1 page document

Include:

* Students' Names and Numbers
* Vulnerability - CVE-2019-0708 - Bluekeep
  + Basic description of vulnerability
  + How you plan to demonstrate the exploit

Sources that can be used to research:

<https://www.youtube.com/watch?v=AkXM2wywMN0>

<https://www.cvedetails.com/cve/CVE-2019-0708/>

<https://www.zerodayinitiative.com/blog/2019/5/27/cve-2019-0708-a-comprehensive-analysis-of-a-remote-desktop-services-vulnerability>

<https://www.csa.gov.sg/singcert/alerts/microsoft-remote-desktop-services-remote-code-execution-vulnerability-cve-2019-0708>

<https://www.cyber.gov.au/acsc/view-all-content/alerts/microsoft-windows-security-vulnerability-bluekeep-cve-2019-0708>

<https://www.avanet.com/assets/pdf/sophos-security-rdp-exposed-the-threats-thats-already-at-your-door-en.pdf> → Shows how many devices are affected and can be used to substantiate why the vulnerability is critical (for assignment 2)

<https://www.youtube.com/watch?v=Uua3Ed7W7-k> → This just shows us the metasploit way so we cannot apply it to our actual exploit but we can use it as reference

<https://www.exploit-db.com/exploits/47416> → also metasploit but shows us the payload used

<https://github.com/CVE-2019-0708/CVE-2019-0708> → POC

<https://www.zerodayinitiative.com/blog/2019/5/27/cve-2019-0708-a-comprehensive-analysis-of-a-remote-desktop-services-vulnerability> → explains in further detail how RDP works (we can use it in assignment 2)

<https://github.com/rapid7/metasploit-framework/pull/12283> → explains in further detail how RDP works (we can use it in assignment 2)

**Paul’s Wine Network**

BlueKeep CVE-2019-0708

Group Members: Hannah Mahalia Manalac Susanty (33329151)

Siti Hajar Binte Abdul Malek (33249812)

Lee Jihu (34061648)

**Summary of Vulnerability**

CVE-2019-0708 also known as BlueKeep is a vulnerability to execute arbitrary code remotely without having to go through normal authentication steps using Windows Remote Desktop Services (RDS). The RDS allows a user to access a remote computer or virtual desktop over the network. BlueKeep was discovered in Microsoft’s Remote Desktop Protocol (RDP) (Chavez, 2019) and affects several operating systems, such as Windows Vista, Windows 7 and Windows XP. This vulnerability has a CVSS score of 9.8 indicating that it is a critical vulnerability that severely affects the confidentiality, integrity and availability of data (National Vulnerability Database, 2019).

The exploitation of this vulnerability requires the attacker to penetrate the target host system using Remote Desktop Protocol and remotely send codes that are specially crafted. After successfully injecting the codes into the kernel, the attacker could have control of the target system and could then have access to create accounts with full rights, install malicious softwares, and read, edit and delete data. (Singapore Computer Emergency Response Team, 2019) The biggest characteristic of the BlueKeep vulnerability is that it could be used in the exploitation of other vulnerabilities or amplify existing malware, such as WannaCry by allowing these malware to self propagate without any human interaction similar to a worm (Heller, 2019).

**Proposed Demonstration of Exploit**

The 64 bit Windows 7 operating system is required for the demonstration of exploitation. The Remote Desktop Protocol service has to be enabled in the target device as it is known to be vulnerable to CVE-2019-0708. A payload will be sent to the target which will cause blue screen of death (BSOD) errors.

**References**

Chavez, A. (2019, July 9). *An Overview of Bluekeep*. Retrieved from Silent Sector Expertise-Driven Cyber Security: https://www.silentsector.com/blog/an-overview-of-bluekeep-cve-2019-0708

Heller, M. (2019, June). *BlueKeep (CVE-2019-0708)*. Retrieved from Search Security Tech Target: https://searchsecurity.techtarget.com/definition/BlueKeep-CVE-2019-0708

National Vulnerability Database. (2019, May 16). *CVE-2019-0708 Detail*. Retrieved from National Institute of Standards and Technology: https://nvd.nist.gov/vuln/detail/cve-2019-0708

Singapore Computer Emergency Response Team. (2019, May 15). *Microsoft Remote Desktop Services Remote Code Execution Vulnerability (CVE-2019-0708)*. Retrieved from Cyber Security Agency of Singapore: https://www.csa.gov.sg/singcert/alerts/microsoft-remote-desktop-services-remote-code-execution-vulnerability-cve-2019-0708