XYZCorp HQ Penetration Test Report

Ryan Morganti

CSC 436

**Executive Summary**

A network security test was conducted against the internal computers at XYZCorp HQ in December of 2022. This report details the methodologies, findings, and remediations for said network. A total of 6 hosts were discovered and tested.

**Key Findings:**

Of the various findings, we discovered several that may be exploitable by a malicious actors. Some of the most important are as follows:

* A vulnerability in the webserver that allows command execution
* A vulnerability in the ftp server version that allows remote access
* The use of unpatched, outdated systems
* Plain text passwords on systems that could allow an attacked user account access

**Recommendations:**

We recommend that XYZCorp HQ undertake the following:

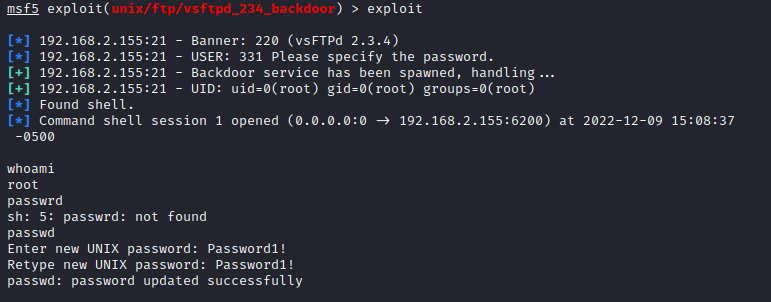
* Review the webserver code to disallow additional, unclean input
* Update vsftp to a patched version
* Perform an update and review of Windows XP uses and perform an increased firewall around the computer
* Perform a review of user’s files and storage of passwords in clear text.

# Attack Narrative

We started the test by first scanning the network to enumerate the hosts and discover open ports. Based on the initial information and the results from the nmap scan, we determined that there are 6 active hosts, 3 Linux based, and 3 Windows based. With this information we decided to attack the Linux portion first and then the Windows hosts second.

Host 192.168.2.155 – FTP Server

From the nmap scan we determined that the client was using vsftpd version 2.3.4 which has a vulnerability that an attacker can exploit to get root access on the machine. Using this exploit, we were able to get remote access and change the root password on the machine.



With credential access to the root user, we were able to enter in over ssh and explore the machine. After enumerating the file system, and bash history we were able to determine what previously was run and any important files.

Text

Description automatically generated

Based on the bash history, we discovered that an RSA key is stored as plain text and is used to authenticate to user dsu on a different Linux host. We then proceeded to rerun the command and gained access onto a new host.

Host 192.168.2.20 – Linux 3

We gained access to this host from the FTP server using the saved RSA credentials and ssh.

Text

Description automatically generated

From there we enumerated the file system and found an executable and source code called runme. We examined the file and determined that it created root level access when executed. Using the source code, we figured out that the required input was a y, which when entered during run time dropped you into a root shell.

A screenshot of a computer screen

Description automatically generated

Host 192.168.2.224 – Web Server

Initially we opened the web server that is hosted on this machine to look at the site. The site itself allows a chaining of commands in the input field. By adding an ; at the end and then typing a Linux command, the results of that command are executed and returned to the screen. An attacked could use this to run malicious commands or get a shell to that machine. We created a php web delivery attack that when pasted into the input field and submitted will return a shell back to our meterpreter session. The results are documented below, with full access to the www-data user on said machine.

Text

Description automatically generated

Host 192.168.2.202 – Windows XP

Switching over to the windows machines, we started with the XP machine as it was the most likely to be exploitable due to it running an older operating system. Since the nmap scan returned that port 445 was accessible, a smb exploit could be possible. This was further investigated, and an exploit of ms17\_010 was tried against the host. The results yielded an active shell session on the host machine.

Text

Description automatically generated

Within this shell session, we enumerated the file system and did not find anything interesting. We then launched the incognito extension and listed the active user tokens on the machine. We discovered a domain username dwigt on the machine and attempted to impersonate him and gain access to his account on the local machine.

Text

Description automatically generatedText

Description automatically generated

After gaining this access, we discovered that dwigt is a domain administrator account, so we were able to use this to further our access to the domain. Using his permission level we created a new domain net user with a password known to us. We then added this user to the Domain Admins group which would give us access and privileges on other computers with the same domain.

Text

Description automatically generated

Text

Description automatically generated

With this created, we then turned our attention to the other windows machines on the network.

Host 192.168.2.147 – Windows 10

We also determined from the initial nmap scan that this host had an open smb port. To gain access we ran the smb/psexec exploit with the credentials set for the newly created domain admin user. This dropped us directly into a shell on the machine with full access control.

Text

Description automatically generated

With this access, we started enumerating the file system and discovered a powershell script living on the user mike’s desktop. Within this script was his plain text password. We copied this password and went to attack the domain controller using his account.

A screenshot of a computer

Description automatically generated with medium confidence

Host 192.168.2.100 – Domain Controller

Having the user mike’s credentials, we again tried the smb/psexec exploit as before but with updated credentials. Like before this dropped us into a shell on the domain controller.

Text

Description automatically generated

Once we had access to the domain control, we enumerated the file system and found the flag and password file on the administrators desktop.

Text

Description automatically generated

# Findings & Remediation

Below is a list of vulnerabilities, their rating, and their remediation all broken down by host.

192.168.2.155

vsFTP 2.3.4 – CVSS Score: 10.0. Remediation of updating to a newer version of vsFTP.

192.168.2.20

Saved RSA Key – CVSS Score: 4.7. Remediation of changing the ssh RSA key for all users on the machine.

192.168.2.224

Unsafe input sanitization – CVSS Score: 7.3. Remediation of updating the php to disallow additional chained commands by stripping or sanitizing input.

192.168.2.202

MS17\_010 – CVSS Score: 10.0. Remediation of updating service packs and properly securing the SMB shares on the computer.

192.168.2.147

Stored Plain Text Passwords – CVSS Score: 4.5. Remediation of properly encrypting passwords saved in files or removing them all together.

192.168.2.100

Stored Plain Text Passwords – CVSS Score: 4.5. Remediation of properly encrypting all passwords or removing them from files on the system.

# Summary

The network test performed against XYZCorp HQ is detailed in the above pages. All findings are presented as is at the time of writing of this report. We are not held responsible for future release of new vulnerabilities in the systems or for any missed exploit techniques. In general, this report details our findings given the time allocated and methods known at the time of writing.

Overall, the company employs good security practices with firewall configurations that prevent certain attacks. Without finding credentials saved on hosts, lateral movement of the network would have been significantly more difficult to achieve. Of the vulnerable hosts, a few small updates would prevent the attack methods used and further secure the network. If the company chooses to follow our recommendations, the security of the company’s network would be greatly improved.