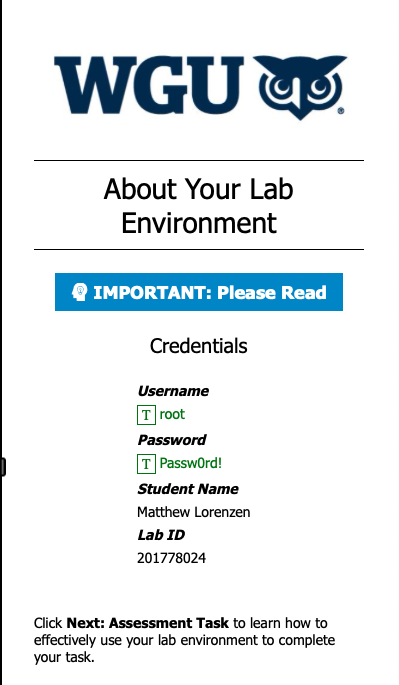
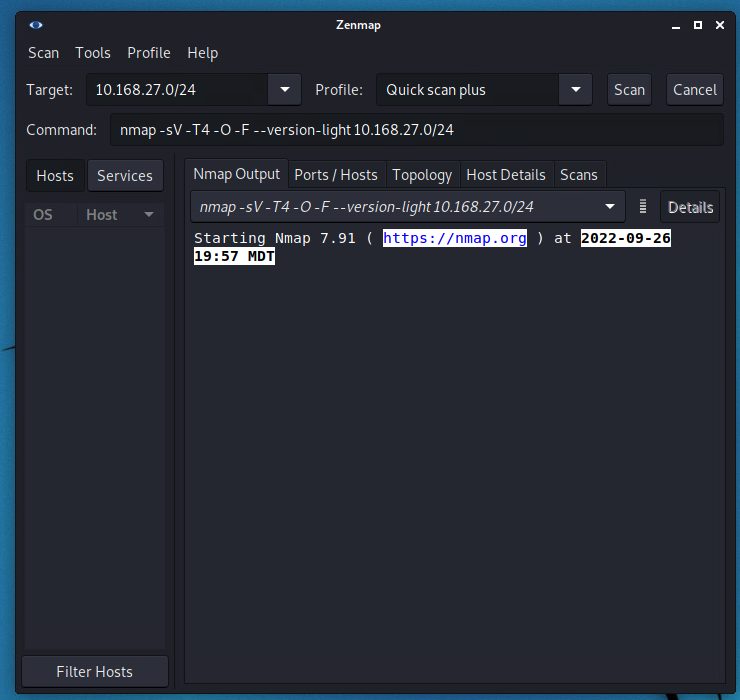
**Getting Started Task 1 Template**

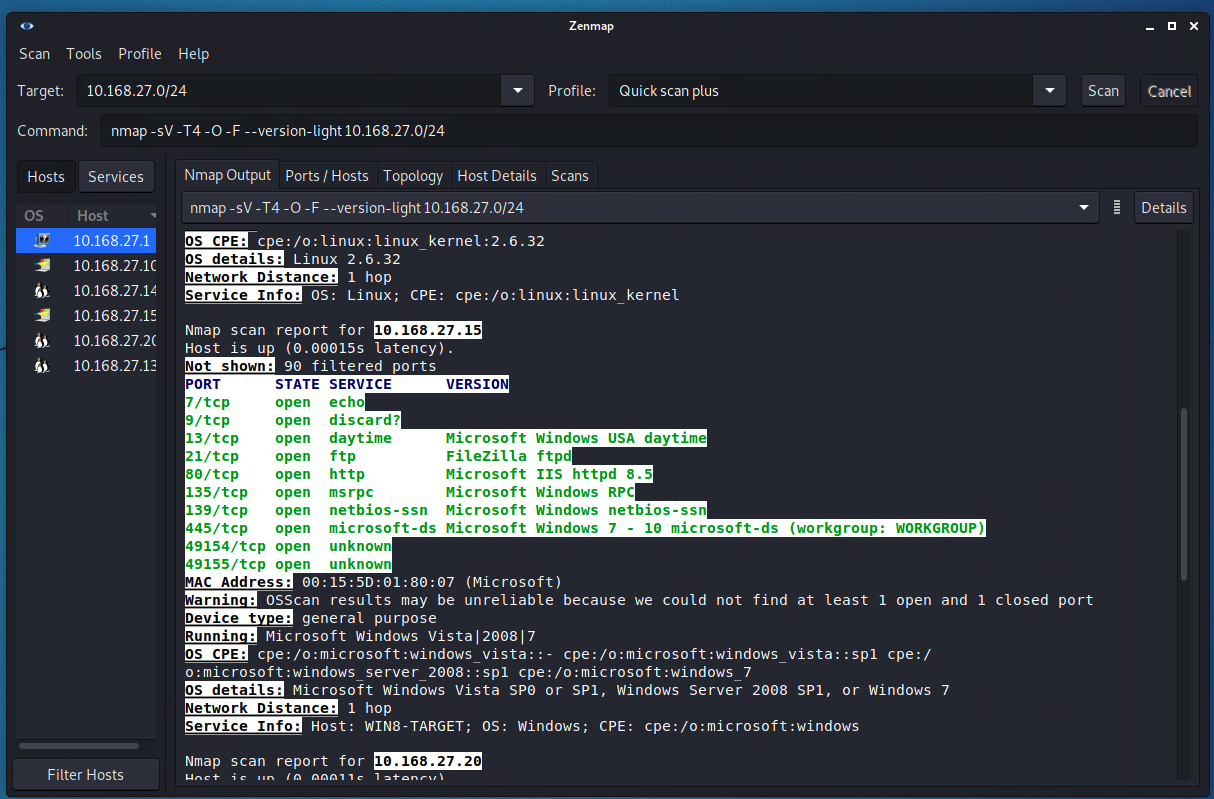
Use the template outline below to capture the rubric requirements and key points and to serve as your task report. After you have captured the appropriate data, massage each section into the required number of paragraphs and ensure you have captured all the required points highlighted.

1. **Network Topology**

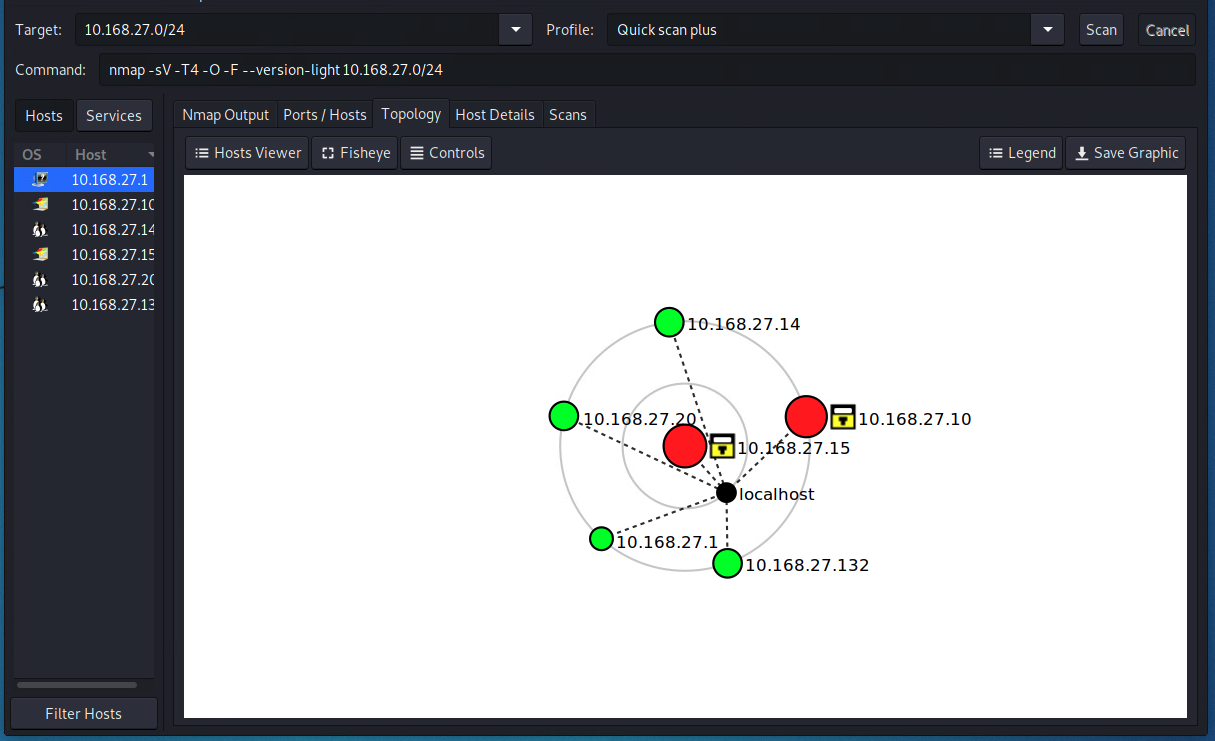


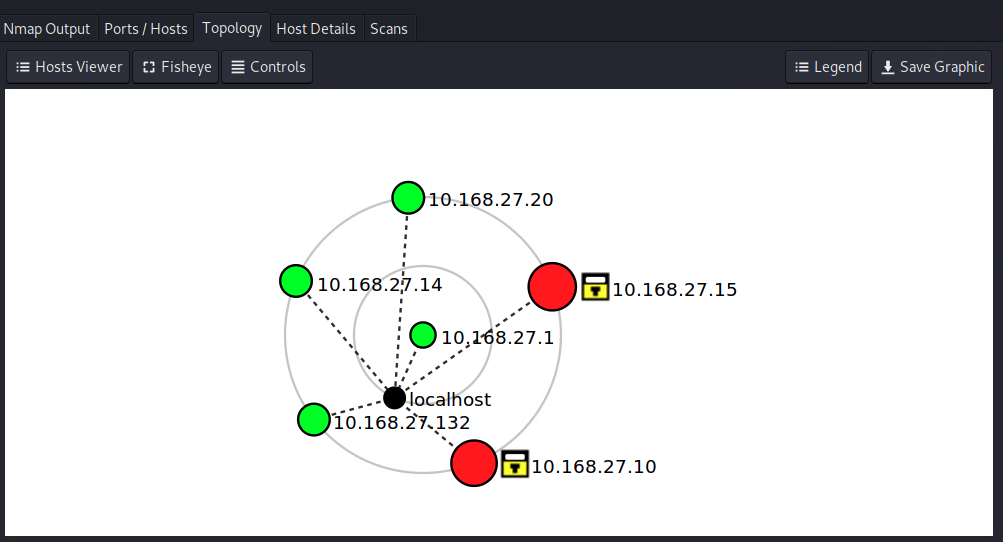
Screenshots of running nmap.





Screenshot of Zenmap Topology

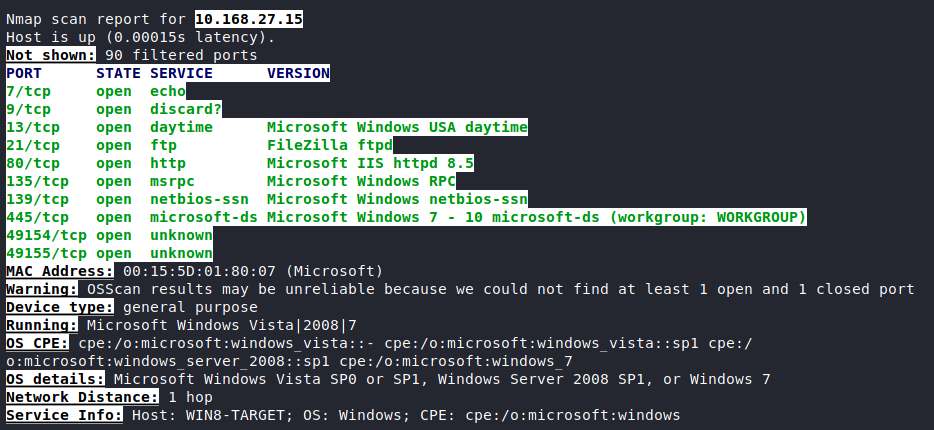




**B Summary of Vulnerabilities and Implications**

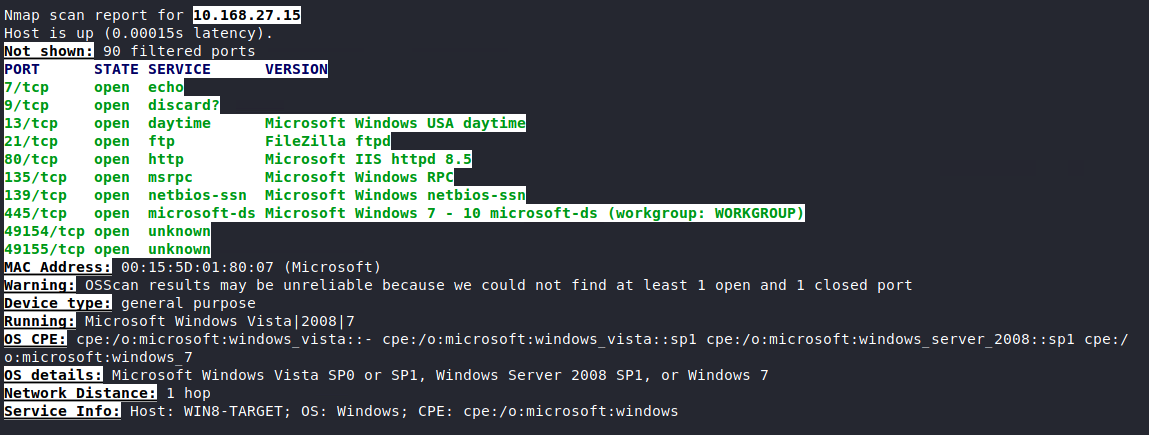
**First vulnerability**

Windows 7 – SMB Remote Code Execution vulnerability (*CVE - CVE-2017-0144*)



**Second vulnerability**

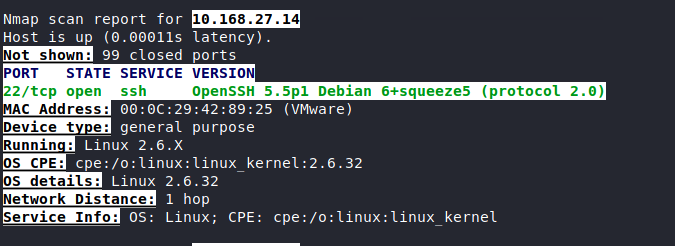
Windows MSRPC – Information Disclosure vulnerability – Allows for further compromise a system, attacker can then run customer scripts and applications. (*CVE - CVE-2018-8407*)



**Third vulnerability**

And the potential implications

OpenSSH 5.5pl – Allows remote servers to obtain sensitive information from memory by requesting buffer by reading the private key (*CVE - CVE-2016-0777*)

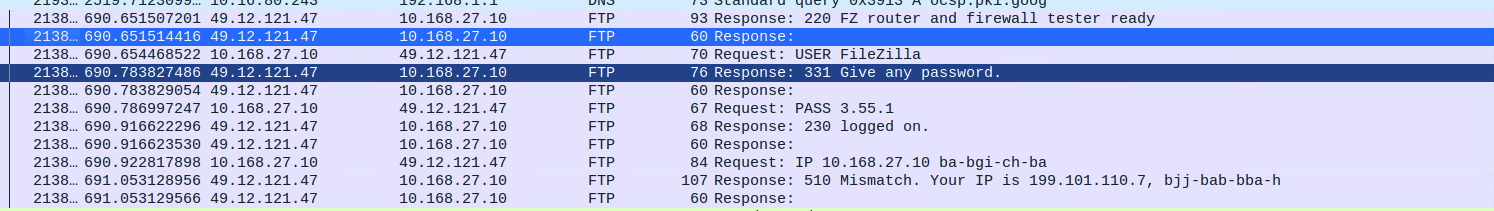


**C. Wireshark Anomalies**

**First Anomaly**

And evidence, plus the range of packets

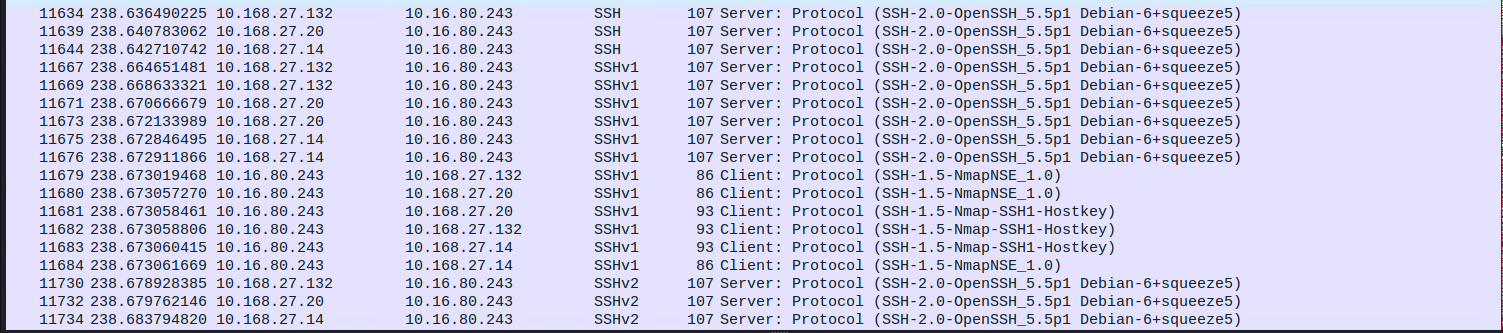
FTP (FileZilla) – Buffer Overflow allowing for remote authenticated attackers to cause a denial of service and remote code execution. (*CVE - CVE-2006-2173*)



**Second Anomaly**

And evidence, plus the range of packets

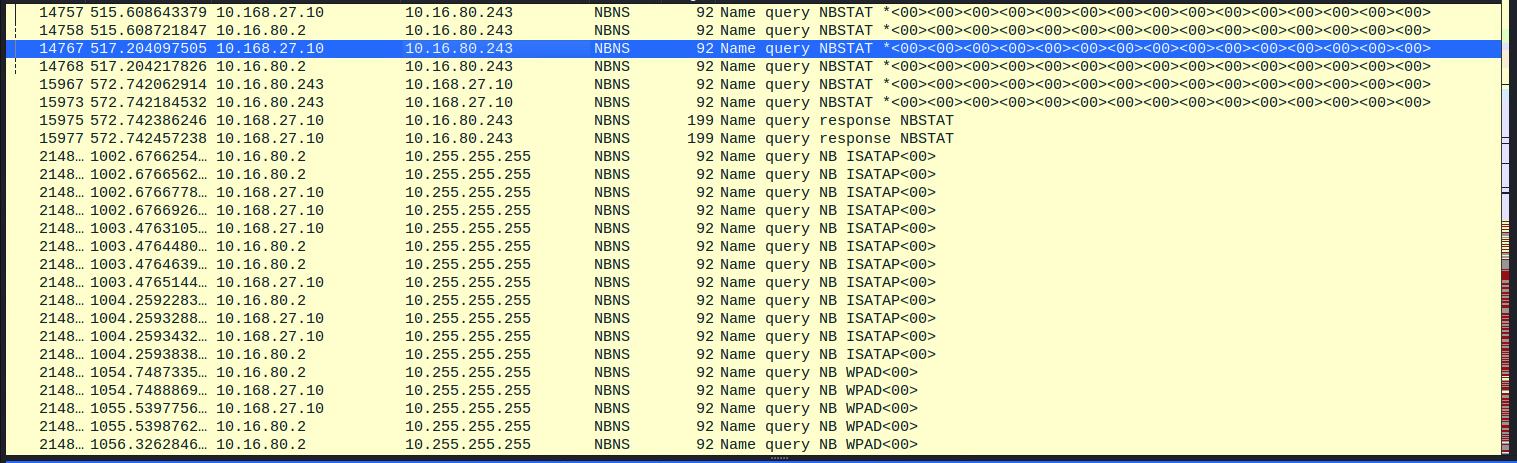
SSHv1 OpenSSH 5.5pl – Allows remote servers to obtain sensitive information from memory by requesting buffer by reading the private key (*CVE - CVE-2016-0777*)



**Third Anomaly**

And evidence, plus the range of packets

Heap-based buffer overflow in the nbns\_spoof function allows for remote denial of service or possible remote code execution. (*CVE - CVE-2014-9377*)



**D. Implications of each Wireshark Anomaly**

**Implications of taking no action 1**

By leaving this anomaly exposed the organization could suffer a potential remote code execution that will allow the attacker to traverse the directory structure on the victim machine. (*NVD - CVE-2006-2173*)

**Implications of taking no action 2**

By leaving this anomaly exposed the organization is at risk for the victim machines memory to be compromised allowing the attacker to read private keys. This can lead to privilege escalation and pivoting on the network. (*NVD - Cve-2016-0777*)

**Implications of taking no action 3**

Leaving this vulnerability un-remediated leaves, the organization at risk for a denial-of-service attack through the Ettercap 8.1 tool. (NVD - CVE-2014-9377)

**E. Recommended Solutions**

**First Vulnerability**

Recommend solution which is supported by a reliable source

The recommended solution is to patch with either the Security Only or Monthly rollup (KB4012216/KB4012212) provided from Microsoft. (*Security Update Guide - Microsoft Security Response Center*)

**Second Vulnerability**

Recommend solution which is supported by a reliable source

The recommended solution from Microsoft would be to patch the system using KB4462927 from Microsoft (*Security Update Guide - Microsoft Security Response Center*)

**Third Vulnerability**

Recommend solution which is supported by a reliable source

The recommended solution for OpenSSH 5.5pl would be to upgrade systems to GPFS V3.5.0.31 or by disabling “UseRoaming” in the ssh\_config file. (*Security Bulletin: Vulnerabilities in OpenSSH Affect GPFS V3.5 for Windows (CVE-2016-0777, CVE-2016-0778)*)

**First Anomaly**

Recommend solution which is supported by a reliable source

FTPD FileZilla vulnerability, the recommendation to mitigate is to patch the FileZilla client to version 2.23 or later. (*FileZilla PORT and PASS Command Denial of Service CVE-2006-2173 Vulnerability Report*)

**Second Anomaly**

Recommend solution which is supported by a reliable source

The recommended solution for OpenSSH 5.5pl would be to upgrade systems to GPFS V3.5.0.31 or by disabling “UseRoaming” in the ssh\_config file. (*Security Bulletin: Vulnerabilities in OpenSSH Affect GPFS V3.5 for Windows (CVE-2016-0777, CVE-2016-0778)*)

**Third Anomaly**

Recommend solution which is supported by a reliable source

To prevent nbns\_spoofing an organization would need to implement a combination of network traffic filtering and host-based security, configured to block traffic not necessary to the infrastructure. By further applying extended Access Control Lists to block outside or untrusted network traffic. (*Filter Network Traffic, Mitigation M1037 - Enterprise | MITRE ATT&CK®*)

**References**

Compile all references used in the paper here, deduplicated, and in order of the author’s last name

*CVE - CVE-2014-9377*. cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9377. Accessed 26 Sept. 2022.

*CVE - CVE-2016-0777*. cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0777. Accessed 26 Sept. 2022.

*CVE - CVE-2006-2173*. cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2173. Accessed 26 Sept. 2022.

*CVE - CVE-2018-8407*. cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8407. Accessed 26 Sept. 2022.

*Security Update Guide - Microsoft Security Response Center*. msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-8407. Accessed 26 Sept. 2022.

*CVE - CVE-2017-0144*. cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144. Accessed 26 Sept. 2022.

*NVD - CVE-2006-2173*. nvd.nist.gov/vuln/detail/CVE-2006-2173. Accessed 26 Sept. 2022.

*NVD - Cve-2016-0777*. nvd.nist.gov/vuln/detail/cve-2016-0777. Accessed 26 Sept. 2022.

*NVD - CVE-2014-9377*. nvd.nist.gov/vuln/detail/CVE-2014-9377#vulnCurrentDescriptionTitle. Accessed 26 Sept. 2022.

*---*. msrc.microsoft.com/update-guide/vulnerability/CVE-2017-0144. Accessed 26 Sept. 2022.

*Security Bulletin: Vulnerabilities in OpenSSH Affect GPFS V3.5 for Windows (CVE-2016-0777, CVE-2016-0778)*. [www.ibm.com/support/pages/security-bulletin-vulnerabilities-openssh-affect-gpfs-v35-windows-cve-2016-0777-cve-2016-0778. Accessed 26 Sept. 2022](http://www.ibm.com/support/pages/security-bulletin-vulnerabilities-openssh-affect-gpfs-v35-windows-cve-2016-0777-cve-2016-0778.%20Accessed%2026%20Sept.%202022).

*FileZilla PORT and PASS Command Denial of Service CVE-2006-2173 Vulnerability Report*. exchange.xforce.ibmcloud.com/vulnerabilities/26303. Accessed 26 Sept. 2022.

*Filter Network Traffic, Mitigation M1037 - Enterprise | MITRE ATT&CK®*. attack.mitre.org/mitigations/M1037. Accessed 26 Sept. 2022.