# Virtual Machine Cyber Risk Assessment

For Old Dominion University

December 16, 2022

By:

Aaron Hernandez, CyberSecurity

Evan Liu Phillips, CyberSecurity

Elija Bullock, Computer Engineering

Furkan Ilgin, Electrical Engineering

ahern020@odu.edu, eliup001@odu.edu,
ebull001@odu.edu, filgi001@odu.edu

# Document Properties

| | |
|---|---|
| **Title** | Virtual Machine Cyber Risk Assessment Report |
| **Version** | 1.0 |
| **Authors** | Aaron Hernandez, Evan Liu Phillips, Elija Bullock, Furkan Ilgin |
| **Classification** | Classified |

# Version Control

| **Version** | **Date** | **Authors** | **Description** |
|---|---|---|---|
| V1.0 | December 16, 2022 | Aaron Hernandez, Evan Liu Phillips, Elija Bullock, Furkan Ilgin | Final Draft |

ahern020@odu.edu, eliup001@odu.edu,
ebull001@odu.edu, filgi001@odu.edu

# Table of Contents



# List of Tables and Figures

## Tables



## Figures



ahern020@odu.edu, eliup001@odu.edu,
ebull001@odu.edu, filgi001@odu.edu

# 1. Executive Summary

This report covers the risk/vulnerability assessment performed on Old Dominion University's virtual machines on the CCI pool. The objective of the assessment was to find potential vulnerabilities within the CCI pool's virtual machines, exploit them and then define and categorize them on severity.

## 1.1 Scope of work

This risk assessment covers four of the virtual machines on the CCI pool: Windows 7, Ubuntu, Metasploitable, and Windows XP(192.168.10.9, 192.168.10.10, 192.168.10.11, 192.168.10.14). These virtual machines were scanned with no prior knowledge of potential vulnerabilities or weaknesses.

## 1.2 Project Objectives

The four virtual machines were scanned and multiple vulnerabilities were discovered, ranging from low to critical severity. Vulnerabilities found entailed unsupported operating systems among multiple virtual machines, weaknesses in the Remote Desktop Protocol, and flaws in software installations that if gone unchecked could allow a bad actor to execute malicious code or gain control of the machine.. All four virtual machines in the CCI pool have been assessed to have vulnerabilities, although some of them had less vulnerabilities than others.

## 1.3 Assumption

While writing this report, we assumed that all 4 IP addresses were considered to be public IP addresses. Furthermore, we assumed that these scans were following the code of ethics.

## 1.4 Timeline

The timeline of our assessment is as below:

| Vulnerability Test | Start Date/Time | End Date/Time |
|---|---|---|
| Test 1 | 10/25/2022 | 12/16/2022 |

*Table 1- Vulnerability Testing Timeline*

ahern020@odu.edu, eliup001@odu.edu,
ebull001@odu.edu, filgi001@odu.edu

# 1.5 Summary of Findings

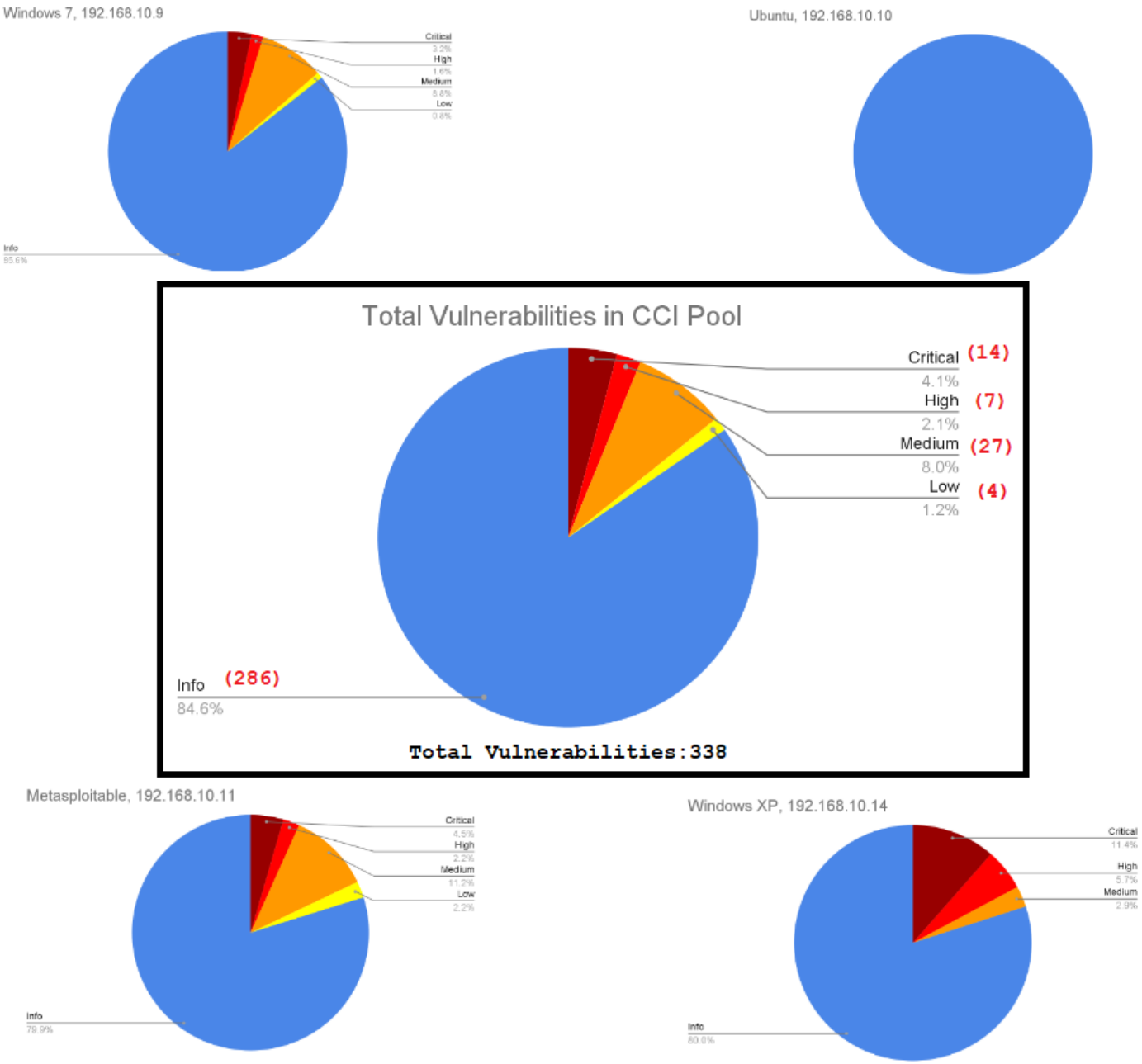



*Figure 1- Total Overview of Vulnerabilities*

In summary, when percentages of vulnerabilities are analyzed it is clear that Windows XP has the highest percentage of critical vulnerabilities. Windows XP users need to pay more attention to information security and data storage. If an attacker accesses one of the servers, they could corrupt the data or steal some information from the user.

| Vulnerability | Windows 7 | Ubuntu | Metasploitable | Windows XP |
|---|---|---|---|---|
| Critical | 4 | 0 | 6 | 4 |
| High | 2 | 0 | 3 | 2 |
| Medium | 11 | 0 | 15 | 1 |
| Low | 1 | 0 | 3 | 0 |
| Info | 107 | 44 | 107 | 28 |

*Table 2- Vulnerability Table*

On the other hand, as a result of our Nessus scan, as it can be seen from the table above, we could not find any vulnerabilities in Ubuntu.While this does not mean that Ubuntu is absolutely safe, compared to other 3 OS's analyzed in this experiment, it is possible to assume that it is safer. There are no critical vulnerabilities reported.

# 2. Methodology

For the following results, Nessus on the Kali internal workstation was used. A new project was created in the Nessus page where the IP addresses of the target virtual machines were inputted and the project was run through an advanced scan. The virtual machines were scanned by each of the four group members to get maximum results.

| **Vulnerability Name** | **CVSS Score** | **Vulnerable Service** | **Scenario** |
|---|---|---|---|
| Microsoft Windows Server Service Crafted RPC Request | CVSS 10 | OS | Attackers are able to gain remote access can run arbitrary code and overflow the OS |
| Open SSH Package Random Number Generator | CVSS 10 | SSH | Hackers are able to easily acquire the private portion of the remote Key. Once gained they are able to use this to decrypt the remote session. |
| MB Buffer Overflow Remote Code Execution Vulnerability. | CVSS 10 | SMB | Remote attackers are able to execute arbitrary code via malformed values of unspecified SMB packets. This can cause a buffer overflow sequence. |
| Bind Shell Backdoor Detection | CVSS 9.8 | SHELL | Attackers can use an unauthenticated shell and connect to the remote port and send commands. |
| Apache Tomcat AJP Connector Request Injection | CVSS 9.5 | HTTP | Hackers are able to exploit this vulnerability and gain access to red web files from a vulnerable server. They will also be able to upload malicious code and gain remote access. |
| NFS Exported Share Information | CVSS 7.5 | OS | Hackers are able to easily mount a NFS file system even if its denied on the access list. |
| Bind Server | CVSS 5.9 | DNS | An attack can either guess or know the TSIG Key and can gain remote access to the device due to a bind server vulnerability |

*Table 3- Ranked Vulnerabilities*

# 3. Detailed Findings

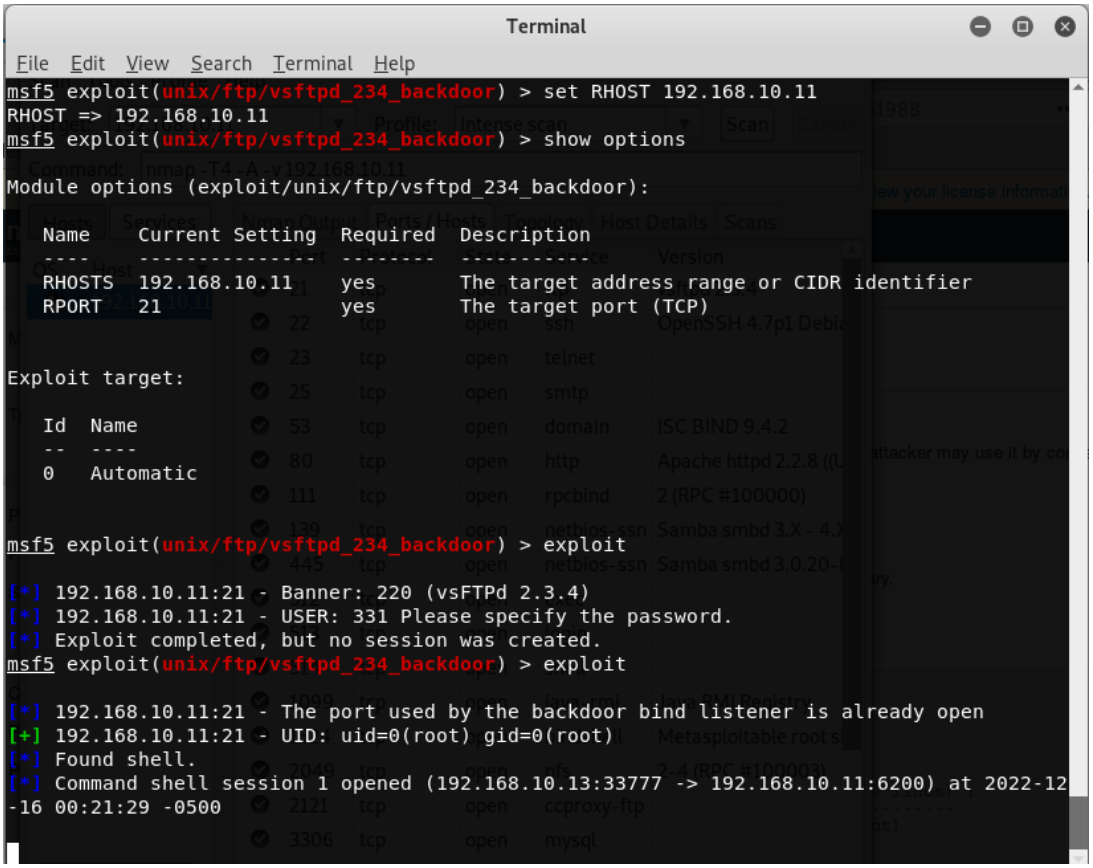
Detailed tables consisting of open ports from the target virtual machines are attached in the supplementary document. Referral to Table 3 above gives insight to the most severe vulnerabilities discovered through the Nessus scan. Most of the top severity vulnerabilities found have severe repercussions if exploited, as the nature of the exploit can allow attackers to execute code with privilege and gain access to the system. Consequences of potential exploits include loss of data and confidentiality, having attackers gaining access to privileged shells, and loss of company integrity.

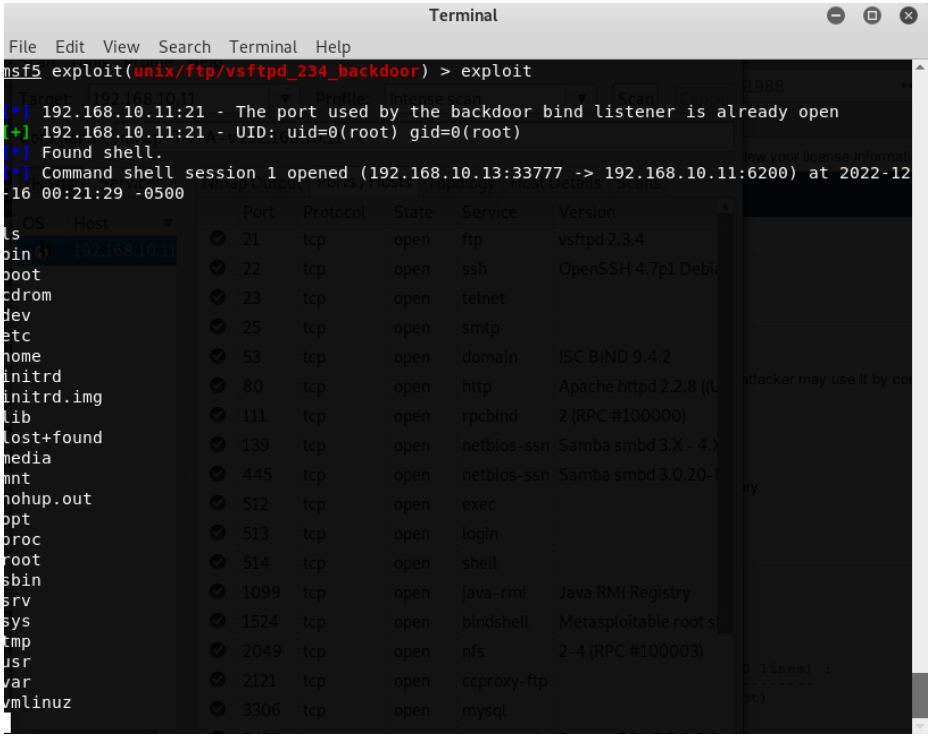
Many of these vulnerabilities can be abated by updating/upgrading the operating system to a supported version, reinstalling bad installations of software, and better firewall structure and filtering.

To further verify the discovered vulnerabilities, Metasploit was used to test several of the vulnerabilities per virtual machine.

- **Metasploitable(192.168.10.11) Exploitation**

*[192.168.10.11: open port 21 vsftpd 234 remote shell vulnerability]*
Version 2.3.4 of vsftp had a backdoor that was slipped into the servers hosting the source code by an unknown person. Thisversion of VSFTP included on the Metasploitable VM contains a vulnerability that opens a backdoor shell. If a user attempts to connect using a username that ends in a smiley :), it opens a backdoor shell.
This vulnerability allows the user to obtain a root shell, which means it can view the contents of files, modify things, corrupt files, all by attempting to login with a username ending in :). Even though the login attempt is unsuccessful it will still allow the user to perform the task mentioned above.




*Figures 2&3- Exploitation of Metasploitable: Open Port 21*

- **192.168.10.11: VNC Weak Password Vulnerability**

VNC (Virtual network Computing) package is a remote, graphical interface.The authentication system developed by VNC has a weak encryption algorithm, which means it can be brute-forced easily. A static key is used, and all passwords are truncated to 8 characters. If the encrypted passwords are obtained, then it would be easy to decrypt them.If this vulnerability is successfully exploited,an attacker could gain remote access to the host.

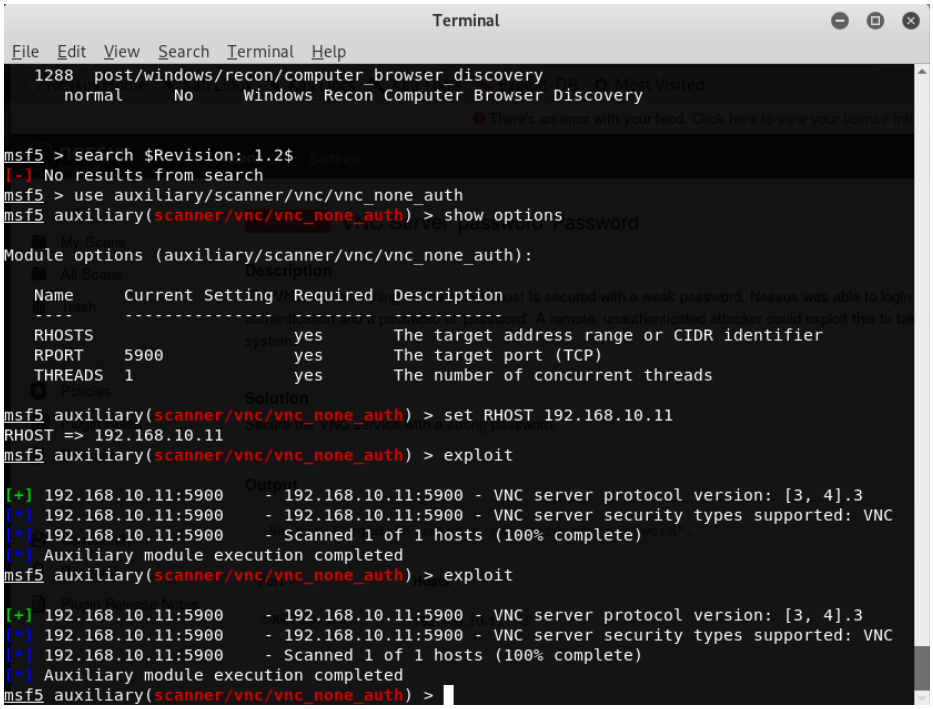



*Figure 4- Metasploitable Cont. VNC*

- **Windows XP(192.168.10.14) Exploitation**

*[192.168.10.14: MS08-067 Vulnerability]*

Vulnerability in Server Service Could Allow Remote Code Execution (958644).This vulnerability allows remote code execution if an affected system received a specially crafted RPC request. Especially on Windows XP, and Windows Server 2003 systems, an attacker could easily exploit this vulnerability without authentication to run arbitrary code.

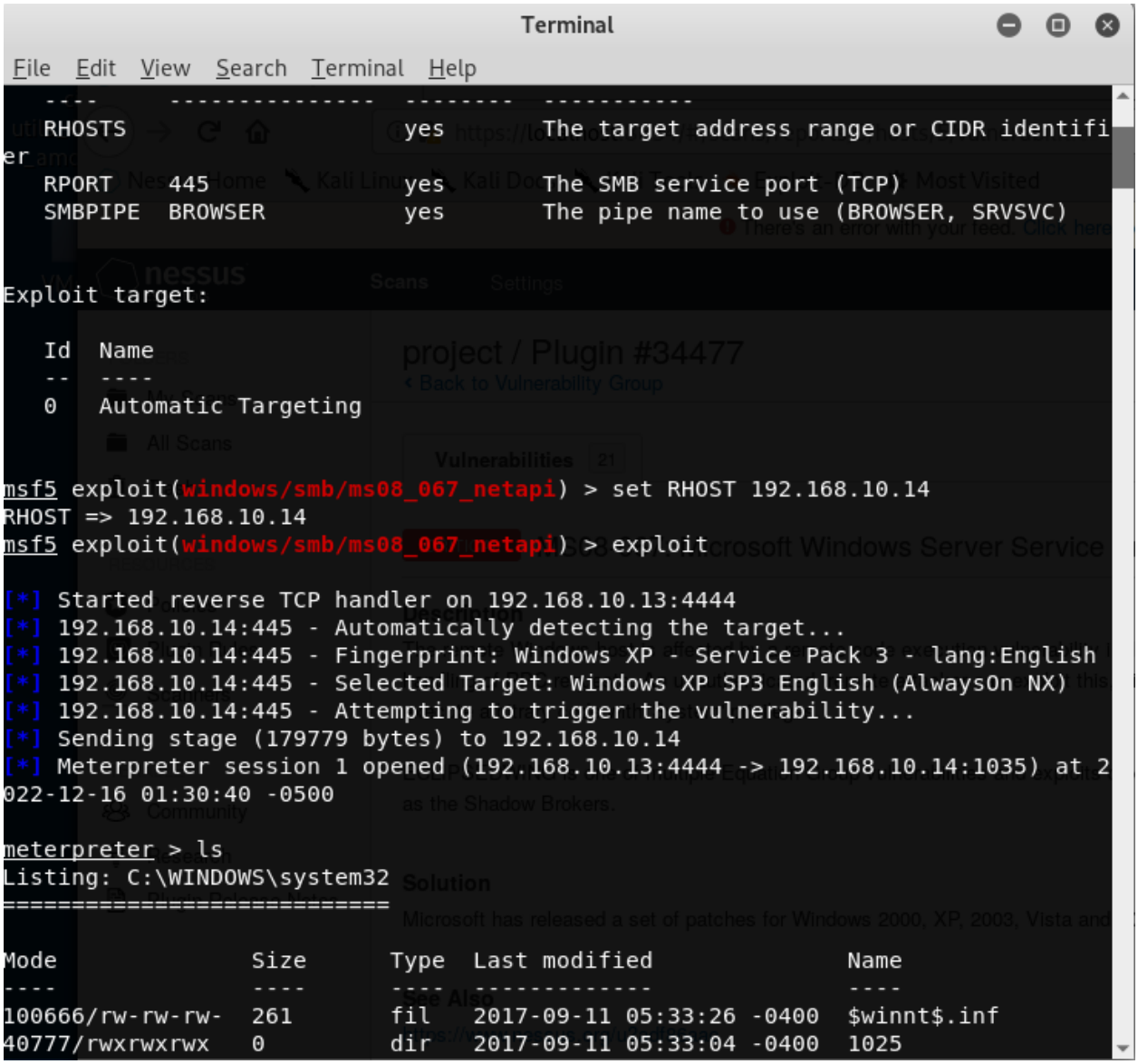



*Figure 5- XP Remote Code Execution Exploitation*

*[192.168.10.14 MS17-10 vulnerability]*.

Remote code execution vulnerabilities exist in the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests. Microsoft Windows SMB Server is prone to a remote code-execution vulnerability. Successful exploits will allow an attacker to execute arbitrary code on the target system. Failed attacks will cause denial of service conditions. Related CVE's: CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148

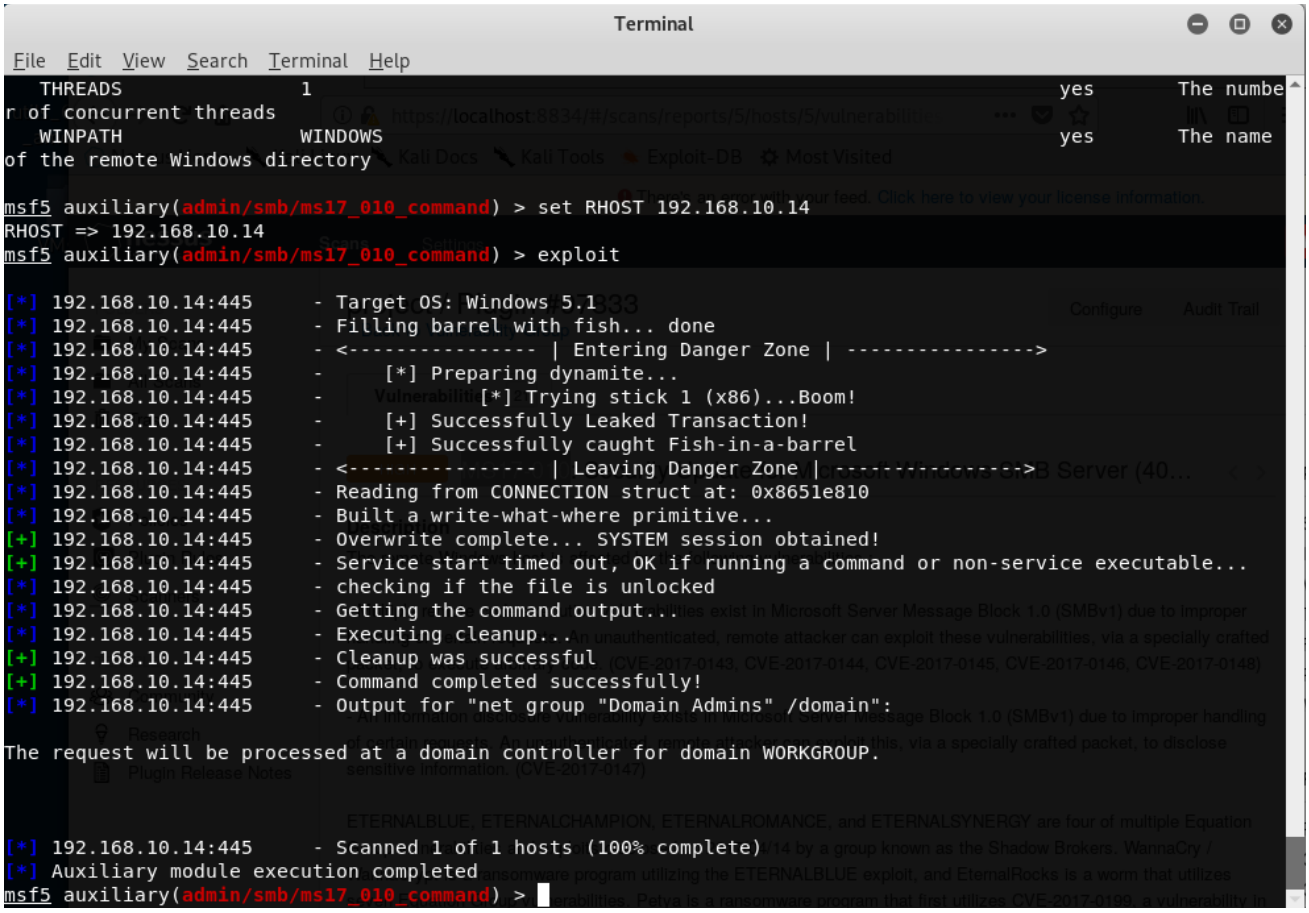



*Figure 6- XP SMB1.0 Execution Exploit*

- **Windows 7 Vulnerability Exploitation**

*[192.168.10.9: MS12-020 Vulnerability.]*

An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. This vulnerability exists,because RDP accesses an object in memory that has been improperly initialized or has been deleted.

If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it. So eventually it will take over the control.

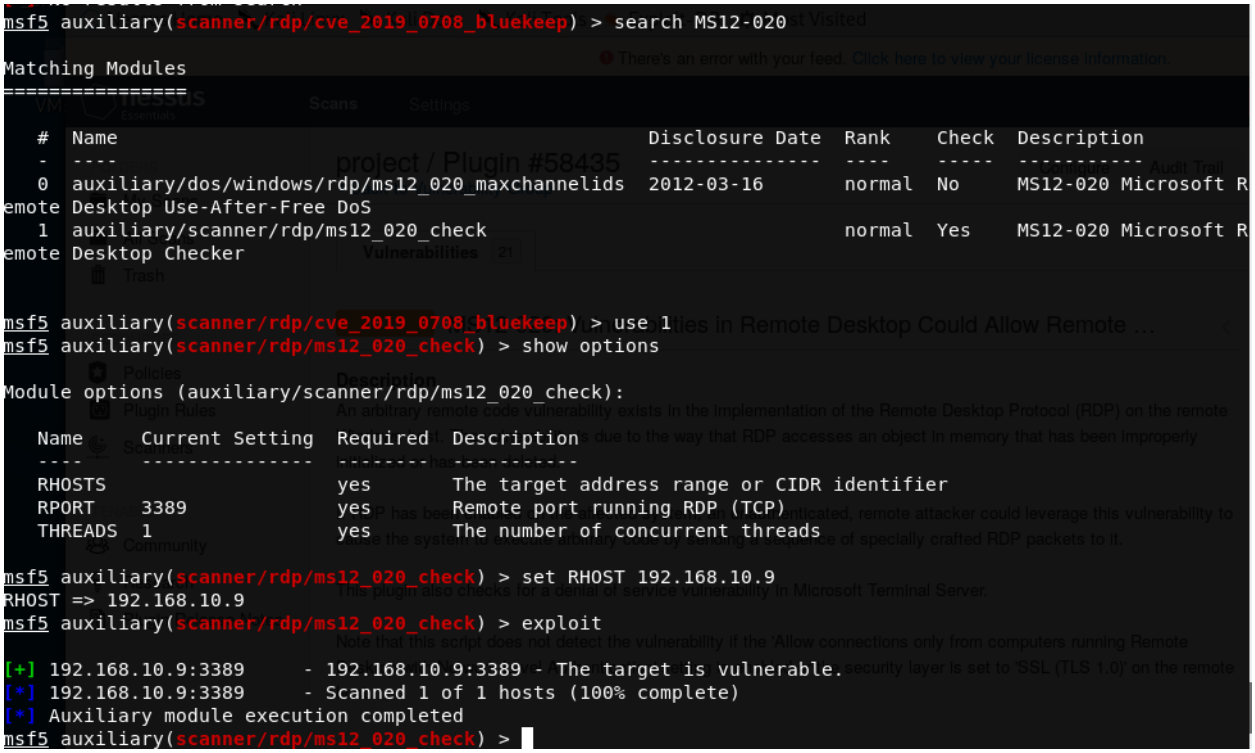



*Figure 7- Windows 7 MS12-020 Exploit*

# 4 Reference

*NIST National Vulnerability Database.* NVD. (n.d.). Retrieved December 15, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2020-1938

*NIST National Vulnerability Database.* NVD. (n.d.). Retrieved December 15, 2022, from https://nvd.nist.gov/vuln/detail/cve-2008-4250

*NIST National Vulnerability Database*. (n.d.). Retrieved December 15, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2020-8617

*NIST National Vulnerability Database.* NVD. (n.d.). Retrieved December 15, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2008-0166#vulnCurrentDescriptionTitle

*NIST National Vulnerability Database.* NVD. (n.d.). Retrieved December 15, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2008-0166

*NIST National Vulnerability Database.* NVD. (n.d.). Retrieved December 15, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2020-1745

ahern020@odu.edu, eliup001@odu.edu,
ebull001@odu.edu, filgi001@odu.edu