’s Boss Phone Model  Timing of when Rupini’s Boss is likely to use her devices (phone and laptop)  Check for commonly used applications in Rupini’s on her own company-given device  Conduct Active Recon on Rupini’s Systems  Nmap scans on the company’s network  Find out devices running on network  TCP Scan  ACK Scan and many more  Find out version and OS of devices found on the network  OS fingerprinting  **Second Phase (Breaking in):**   * + - 1. Mdm Sangeetha has to gain access into devices found in the company’s network.          1. From her Kali Linux BYOD,   **Mdm Sangeetha shall exploit CVE-2019-16724** that is found in File Sharing Wizard (1.5.0) to gain access to the Windows 7 computer belonging to the boss.  **Mdm Sangeetha shall exploit CVE-2020-6418** that is found in Google Chrome builds prior to 80.0.3987.122 to gain access to the Windows 10 computer belonging to the manager.  **Mdm Sangeetha shall exploit CVE-2020-0796** named CoronaBlue to allow RCE onto the File Server in the company’s network.  *The details of the exploits and CVEs are listed below in the “Vulnerabilities” section*   * + - 1. For breaking into Rupini’s Boss Android device,          1. *Mdm Sangeetha has to have in mind the following first before she can do so:*   *Timing of when Rupini’s Boss uses her phone.*  *When she turns on her Android’s Bluetooth to listen to music*  Mdm Sangeetha shall make use of the timings to conduct Android attacks.   * 1. From her Kali Linux BYOD,      1. **Mdm Sangeetha shall exploit CVE-2020-0022,** named BlueFrag to exploit Rupini’s Boss android phone Bluetooth capability to allow RCE.      2. If that fails**, Mdm Sangeetha shall exploit CVE-2020-8899,** named Samsung Qmage MMS Exploit.   **Third Phase (Post Exploitation):**  Post Exploit Objectives  Mdm Sangeetha will find and extract the files that are related to Rupini’s Textiles’ client as well as extract their company’s supplier information and send the sensitive information to the rival’s company (Royal Maggie Silks).  **Post Exploitation Activity**  SERVER AND WORKSTATION POST EXPLOIT   1. Information Gathering 2. Elevation of Privileges by Exploiting NTLM Hashes 3. Data Exfiltration (Server and Workstation) 4. Keylogging    1. Monitor all user keystrokes on the Windows 7 VM 5. Covering tracks (Log deletion) 6. Pivoting 7. Credential Harvesting using Ettercap 8. ARP Poisoning   ANDROID POST EXPLOIT   1. Webcam Hijack using Attacker’s Android Phone (MSF)    1. Monitor the target PC live from the attacker’s Android device 2. Install Malicious APK using MSFVenom (Backdoor Attack)   **Vulnerabilities**  ***1.Workstation***  Target: Windows 7 VM  **Exploit: File Sharing Wizard (1.5.0)**   * Main Vulnerability: **CVE-2019-16724** * Allows a remote attacker to obtain arbitrary code execution by exploiting a Structured Exception Handler (SEH) based buffer overflow in an HTTP POST parameter   Target: Windows 10 VM  **Exploit: Google Chrome Remote Code Execution POC**   * CVE-2020-6418 * Type confusion in V8 in Google Chrome prior to 80.0.3987.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.      1. ***Server***   Target: Windows Server 2019 (File Server)  **Exploit: CoronaBlue**   * Main Vulnerability: **CVE-2020-0796** * It is a wormable Remote Code Execution (RCE) vulnerability that is exploited by sending a specially crafted packet to a targeted SMBv3 server. The attacker does not need to be authenticated for this exploit.   **Exploit: SMBleed**   * Main Vulnerability: **CVE-2020-1206** * This primarily takes advantage of the Sever Message Block (SMB) communication protocol decompression function and allows us to read its kernel memory remotely and edit the compression function.  1. ***Android***   Target: Android 7.0 Nougat  **Exploit: BlueFrag - an Android Bluetooth Zero-Click RCE**   * Main Vulnerability: **CVE-2020-0022** * Bluetooth packets are processed by the Bluetooth chip (also called a controller), and then passed to the host (Android, Linux, etc.). Both, the firmware on the chip and the host Bluetooth subsystem, are a target for Remote Code Execution (RCE) attacks * The initial flaw used for this exploit is still present in Android 10, but when utilizing an additional bug in Bionic (Android’s libc implementation), it makes exploitation way easier.   **Exploit: Samsung Qmage MMS Exploit**  - Main vulnerability: **CVE-2020-8899**  - There is a buffer overwrite vulnerability in the Quram qmg library of Samsung's Android OS versions O(8.x), P(9.0) and Q(10.0). An unauthenticated, unauthorized attacker sending a specially crafted MMS to a vulnerable phone can trigger a heap-based buffer overflow in the Quram image codec leading to an arbitrary remote code execution (RCE) without any user interaction. The Samsung ID is SVE-2020-16747.  **Setup:**  *Victim Machines*   1. Windows 10 VM 2. Windows Server 2019 VM (File Server) 3. Android 7 Nougat   *Attacker Machines*   1. Kali Linux 2021.1 VM 2. Android Phone 9 Pie   **Network Diagram:** |  |
| Sarah Do | CSF02 |  |
| Tan Jia Shun -L | CSF02 |  |
| 11 | Team Green | Ezra Ho Jincheng -L | CSF03 |  | CVE-2019-0708 (Windows RDP)  CVE-2021-3560 (Polkit vulnerability) | Case Scenario:  Pen-Tester is tasked a grey-box penetration testing job. We will be using LogMeIn Hamachi program to aid in our assignment, simulating an over-the-internet attack. However, this is much safer for the host machines as it does not directly expose the machines to the malicious behaviors the Internet offers. It is also much like port forwarding, but in a more secure manner.  LogMeIn Hamachi is a hosted VPN service which requires each of the systems to be authenticated to be allowed access into a “network”. The “network” can either be hosted in a Mesh, Hub-and-Spoke, or Gateway configuration.  Project Outline:  It was not permitted on the company side to scan their servers. However, we are allowed permission to scan the Windows 10 Administrator device and a Ubuntu Linux machine.  Network Diagram:    Setup:  Attacker Kali Linux: Kali Linux 2021.1  Company Windows 10 Admin: Windows 10 Pro, Version 1607  Company Linux PC: Ubuntu 20.04.20  CVE Details:  CVE-2021-3560 (Polkit Vulnerability)   * + <https://www.whitesourcesoftware.com/vulnerability-database/CVE-2021-3560> * CVE-2019-0708 (Windows RDP)   + <https://www.cvedetails.com/cve/CVE-2019-0708/>   Post-Exploitation Activities:   1. Information Gathering 2. Creating and Modifying User Accounts 3. Escalated Privileges 4. Data Exfiltration 5. System Passwords |  |
| Hannah Leong Jia Wen | CSF03 |  |
| 12 | Team thesaurus | Chia Kai Zer | CSF03 |  | CVE-2017-0143  CVE-2008-4250 | Case Scenario: George owns a small e-commerce company. To test the current network security measures George has decided to hire a small team of pen-testers to penetrate into the network. The pen testers are tasked to test the vulnerabilities in the network and gain access to the server and the workstation.    Network Diagram:   Setup Kali Linux 2021.1 VM (attacker)  Windows 7 workstation (victim)  Windows server 2003 (victim) Exploitation Used:  CVE-2017-0143 (Windows SMB Remote Code Execution Vulnerability)     * allows remote attackers to execute arbitrary code via crafted packets * Windows Server 2003 and Windows 7     <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>    CVE-2008-4250 (Server Service Vulnerability)     * allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization * Done on Windows Server 2003   <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2008-4250> Post-Exploitation  1. Escalating the privilege (getsystem) 2. Persistence (run persistence) 3. System password (tools: john the ribber, kiwi) 4. Remote desktop 5. Getting the database (MSSQL) 6. File transfer protocol       **Setup:**  *Victim Machines*   1. Windows 7 VM 2. Windows 2003 server VM     *Attacker Machines*   1. Kali Linux 2021.1 VM |  |
| Gerald Chua | CSF03 |  |
| Lim Shu Zheng | CSF03 |  |
| 13 | Team Friday the Thirteenth | Ng Chin Tiong Ryan -L | CSF03 |  | **SambaCry and Zerologon** | 1. **CVE-2017-7494 (Samba RCE/SambaCry) - primary exploit** 2. **CVE-2020-1472 (Zerologon) - secondary exploit** 3. CVE-2020-1350 (SIGRed)     Case:  Mel is a disgruntled employee of Company13. During COVID-19, the company deployed the Hamachi VPN service to allow employees to work from home, to access the company file shares via the Samba protocol hosted on an Ubuntu File server. Mel decides to use this opportunity to attack the outdated version of Samba and compromise the server. Since the File Server is tied to the Active Directory Domain, Mel can pivot to exploit the Domain Controller with the Zerologon vulnerability to exploit domain credentials and exfiltrate the company’s data.  Setup:   1. Hamachi Software to simulate VPN environment (for both Kali and Ubuntu Server) 2. Ubuntu Server 18.04 w Samba < 4.6.7 3. Windows Server 2019 Domain Controller 4. Kali Linux 2021.1 (Attacker Machine)   Post-Exploitation Activities   1. Pivoting 2. Domain Reconnaissance 3. Antivirus Evasion and Deactivation 4. Covering tracks (Log deletion) 5. File Server Data Exfiltration |  |
| Ng Ray Son | CSF03 |  |
|  |  |  |
| 14 | Team Oreo Cookie | Darien Tan Wei Hao | CSF01 |  | CVE-2016-5195 (DirtyCow)  MS17-010 (EternalRomance)  CVE-2020-7384 | Case scenarioScenario details Team Oreo Cookie was approached by Synechron Tech, a company based in Singapore, to carry out a penetration test on their company’s network. Synechron Tech is a SME that offers office equipment revolving around technology such as workstations and printers to their customers.  Synechron Tech is a fairly new company with little to no prior experience on secure networks and the setting up of one. The current network topology and systems at their Headquarters is being managed by a newly employed Network and Systems Administrator, who suggested to the company, Synechron Tech, a penetration test from Team Oreo Cookie after attempting to fix up the efforts of the previous employee.  The penetration test was agreed to be carried out in a gray-box test method.   Synechron Tech’s network details We will be using Virtual Machines to set up the scenario network, including but not limited to the Workstations, Firewalls and Servers.  Synechron Tech has a main Router, Switch and Wireless Access Point.   * The router and switch are used to manage network traffic as well as separate and manage various network devices and the LAN network. * The Wireless Access Point is to allow for wireless network devices to connect.   Synechron Tech has another Wireless Access Point located outside the LAN.   * This Wireless Access Point is for guests and clients to use in an attempt to separate them.   Synechron Tech has 1 Linux server and 2 Windows servers.   * The 1 Linux server is currently being used as a File server for Synechron Tech to host their confidential files. * The Windows servers are used for:   + Domain controller   + Their old file server, currently being used as a backup file server.   Synechron Tech has several Windows Workstations throughout the network for employee use.   * 1 set of Windows 7 machine * 2 sets of Windows 10 machines   Synechron Tech has 1 Android Device connected to the internal network.   * Purpose of Android Device is for handling mobile payments from Customers.    Synechron Tech’s network diagram Inserting image... Assignment project outlineScenario setupSetup requirements  * Kali Linux (Attacker VM) * Windows 10 VM * Windows 7 VM * Windows Server 2019 * Linux Server (Ubuntu 2015) * Android 8.1-Oreo (<https://www.osboxes.org/android-x86/#android-x86-8-vmware>)  Vulnerabilities and exploitsAndroid As we all know, mobile devices store more information as compared to desktops or workstations. This means that we would be able to extract sensitive information about the company from the phone using social engineering.  Using ngrok, msfvenom and metasploit, we would be able to create a payload and use the exploit (through metasploit). We would then use social engineering methods to get the victim to download the malicious APK, for which we would then be able to execute commands on the android device.    Link: <https://www.cvedetails.com/cve-details.php?cve_id=CVE-2020-7384> Windows Server The windows server in this scenario is being employed as a backup file server for the company to store backups of information being stored on the current live file Linux server.  The exploit planned to be used is called ‘EternalRomance’, with the Microsoft Bulletin code of MS17-010. If executed successfully, it will allow us to access an administrator shell on the Windows Server machine. It requires us to have access to a regular user account on the target server.  Link: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010> Linux Server The Linux server in this scenario is being employed as a file server for the company to store information.  To obtain root access to the server from a user account through privilege escalation, CVE-2016-5195 (DirtyCow) is the CVE of the vulnerability we plan to exploit in the Linux server. How it works is that it allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, hence the name DirtyCow.  Link: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2016-5195> Post-exploitation activities Data exfiltration (android and windows)  Obtain user and server credentials (windows)  Persistence (android)  Obtain system information (for servers) |  |
| Lim Yi Jie |  |
| 15 | Team Banana Cookie | Jason Chua | CSF01 |  | AS-REP Roasting (Initial Reconnaissance & Exploit)  JuicyPotato (Privilege Escalation) | **Case Scenario**  Team Banana Cookie was contacted by Calypso Internal Pte Ltd to penetration test their network. Calypso Internal Pte Ltd is a starting company and does not know much about starting up a secure network hence they reached out to the team on their website, <https://team.nullsecsig.com/>. The project was to be done in a black box penetration testing with the goal of achieving remote code execution with administrative permission.  **Network Diagram**    **Project Outline**  Create a scenario for windows-based attack to allow us to better familiarize with Windows AD server attacks and one of the possible attack vectors on it. This will include the exploitation to get access to a user account and further exploited to get administrative permissions.  **Steps**   1. Retrieve hashes for accounts that do not require Kerberos pre-authentication. 2. Crack the hashes of type “Kerberos 5 TGS-REP etype 23” with hashcat and a custom wordlist (retrieved from CeWL-ing the web server and applying permutations) 3. Access a private share, with READONLY permission for the cracked password’s user and retrieve an Active Directory backup.   **Setup**  Attacker: Kali Linux 2021.2  Victim: Windows Server 2016  Victim: Windows 10  Setup an Active Directory Domain on the Windows Server 2016 and create 2 new user accounts. The 3 users will then be all connected to the domain. Make sure one of the accounts to have SelmpersonatePrivilege or SeAssignPrimaryToken so that it can be exploited to allow for privilege escalation. (The "Impersonate a client after authentication" user right (SeImpersonatePrivilege) is a Windows 2000 security setting that was first introduced in Windows 2000 SP4. By default, members of the device's local Administrators group and the device's local Service account are assigned the "Impersonate a client after authentication" user right. The following components also have this user right:  - Services that are started by the Service Control Manager  -Component Object Model (COM) servers that are started by the COM infrastructure and that are configured to run under a specific account)  This means that IIS service account will have the SeImpersonatePrivilege setting enabled by default.  **Post-Exploitation Activities**   1. Retrieve sensitive Information 2. Persistence 3. Clear Log Files 4. Query state of firewall 5. Query information about server and workstation |  |
| Lim Kai Xian | CSF01 |  |
|  |  |  |
| 16 | Team Choco Cookie | Zuriel Shanley Tanyory | CSF01 |  | Leveraging Tracetogether vulnerability in a pen-testing world | **Scenario**  **Who we are:**  Private Pen-tester,  Hired by the Chief Security Officer of Treadway Enterprise - Dr Albert Jones  **Target:**  Mr Charles William  35 years old  Chief Executive Officer, Treadway Enterprise  **Network Diagram**      **Background**  Team Choco Cookie was hired by the CSO of Treadway Enterprise to pen-test their company. The 2 files that the team is supposed to find are located on the CEO’s mobile phone and a company laptop that is assigned to the CEO. It is the company’s policy to prevent their employees from bringing their work laptop home and the company itself has multiple firewalls, one being a firewall designated to protect the CEO’s laptop.    **Part 1**   1. Perform Eagle’s Eye attack to find out Victim’s exact coordinate through social engineering. Passive recon shows that the victim loves to do illegal online horse betting through Facebook group chat.    1. Attacker created a fake Facebook account and sent the victim a fake WhatsApp group chat invite which will expose the victim's exact coordinates anywhere in the world.    2. Can also obtain sensitive information e.g., Android version of victim’s phone. 2. From the previous attack, we follow the victim to a cafe called Lowercase, where he has to switch on his Bluetooth connection for Safe Entry. Victim has a date, which gives us ample of time to launch the attack.    1. Attacker Run BlueBorne exploit on target machine.    2. Gain Remote Code Execution to target phone.    3. Conduct the attack through a mobile phone to prevent suspicion. 3. Obtain half of the text file containing the bank account detail of our pen-tester fee (data exfiltration) 4. Download a backdoor apk + txt file from a remote cloud location and social engineer victim to install the backdoor for persistency and command & control (persistency)   **Part 2**   1. Perform Evil twin attack on our secondary victim, Manager working at Treadway Enterprise. Performing evil twin attack allow us to obtain employee’s credentials to their email account, through specially crafted website mimicking Microsoft Outlook.    1. Employee goes to Starbucks for coffee every morning at 9 am to 10am, easily perform the attack during that period. 2. Attackers act as potential customer to Treadway enterprise, create a trojan hidden inside a word document or pictures.    1. Obtain the other half of the text file containing the bank account details (data exfiltration)    2. Install keylogger onto the victim’s PC to obtain sensitive information to serve as evidence to the the CSO of Treadway Enterprise   **Pen-test Environment Setup**:   1. Victim’s PC, Windows 10 2. Victim’s mobile phone, Android 6 3. Attacker PC, Kali Linux 4. Attacker mobile phone, Android     **Exploits:**   1. [CVE 2020-0781](https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0781) BlueBorne 2. Eagle’s Eye Attack 3. Evil Twin Attack 4. Spear fishing (to inject malware into victim’s machine)     **Post Exploitation:**   1. Persistence 2. Keylogging 3. Escalation of Privileges 4. Data Exfiltration 5. Command & Control |  |
| Ang Si Hao |  |  |
|  |  |  |
| 17 | Team Fried | Alyssa Chwee | CSF01 |  | Penetrating Insecure Network and End-User Devices with Macros and Exploits | **Use Case Scenario**  John is the owner of XYZ Books Company, a small company he recently started to earn more money during the pandemic. As the company is new, their network and devices are barely protected and not properly configured with security mechanisms such as Firewall and IDS. Due to his limited budget, he enlisted two cybersecurity students to help pen-test his company network. The pen-testers are not given any information about his network and are allowed to freely exploit his network with any means.  John uses the company’s PC but allows his staff to bring their own devices and connect it to the company’s Wireless AP. The pen-testers will perform reconnaissance on the company and use social engineering tactics to trick one of the staff, Simon, into downloading a malicious document and allowing the pen-testers access to their insecure laptop via a reverse shell connection.  Using arp-scan, other hosts on the same network can be discovered along with their IP addresses. These hosts will be scanned using NSE to locate vulnerabilities to exploit.  Pen-testers will then pivot and gain access to John’s PC using **EternalBlue Exploit (CVE-2017–0144).** The Database Server found on the same network contains confidential information and can only be accessed by John. Port 1433 is open, and pen-testers will exploit it using Metasploit **(exploit/windows/mssql/mssql\_payload)** and John’s credentials found on his computer.  Post-Exploitation Activities will be carried out on all compromised hosts, such as Persistence, Credential Harvesting, Privilege Escalation, and Information Gathering.  **Project Outline:**  Our project aims to highlight how dangerous it can be to allow bring your own devices (BYOD) without proper network segmentation, firewall protection, and security management. Our project also shows the importance of updating and upgrading devices to prevent attacks and storing credentials securely.  We will be making use of msfvenom to craft a malicious document to exploit an insecure device lacking anti-virus protection and allowing a reverse shell connection to the pen-tester's machine outside of the company network.  To pivot into other machines, the EternalBlue exploit is used. The EternalBlue exploit makes use of a vulnerability in Microsoft’s Server Message block (SMB) protocol in older unpatched versions of Windows Operating Systems to gain access to the target machine.  Lastly, we will exploit the Database Server with port 1433 using Metasploit’s mssql\_payload which exploits xp\_cmdshell in order to open a Meterpreter shell.  **Virtual Machines:**   1. Kali Linux VM (Pen-Tester's Machine) 2. Windows 7 VM (Simon’s and John’s) 3. Windows Server 2019 (Database Server running MS SQL)   **Detailed Steps:**   1. Perform reconnaissance on the company to identify staff, emails, and personal details 2. Craft a malicious document using msfvenom and send to Simon 3. Reverse shell session opens between compromised laptop (Simon’s) and Attacker 4. Scan network with arp-scan to discover other hosts on network 5. Escalate privileges and establish persistence in Simon’s Laptop 6. Perform vulnerability scanning using NSE 7. Pivot into John’s PC using EternalBlue exploit 8. On John’s PC — Credential Harvesting, obtain Database Account password 9. Exploit Database Server using Metasploit (exploit/windows/mssql/mssql\_payload) and perform information gathering.   **Post-Exploitation Activities**   1. Gaining Persistence 2. Credential Harvesting 3. Privilege Escalation 4. Information Gathering |  |
| Loke Ying Xia | CSF01 |  |
|  |  |  |
| 18 | Team Chickin | Livia Poernomo | CSF01 |  | Exploit a network and take over remote devices using a compromised machine. | **Case Scenario:**  ABC company is a small start-up food stall company composed of a group of new graduates Alex, Ben and Clorise. Due to the lack of funds, the group decided that the bare minimum security for their IT infrastructure and machines would be sufficient. A team of hackers have discovered the vulnerabilities of the company network and is now planning to sabotage the start-up company and the employees.    **Network Diagram:**      **Project Outline:**  Hackers visited ABC’s company food stall and connected to their network via the Wi-Fi given for free to the customers of ABC food stall. Through reconnaissance, hackers are able to identify the devices connected to the router.  Hackers launched an MITM attack on the PC used by Alex. They can perform MITM attacks to infect the traffic with malware and sniff credentials and information from the packets exchanged from device to the server and vice versa.  Hackers then perform session hijacking through HTTP, gaining access to the email used by the team members to exchange files, therefore, crafting spear phishing emails to the other members working from home with the existing information in the email account.  Spear phishing emails are equipped with malicious files, which tricks the other members to download them. The malicious files will help the hackers to gain control over Ben’s laptop and Chlorise’s android phone. Hence, Ben’s laptop and Chlorise’s android phone are compromised.  From Ben’s compromised device, hackers are able to do domain reconnaissance and vulnerability scanning using various tools. After the process is done, pivoting is then carried out to a Windows 10 Device in Ben’s network, making use of the EternalBlue exploit.  **Setup:**   1. Windows 10 (Alex’s PC) 2. Windows 7 (Ben’s Laptop) 3. Windows 10 (Device in Ben’s Private Network) 4. Android Phone (Chlorise’s Mobile Phone) 5. Kali Linux (Attacker’s Machine) 6. Palo Alto Firewall acting as a router   **Exploitations:**   1. MITM (Packet Modification) 2. Session Hijacking CVE-2016-3306 3. Social Engineering (Spear Phishing) 4. Escalation of Privilege on PC CVE-2019-0543 5. Remote Code Execution via RDP CVE-2019-0708 6. EternalBlue CVE-2017–0144     **Post-Exploitation Activities:**  Windows 10 Machine (Alex’s PC)   1. Session Hijacking 2. Data Exfiltration   Windows 7 Machine (Ben’s Laptop)   1. Privilege Escalation 2. Remote Code Execution 3. Domain Reconnaissance 4. Pivoting 5. Data Exfiltration   Android Phone (Chlorise’s Phone)   1. Data Exfiltration 2. Remote Device Access |  |
| Joanne Ang | CSF01 |  |
|  |  |  |
| 19 | HEY WAI KEET | Ng Wai Keet - L | CSF01 | 91727502 | The hidden danger in NAT Slipstreaming. | **Case scenario:** Through exploiting a website vulnerable to Stored XSS (Cross-Site Scripting), a malicious script capable of performing NAT Slipstreaming was injected into the website. John, a normal internet user, had accessed this vulnerable website with the script injected. This made his network vulnerable as the script opens up his ports in the network and made it possible to the attacker to bypass any NAT devices and gain access to TCP devices in his network.  With access to his network, the group of hackers can then perform pivoting attack, and gain unauthorized access to all devices available in the network.  **Network Diagram:**  **Setup:**  Palo Alto Firewall  Layer 3 Switch  Android Device  Windows 7 Workstation  Network Printer  **Exploitation:** NAT Slipstreaming will be used to exploit a user’s browser to open the  **https://nvd.nist.gov/vuln/detail/CVE-2020-28041**  **Post-Exploitation:** 1. Pivoting attack from Android Device  2.Gain reverse shell on Windows 7 Workstation  3.Get sysinfo  4.Control on IOT connected to workstation  5. Webcam control  6. File traversal  7. Keylogging  8.Retrieve sensitive information  9.Gain access on printer  10.Print out a picture remotely |  |
| Lim Jun An Bryan | CSF01 | 82615878 |  |
| Li Zibin | CSF01 | 86707914 |  |
| 20 | Team Sam's Well | Caasi John Rian Domingo - L | CSF01 |  | Dangers of Social Engineering and | **Case scenario:**  XYZ company is a small start-up company. Recently they decided to move their operations to another new site, where they have upgraded all existing tech infrastructure. In order to prevent downtime for the potential customers, they have decided to leave their old site running until they have confirmed and are ready to operate on the new site.  At their old site, they had a Windows server 2003 machine acting as a file server and a Linux server acting as a web server. They also have a few employees working there as a sub office space for the time being with no one in the front desk.  **Network diagram:**    **Setup:**  List of VMs:   * Windows server 2003 (File server to store employee information) * Ubuntu Server (Scratch) - Web server * Ubuntu Server (Scratch) - (SQL File server to store customer information) * Kali Linux (attacker Machine)   **Exploitation:**   1. Evil twin attack to connect to network (MITM attack) 2. Scan network for connected devices and OS versions 3. Scan file server for open ports 4. Discover ThinVNC by typing the IP address of the file server with the open port found 5. Attack windows server 2003 machine using ThinVNC (CVE-2019-17662) to gain access.   **Post-Exploitation**   * Persistent backdoor -> use metasploit from then on * Pivot Attack to Ubuntu Web server (Shellshock attack CVE-2014-6271) * Website Defacement of Ubuntu web server website (change website html within apache directory) * Data Exfiltration from Windows 2003 file server * Pivot Attack to Ubuntu File server (distcc exploit in msfconsole) * Date exfiltration from Ubuntu file server |  |
| Nicholas Goh Jun Jie |  |  |
| Tay Quan Yi |  |  |
| 21 | huh? | Chua Zhe Yu -L | CSF03 |  | Exploiting EternalBlue & Ensuring Persistence | **Scenario:**  Organization A is a small established company that wants to evaluate their security. They have hired “huh?”, an independent team of white hat hackers to evaluate and pen test their internal network. We have been given the network address of the company’s network.  Main exploit: CVE-2017-0144 (EternalBlue)  Attacker’s PC: Kali Linux 2021.1  Organization’s PCs: Windows 7  Organization’s Server: Ubuntu Server 14.04.6 LTS  Internet (Router): Windows Server 2019  Post-Exploitation Activities   1. Ensuring Persistence using msfvenom payload 2. Pivoting to Ubuntu Web Server 3. Information and Credentials Gathering 4. Dos web server |  |
| Tan Yuan Ming |
| 22 | Team Nocturne | Ng Tze Keat | CSF03 |  | Gaining root privileges to router and execute code to remote machine | **Network diagram:**    **VMs used:**  Attacking machine: Kali Linux 2021  Router: VyOS 1.1.8  DNS server(s): Ubuntu Server  Workstation: Windows 10  File server: windows 7 with FileZilla  **Scenario:**  Team Nocturne has planned to compromise company Praeludium’s internal network and steal their confidential files and information. The team is connected to company’s Wireless AP. They will use Nmap to scan for any Ip addresses that belongs to the VYOS router. After gaining the IP address of the router, the team will take over and change the router’s configurations by exploiting **CVE-2018-18556** and change the company’s DNS to their own DNS server. The team will then attack the file server, which is a **Windows 7 machine with FileZilla** installed, using **CVE-2017-0144(EternalBlue)** to access the confidential data stored within.  **Project Outline:**  **CVE-2018-18556** affects the VyOS 1.1.8 routers. It is a privilege escalation issue, and the default configuration also allows operator users to execute the pppd binary with elevated permissions. Certain input parameters are not properly validated. A malicious operator user can run the binary with elevated permissions and leverage its improper input validation condition to spawn an attacker-controlled shell with root privileges.  **CVE-2017-0144** Microsoft Windows Vista SP2, Windows Server 2008 SP2 & R2 SP1, Windows 7 SP1, Windows 8.1, Windows server 2012 Gold & R2, Windows RT 8.1, Windows 10 Gold, 1511 & 1607, and Windows Server 2012. It allows remote attackers to execute arbitrary code via specially crafted packets sent to a targeted SMBv1 Server also known as “Windows SMB Remote Code Execution Vulnerability.”  For the attack, our team will use a Kali Linux 2021 virtual machine with tools such as the Metasploit Framework. To take over the router and change its configuration, we will first use Nmap to scan the network for the list of IP addresses and find the IP address that belongs to the router. Once that is done, we will exploit CVE-2018-18556 using the metasploit module vyos\_restricted\_shell\_privesc and gain root privileges to change the router’s configurations. The router’s connected DNS server will be changed to our own Ubuntu Server. After gaining access to the router, we will carry on exploiting CVE-2017-0144 on the windows 7 machine by sending crafted packets.  Successfully exploiting the router and Windows 7 machine will allow us to perform the following post exploitation activities:  **Post exploitation:**   * Steal banking information. (Router) * MITM (Router) * Sniffing/Redirecting traffic. (Router) * DNS hijacking (Router) * Changing Logs (File Server) * unauthorized access to confidential files and data in file server:   + malicious file uploads   + Download Files   DNS Server creation:  <https://www.fosslinux.com/7631/how-to-install-and-configure-dns-on-ubuntu.htm>  Dns hijackiing:  <https://levelup.gitconnected.com/ethical-hacking-part-9-dns-hijacking-credential-harvesting-db57302e5131>  **CHOSEN CVEs:**  CVE-2018-18556  <https://www.rapid7.com/db/modules/exploit/linux/ssh/vyos_restricted_shell_privesc/>  CVE-2017-0144(EternalBlue)  <https://www.exploit-db.com/docs/48760>  <https://syang.io/2017/05/17/Simulate-EternalBlue.html>  <https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-0144/> |  |
| Gladys Chua Ling Hui - L |  |  |
| 23 | Team EAT | Elijah Ng Ding Jie -L | CSF02 | 82902337 | **Title:**  Pen-testing of Sky Company’s Network and Systems:  Exploiting WPS in Wireless Access Points, RTSP in IP Camera, client-side exploitation of Windows machine and service-side exploitation of Windows and Linux machines. | **1. Scenario (Use Case) Diagram**    **1. Scenario (Use Case)**   * Team EAT was engaged by a Small-Medium Enterprise (SME) named Sky Company to perform a grey-box pen-test on the company’s network and systems. Sky Company is a company that sells IT products. * Sky Company had previously hired a network and systems administrator to protect their network and systems. However, it was found that the administrator did not enforce proper security configurations and did not routinely patch or update the company’s systems. * Team EAT was therefore engaged to pen-test and discover the vulnerabilities in the company’s network and systems in order to provide recommendations on how they can be patched. Sky Company would like to prevent or mitigate the chances of a cyber attack affecting the business. Sky Company has allowed Team EAT to carry out any proof-of-concept exploitation activities that can prove the severity of the vulnerabilities found.       **1. Scenario (Use Case) – Sky Company’s Network**   * Sky Company’s network consists of servers, workstations, routers, switches, firewalls, and wireless access points.   + Sky Company has a Core Router, Core Switch and main Wireless Access Point (WAP)     - The core switch provides switching between the network devices and hosts connected Sky Company’s LAN.     - The core router facilitates movement of data between different networks, allowing hosts to access the internet.     - The main AP is used to provide a WLAN for hosts to connect wirelessly to Sky Company’s Network.   + Sky Company has a Powerline to extend the WLAN Coverage     - The powerline AP is used to extend the WLAN coverage of Sky Company’s Network.   + Sky Company has a Palo Alto Firewall     - Sky Company is currently using the firewall for testing and evaluation purposes.   + Sky Company has a D-Link IP Camera (IoT Device)     - Sky Company places this IP Camera in their office to monitor its employee activities.   + Sky Company has two Windows and two Linux Servers     - Windows Server 2012 serves as the domain controller for Sky Company’s domain.     - Linux (Ubuntu 8.04) server serves as a File and Web server for Sky Company.     - Windows Server 2008 serves as a second File server for Sky Company.     - Linux (Ubuntu 20.04) server hosts Oracle Database and acts as a Database server for Sky Company.   + Sky Company has multiple end-user Windows Workstations     - Windows 7 Ultimate workstation joined to Sky Company’s domain.       1. Previously used by Sky Company’s network and systems administrator to test Active Directory configuration settings.     - Two Windows 10 Home workstations used by Sky Company’s Employees to access internal resources and the internet. * \*Note: In order to reproduce Sky Company’s network, we will be using Virtual Machines to set-up the Workstations, Servers and Firewall where applicable. We will be either using a Bridged Network Connection or connecting a USB Wireless Adapter directly to the Virtual Machines to connect them to the Router and Wireless Access Points (WAP).       **1. Scenario (Use Case) – Process**   1. Perform a WPS Pin Attack on the D-Link Powerline Router and Wireless Access Point to obtain the credentials needed to connect to the Wireless Access Point (WAP). 2. As the D-Link Powerline Router and Wireless Access Point is connected to the main Wireless Access Point and shares the same network ID, we are able to gain access to the entire network. 3. Scan Sky Company’s network to detect for live hosts as well as vulnerabilities. 4. Perform an ARP spoofing attack on a Windows 10 Home (Version 20H2 Build 19042.1052) machine and Palo Alto Firewall Virtual Machine. 5. Perform a dictionary attack on the D-Link IP Camera’s Real Time Streaming Protocol (RTSP) server to obtain the authentication credentials. 6. Carry out two exploits on an Ubuntu Virtual Machine (Metasploitable 2).    1. Service-side exploitation of the smiley face backdoor vulnerability in the vsftpd (Very Secure FTP daemon) version 2.3.4 server (CVE-2011-2523), which is the default FTP server in Ubuntu, allowing us to gain a shell and execute arbitrary codes remotely.    2. Service-side exploitation of the shellshock vulnerability in the bash shell (CVE-2014-6271) allowing for privilege escalation and execution of arbitrary codes remotely. 7. Perform service-side exploitation of the BlueKeep vulnerability in the RDP (Remote Desktop Protocol) service (CVE-2019-0708) on a Windows 7 Virtual Machine, which is joined to Sky Company’s domain. 8. Perform service-side exploitation, using the EternalBlue exploit, of the vulnerability in the Server Message Block version 1 (SMBv1) server (MS17-010, CVE-2017-0144) on a Windows Server 2012 Virtual Machine, which is the Domain Controller for Sky Company’s domain. 9. Perform a service-side exploit on an oracle database 11g server hosted on Ubuntu 20.04 utilizing its vulnerable TNS listener (CVE-2012-1675). An exploit called TNS Poisoning will be performed on this to perform a MITM attack on the database server and gain sensitive information. 10. Perform a service-side exploit on a vulnerability in Windows 10 Version 1703 (CVE-2019-0841) AppX Deployment Service (AppXSVC) to gain control of sensitive files on the computer. 11. Perform a client-side attack exploiting a vulnerability in the Windows Shell that opens a shell on the Windows 10 Version 1703 workstation and connects it to the attacker’s workstation. This attack will allow us to pivot and perform the next attack. 12. Perform a service-side attack exploiting a vulnerability in the Secondary Logon Service that opens a shell with escalated privileges. The connection made to the Windows 10 Version 1703 will be used to access the Windows Server 2008 machine and execute the attack.  * Note: Further details into the exploits we will be carrying out and vulnerabilities that we will be exploiting is documented in section 3.       **2. Devices & Machines Used for Exploitation**   1. D-Link Powerline Router & Wireless Access Point    * Connection from D-Link Powerline Ethernet Adapter which is connected to Core Switch 2. Windows 10 Home Version 20H2 Build 19042.1052 64-bit Machine 3. Palo Alto Firewall PAN-OS 9.0 Virtual Machine 4. D-Link IP Camera (IoT Device) 5. Ubuntu 8.04 (Hardy) 32-bit Virtual Machine - Metasploitable 2    * Linux Kernel: 2.6.24-16-server    * Serves as a File and Web Server for Sky Company 6. Windows 7 Ultimate Version 6.1 Build 7601 SP1 64-bit Virtual Machine    * Joined to Sky Company’s Domain 7. Windows Server 2012 R2 Datacenter Version 6.3 Build 9600 64-bit Virtual Machine    * Domain Controller for Sky Company’s Domain 8. Windows 10 Home Version 1703 Build 15063.632 64-bit Virtual Machine 9. Windows Server 2008 R2 Version 6.1 Build 7601 SP1 64-bit Virtual Machine    * Serves as a Second File Server for Sky Company 10. Ubuntu 20.04 64-bit Virtual Machine     * Serves as an Oracle Database Server for Sky Company       **3. Assignment Outline Details (Vulnerabilities & Exploits Used)**  Types of Penetration Testing that will be Performed:   1. System Penetration Testing 2. Network Devices Penetration Testing 3. Wireless Network Devices Penetration Testing 4. Remote Communication Penetration Testing      * In order to gain access into Sky company’s network, we will first begin by using Wifite to perform a WPS Pin Attack on the D-Link Powerline Router and Wireless Access Point. This exploit leverages on the weak default WPS Pin of D-Link Powerline Wireless Access Points. This is a vulnerability as the firmware version of this D-Link Powerline Router and Wireless Access Point does not allow for the WPS Pin to be changed or for WPS to be disabled. This exploit would allow us to obtain the pre-shared key and connect to the Wireless Access Point. * Since the D-Link Powerline Router and Wireless Access Point is connected to the main Wireless Access Point and shares the same network ID, we are able to gain access to the entire network. We will then scan Sky Company’s network for live hosts as well as vulnerabilities. Following that, we will proceed to exploit the vulnerabilities and weaknesses found as a proof-of-concept. * Second, we will be using Ettercap to perform an ARP spoofing attack on a Windows 10 Home (Version 20H2 Build 19042.1052) machine and Palo Alto Firewall Virtual Machine. This attack works by poisoning the ARP cache so that all traffic meant for either machine will first be forwarded to the pen-tester’s Kali Linux machine. In our Kali Linux machine, we are able to use Wireshark to sniff and inspect the traffic. Since the Palo Alto Firewall allows unencrypted telnet connections, we are able to sniff the username and password when the Windows 10 machine attempts to use telnet to remotely access the Palo Alto Firewall for administration. * Third, we will be using Hydra to perform a dictionary attack on the D-Link IP Camera’s Real Time Streaming Protocol (RTSP) server. This service-side exploit leverages on the fact that the RTSP server on the D-Link IP camera does not set a fixed maximum number of failed authentication attempts before lockout authentication lockout period. This is a vulnerability as there is no lockout limiting the number of authentication attempts allowed before a lockout period is enabled or the attacking machine’s IP address is blocked. This exploit would allow us to obtain the RTSP authentication credentials and view the live video stream from the IP camera. We would also be able to retrieve and download past recordings. * Fourth, we will be carrying out two severe exploits on an Ubuntu Virtual Machine. * The first is a service-side exploit that leverages on a backdoor vulnerability (CVE-2011-2523) found in version 2.3.4 of vsftpd (Very Secure FTP daemon), which is the default FTP server in Ubuntu. We will be carrying out this exploit manually. The exploit works by entering the “:)” characters as the username when attempting to connect to the FTP server through port 21 remotely and for that reason, it is also known as the smiley face backdoor. This exploit would allow us to gain a shell to the Ubuntu machine on port 6200 and execute arbitrary codes remotely. * The second is a service-side exploit that leverages on a vulnerability in the bash shell (CVE-2014-6271) which would allow us to gain a reverse shell and execute arbitrary codes remotely. This vulnerability is also known as shellshock. We will be carrying out this exploit using Metasploit. When specially crafted code is processed by the Bash shell, it does not sanitise the environmental variables properly and will execute the malicious codes. This exploit allows for privilege escalation in order to execute arbitrary codes remotely. * Fifth, we will be carrying out a service-side exploit that leverages on a vulnerability in the Remote Desktop Protocol (RDP) service (CVE-2019-0708) on a Windows 7 Virtual Machine. This vulnerability is also known as BlueKeep. It is a severe vulnerability because it is wormable and can self-propagate to spread from other machines in the network automatically without human interaction. We will be carrying out this exploit using Metasploit. * The exploit works by setting up a channel with the name of “MS\_T120” on a different channel other than the default channel 31. Malicious data is then sent through the newly set-up channel to close the newly set-up channel and terminate the RDP session. Since the RDP server does not check for the existence of two channels with the same name of “MS\_T120”, a pointer to channel 31 remains, leading to a use-after-free (UAF) vulnerability. This causes heap corruption and allow us to gain a reverse shell to execute arbitrary codes remotely with system privileges, the highest privilege level in Windows. * As a post-exploitation activity, since the Windows 7 Virtual Machine is joined to Sky Company’s domain, we would perform credential harvesting and attempt to obtain the domain administrator’s credentials which can be used in the subsequent exploit. This would be possible if the domain administrator had logged onto the Windows 7 Virtual Machine using his account. * Sixth, we will be carrying out a service-side exploit that leverages on a vulnerability in version 1 of the Server Message Block (SMBv1) server (MS17-010, CVE-2017-0144) on a Windows Server 2012 Virtual Machine, which is the Domain Controller for Sky Company’s domain. This exploit is known as EternalBlue. It is a severe vulnerability because it is wormable and can be used by malwares to self-propagate and spread to other machines in the network automatically without human interaction. We will be carrying out this exploit using Metasploit. * The exploit works by sending specially crafted malicious packets to the SMBv1 Server, which are mishandled by the SMBv1 server, in order to allow us to gain a reverse shell and execute arbitrary codes remotely. When carrying out this exploit on the Windows Server 2012 Virtual Machine, we can provide the domain administrator’s SMB username and password to log onto the Windows Server which would ensure that the exploit would be successful regardless of whether the server has been configured to allow anonymous access to named pipes. The domain administrator’s credentials can be harvested from the Windows 7 Virtual Machine that we had exploited and gained accessed to earlier. As a post-exploitation activity, we will be installing a malicious service that will create a backdoor and ensure persistence. The malicious service will be automatically executed on start-up and allows us to gain a reverse shell as long as the Windows Server is live. * Seventh, we will perform a service-side exploit on an oracle database 11g server hosted on Ubuntu 20.04 utilizing its vulnerable TNS listener. There is an exploit called TNS Poisoning which allows attackers to perform a MITM attack on the database server to gain sensitive information. Firstly, we will use an nmap script as well as a Metasploit module to check if the machine is vulnerable to TNS Poison attacks. Then we will then use a specially crafted TNS Poison script to set up a MITM attack on the database. * This exploit uses a specially crafted application to exploit the CVE-2012-1675 vulnerability to allow attackers to remotely execute database commands by performing a remote registration of a database, instance, or service name that already exists, and then allows attacker to perform a MITM attack. It is also known as a TNS Listener Poison Attack. It is a vulnerability in the TNS listener of Oracle Database found in oracle database 11g and other older versions, and this vulnerability can be exploited without authentication, and can also be exploited over a network, making it very dangerous. * Eighth, we will be carrying out a service-side exploit on Windows AppX Deployment Service (AppXSVC) and exploit a vulnerability in Windows 10 (Version 1703 Build 15063.632) (CVE-2019-0841) on a Windows Virtual Machine. We will perform a dictionary attack on a VNC to gain remote access to the workstation using hydra so that we can exploit the CVE-2019-0841 Vulnerability to gain full control of sensitive files such as the hosts file in C:\Windows\System32\drivers\etc\ * The exploit works by running a specially crafted application to exploit CVE-2019-0841, which is an elevation of privilege vulnerability which occurs when the Windows AppX Deployment Service (AppXSVC) improperly handles hard links. An attacker who successfully exploited this vulnerability could run processes in an elevated context, and can then install programs, as well as view, change or delete data on the computer. This exploit requires the attacker to be logged onto the system already, thus, remote access would be needed such as using VNC. * Ninth, we will perform a client-side attack that exploits a vulnerability in Windows 10 (Version 1703 Build 15063.632) (CVE-2018-8414) to gain remote access to the virtual machine. The vulnerability is a result of improper file path validation by the Windows Shell and can be exploited by running a specially crafted file on the victim’s machine. * This exploit uses the CVE-2018-8414 vulnerability to execute code remotely through a malicious file. When the victim runs the specially crafted file, the code executed can open a shell and connect it to the attacker’s machine. The connection can then be used to perform post-exploitation actions on the victim’s machine. One of which is to connect to the Windows Server 2008 virtual machine to perform the next exploit. * Tenth, we will perform a service-side attack on a Windows Server 2008 virtual machine that is vulnerable to privilege escalation (CVE-2016-0099). The vulnerability stems from the Secondary Logon Service and can be exploited through running an executable on the victim’s machine. * This exploit uses the vulnerability CVE-2016-0099 to open a privileged command shell. With a privileged shell, we can bypass permissions and perform administrator actions. * After each successful exploitation, we will be carrying out several post-exploitation activities. Further details of the post-exploitation activities that we be carrying out is documented in section 4.   **4. Post-exploitation Activities**   1. Ubuntu 20.04 64-bit D-Link Powerline Router & Wireless Access Point    1. Connect to Wireless Access Point       1. Disable and Clear Logs       2. Perform ARP Spoofing/ARP Cache Poisoning on the Network          * Sniff Network Traffic between Windows 10 Home (Version 20H2 Build 19042.1052) Machine and Palo Alto Firewall PAN-OS 9.0 Virtual Machine to obtain Telnet Credentials       3. Exploiting Vulnerabilities on other Hosts in the Network (Including Hosts Connected to the Main Wireless Access Point) 2. D-Link IP Camera (IoT Device)    1. Streaming Live Video Feed    2. Retrieving Past Recordings 3. Ubuntu 8.04 (Hardy) 32-bit Virtual Machine - Metasploitable 2    1. Obtain System Information    2. Obtain Current User’s Privilege Information    3. Gaining an Interactive TTY Shell    4. Extract and Dump User Account Information    5. Extract and Dump Hashed User Account Passwords    6. Cracking Hashed Passwords    7. Escalating Privilege 4. Windows 7 Ultimate Version 6.1 Build 7601 SP1 64-bit Virtual Machine    1. Obtain System Information and Current User’s Privilege Information    2. Obtain List of Running Processes    3. View Screen and Record Webcam    4. Obtain Wireless Access Point Pre-shared Keys    5. Credential Harvesting 5. Windows Server 2012 R2 Datacenter Version 6.3 Build 9600 64-bit Virtual Machine    1. Gathering Domain Controllers, Computers and User Information    2. Installing a Malicious Service to Create a Backdoor and Ensure Persistence    3. Wiping Indicators of Compromise       1. Clearing Windows Events Logs       2. Removal of Malicious Service 6. Ubuntu 20.04 64-bit Server    1. Obtain System Information    2. Get User Credentials    3. Extract Sensitive data on Database 7. Windows 10 Home Version 1703 Build 15063.632 64-bit Virtual Machine    1. Edit the HOSTS file to redirect domain names to malicious sites    2. Gain remote access    3. Access the Windows Server 2008 remotely and execute the privilege escalation exploit. 8. Windows Server 2008 R2 SP1 64-bit Virtual Machine    1. Gain access to sensitive files    2. Change permissions on files to make private files public       **5. Recommendations**   1. We will be providing recommendations as to how the exploits that we have carried out can be prevented and how the vulnerabilities exploited can be patched if applicable. |  |
| Chia Ping Yi Alston | 92975567 |
| Thaddeus Teo E Kai | 97331244 |
| 24 | Team Strawberry | Soh Liu Jing Mabel | CSF02 |  | Exploitation of workstation and database server through remote code execution. | Case Scenario Gold Coin company has been targeted by hackers to conduct an attack on to steal valuable data/crash the company’s system. The hackers are targeting the company’s valuable data that can be stolen for financial gains, since the company is found to have an insecure system that is easy to hack into. Hackers manage to hack into the company network. Network Diagram  SetupVictim’s side  1. Workstation: Windows 10 VM 2. Database Server: Windows Server 2016 VM  Attacker’s side  1. Kali Linux 2021.1 VM  Exploitation Victim’s Workstation (Windows 10)   1. CVE-2019-1181 - Remote Code Execution vulnerability   <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2019-1181>   1. CVE-2019-0787 - Remote Code Execution vulnerability (backup plan)   <https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2019-0787>  Database Server   1. CVE-2017-8565 - Remote code execution on Windows server   <https://www.cvedetails.com/cve/CVE-2017-8565/>   1. CVE-2017-8463 - Remote code execution on Windows server (backup plan #1)   <https://www.cvedetails.com/cve/CVE-2017-8463/>   1. CVE-2017-0292 - Remote code execution on Windows server (backup plan #2)   <https://www.cvedetails.com/cve/CVE-2017-0291/> Post-Exploitation Activities  1. Escalation of Privileges 2. Information Gathering 3. Screen Capture 4. Event log management |  |
| Soh Qi Hui Selina |
| 25 | Team TamiRoni | Ron Joshua A. | CSF03 | 91441387 | **A Comprehensive Exploitation of**:  **Machines and Smart-Devices** | **Case Scenario:**  The Company, **Excelsior**, is a fashion start-up company. With the company in its infancy, it had not known the importance of having a security consultant. This leads to the electronic machines in their network infrastructure being unprotected and unsecured.  This is important as the company handles a large amount of sensitive client data that is regularly updated and sent to-and-fro from their Windows File Server and Windows 10 Machines. A Tablet running Android is put in place to use with special applications embedded inside for auditing and tracking of fashion retail resources of the company. Lastly, a Smart-Car owned by the CEO is connected under the network infrastructure of Excelsior.  Hence, our team has been hired to search for vulnerabilities in the system. After which, protective solutions would be highlighted to stray away from such harmful exploits.  **Network Diagram Excelsior:**    **Set-up:**   1. Kali-Linux [Pen-Tester] 2. Windows File Server 2019 [Target] 3. Windows 10 Machine [Target] 4. Tablet (Android) [Target] 5. Smart-Car [Target]   **Guidelines:**   1. Rules of Engagement  * Generally, a grey-box test as subnet of the network is given.  1. Scoping  * Ping sweep of network ranges * Port scan of target hosts * Vulnerability scan of targets  1. Opensource Tools  * GitHub etc...  1. Nmap  * Target specification using network ID * Targeting ports * Use of NSE * Probing (if needed)  1. Metasploit  * Search of appropriate modules and exploits * Sample of Android Exploit: android/meterpreter/xxxx * Sample of Windows: exploit/windows/local/xxxx * Sample of Smart-Car Exploit: post/hardware/automotive/xxxx   **Exploitation:** [Subject to Expansion and Incrementation]  CVE-2018-8453   * An elevation of privilege vulnerability exists in Windows   <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8453>  CVE-2020-7384   * Allows for a malicious user to craft and publish a file that would execute arbitrary commands on a victim's machine using an msfvenom   <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7384>  CVE-2020-0796   * A Client/Server remote code execution vulnerability exists in Microsoft Servers   <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0796>  CVE-2020-8539   * Allow an attacker to inject unauthorized commands and trigger unintended vehicular functionalities.   <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8539>  **Post-Exploitation:**   1. Sensitive Information Gathering  * Dumping SMS, Call Logs, Contacts from Android Phone * Gathering files from Machines * Video streaming of android camera * Installing arbitrary applications  1. Automotive Vehicle-Network Hacking using Controller Area Network (CAN) vulnerabilities 2. Escalation of privileges 3. Remote Code Execution 4. Remote Access to Device(s) 5. Session Hijacking |  |
| Tammy Ho Ying Hui | 88858549 |
| 26 | Team BS | Liew Jing De Benjamin | CSF03 | 93684229 |  | **Case Scenario**  Company PotatoWedges is a startup company that aims to create and design revolutionary technology and has recently formed its HQ in Singapore. PotatoWedges is concerned about how secure their current network is. If there are any devices or information that has been compromised, it could negatively affect their public image and lose a lot of profit.  We are hired to attempt to infiltrate their private network in HQ (without using the internet). Our goal is to try and find ways to obtain unauthorized information as well as causing potential destruction to their company. Note that we will be testing in the range of the private network.    **Network Diagram**  The following network diagram shows the network structure of our case scenario.    \*Note that this Wi-Fi connection is using WPA2 Wi-Fi security.      **Devices used**  Devices shown in the network diagram (without the router and WAP as those are unknown)   * File Server   + Windows Server 2012 * Client PCs   + Windows 10 * Attacker machine   + Kali Linux 2021.1     **Test the following exploits**  In our presentation we will showcase a step-by-step process of successful exploits. The following exploits shown are to be tested (and more if we can find any that is related to our goal):  **WPA2**   * **CVE-2018-6402**   + Devices can be forced to deauthenticate and connect to another Wi-Fi network with the same SSID   + Method used:     - Create fake access point (evil twin attack)     - Hostapd-wpe:   <https://github.com/OpenSecurityResearch/hostapd-wpe>   * **CVE-2019-15126 (kr00k)**   + A KRACK related exploit that allows attacker to decrypt packets even in a WPA2 Wi-Fi security   <https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf>    **Windows**   * **CVE-2020-1113** A security feature bypass vulnerability exists in Microsoft Windows when the Task Scheduler service fails to properly verify client connections over RPC, aka 'Windows Task Scheduler Security Feature Bypass Vulnerability'.      * **CVE-2019-1181**   Exists in Remote Desktop Services. Attackers can install programs, or view, change, or delete data.     * **CVE-2021-31968**   DOS Vulnerability in Remote Desktop Services    **Post Exploitation activities**     * “Freeload” off private Wi-Fi network (low security risk) * *Using the private Wi-Fi network to perform illegal activities (illegal activities if found can be traced to the private network’s public IP address) [potential post exploitation but we won’t be doing this]* * Decrypt WPA2 packets, packet sniffing * Run arbitrary code as an administrator * Install programs * View, change, or delete data * Create new accounts with full user rights * Denial of Service * Privilege escalation     **Others**  We will also include the following for our assignment   * Performing quick reconnaissance before attempting exploits * Recommendations on how to prevent exploits shown |  |
| Debbie Hii Wenxin | 86933007 |
| 27 | Team - | Tsen Fan Loong  Xie Zhuohan | CSF03 |  |  | **Case Scenario**  Company ABX is a start-up company led by traditional thinkers and wants to better understand and secure their company infrastructure. To discover the vulnerabilities in their network, they requested us to perform penetration testing on the company’s network infrastructure and to exploit any device on the network and report our findings.  **Diagram**    **Machines involved**   * Kali Linux VM * Windows 10 VM * Windows Server VM * pfSense Firewall VM   **Exploitation**  CVE-2016-10709   * Exploiting a bug in a specific pfSense post authentication php page allowing injection of arbitrary OS commands as a root user * Changing firewall configurations to allow communication with “internal network”   **Post-exploitation**   * Pivoting |  |
| 28 | Team Peanut | Shayne Low  Ray ‘En | CSF02  CSF02 | 90725505  96547623 | **Project Title:**  Reverse Shell Sessions | **Case Scenario**  Tom is an experienced ethical hacker. While browser the internet he came across an ad-scam stating that Tom’s machine has been infected by a malware and requires immediate attention. Knowing well that this was a scam, Tom wanted to expose these tech support scammers and locate their base of operation by conducting a reverse remote attack.  Tom went ahead to set up at Windows 10 virtual machine and called the ad-scam to carry out his act.  The scammer who identifies himself as Rajeeb Kumar told Tom that he needs to install a remote access software to gain access to Tom’s virtual machine. This allows Rajeeb to then carry out his scam, such as showing fake malicious files and websites that ‘prove’ Tom has been infected. Rajeeb will then install his backdoor on Tom’s computer so that he can have a persistent connection to Tom’s network. Rajeeb will then give a spoofed website link for Tom to enter his bank credentials to pay for services, where the credentials will be dumped in his own file server.  *Tom (Victim/Ethical Hacker)*  *Rajeeb Kumar (Scammer/Attacker)*  **Scenario Diagram**        **Set-Up (Details subject to change during assignment**  2 Windows 10 VM (Victim & Client)  1 Kali Linux 2021 VM 1 Simple HTTP Web Server hosted on Kali (NOT BEING PENTESTED, JUST TO HOST SPOOFED WEBSITE)  Linux File Server (Debian 10.7.0)  **Vulnerabilities** CVE-2017-8759   * Microsoft .NET Framework 2.0, 3.5, 3.5.1, 4.5.2, 4.6, 4.6.1, 4.6.2 and 4.7 allow an attacker to execute code remotely via a malicious document or application, aka ".NET Framework Remote Code Execution Vulnerability."   **Post-exploitation Activities**   1. Network Scanning 2. Pivoting to the Attacker’s File Server 3. Installing a backdoor 4. Credential Dumping |  |