Powered by

NXT WAVE | iB HUBS

CCBP Foundations: Cybersecurity

Project Report

K Rushikesh Reddy

9th June 2021

Disclaimer

These investigations are performed as a practical hands-on of the concepts learned during the CCBP Foundations program and have no reference to any real-world illegal or unethical activities. The Company or the trainers will not be liable for any kind of misuse of any content or knowledge gained in the training by any of the participants.

Executive Summary

As a part of CCBP Foundations, we have performed Penetration Testing on **metasploitable2** and identified the vulnerable apps in it. We have exploited one of the vulnerable apps in the system and assessed the level of risk.

During the assessment, we have identified **1** HIGH-risk issues, **1** MEDIUM risk issues, and 0 LOW-risk issues.

In addition, we have also performed Open Source Intelligence Gathering on a predefined target and identified publicly available information.

Problem Statement 1 | Exploiting Samba

Phase 1: Intelligence Gathering

Technique Used:

Port Scanning

A technique to know the Open Ports / Services running on the system

Network mapping

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses

Tools and Commands Used:

nmap (Network Mapper)

Nmap tool allows a user to quickly and thoroughly learn about the systems on a network. It has the ability to quickly locate ports & services associated with that host (system/machine).

Syntax: `nmap [Flags] <IP Address>`

Command used

```
nmap -sV <target IP>
```

This command helps to know the open ports as well as service versions running on those ports

Output:

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.0.2.5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-08 10:21 EDT
Nmap scan report for 10.0.2.5
Host is up (0.0072s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux
; CPE: cpe:/o:linux:linux_kernel
```

Observations:

- Service: **netbios-ssn**
- Version: **Samba smbd 3.X - 4.X**
- Port: **139,445/tcp**

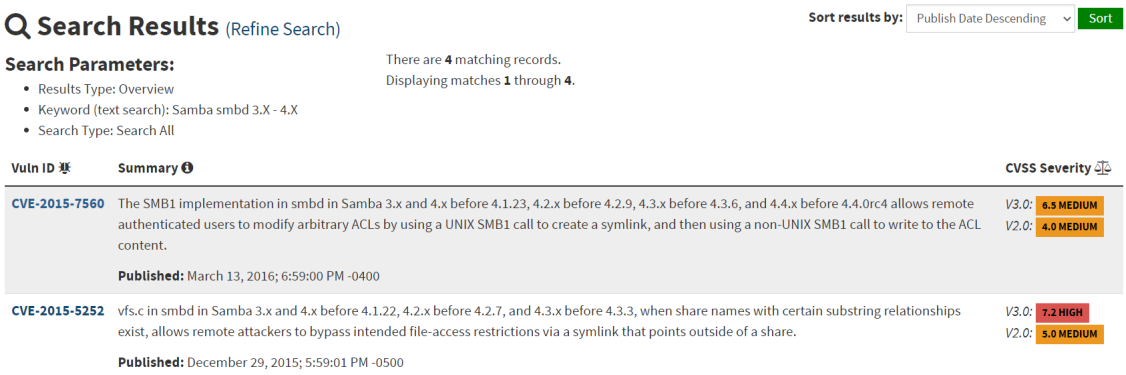
Phase 2: Vulnerability Assessment

Vulnerability assessment is done by searching for known vulnerabilities in the [NIST National Vulnerability Database]

Service:

Samba smbd 3.X - 4.X

Keep a screenshot highlighting the CVE



Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

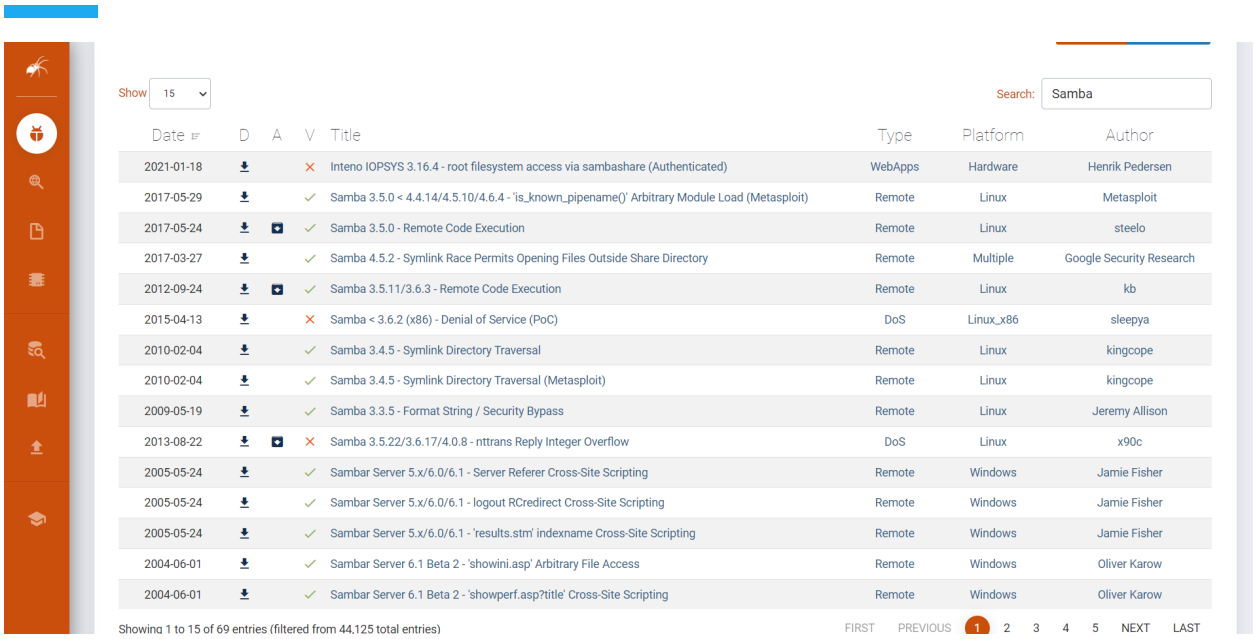
- Results Type: Overview
- Keyword (text search): Samba smbd 3.X - 4.X
- Search Type: Search All

There are **4** matching records.
Displaying matches **1** through **4**.

Vuln ID	Summary	CVSS Severity
CVE-2015-7560	The SMB1 implementation in smbd in Samba 3.x and 4.x before 4.1.23, 4.2.x before 4.2.9, 4.3.x before 4.3.6, and 4.4.x before 4.4.0rc4 allows remote authenticated users to modify arbitrary ACLs by using a UNIX SMB1 call to create a symlink, and then using a non-UNIX SMB1 call to write to the ACL content. **Published:** March 13, 2016; 6:59:00 PM -0400	V3.0: 6.5 MEDIUM V2.0: 4.0 MEDIUM
CVE-2015-5252	vfs.c in smbd in Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, when share names with certain substring relationships exist, allows remote attackers to bypass intended file-access restrictions via a symlink that points outside of a share. **Published:** December 29, 2015; 5:59:01 PM -0500	V3.0: 7.2 HIGH V2.0: 5.0 MEDIUM

Observations:

CVE ID	CVE Description	CVSS Severity	Impact Score
CVE-2015-7560	The SMB1 implementation in smbd in Samba 3.x and 4.x before 4.1.23, 4.2.x before 4.2.9, 4.3.x before 4.3.6, and 4.4.x before 4.4.0rc4 allows remote authenticated users to modify arbitrary ACLs by using a UNIX SMB1 call to create a symlink, and then using a non-UNIX SMB1 call to write to the ACL content. **Published: March 13, 2016; 6:59:00 PM -0400**	Medium	6.5
CVE-2015-5252	vfs.c in smbd in Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, when share names with certain substring relationships exist, allows remote attackers to bypass intended file-access restrictions via a symlink that points outside of a share.	High	7.2



Show 15 Search: Samba

Date	D	A	V	Title	Type	Platform	Author
2021-01-18			✗	Inteno IOPSYS 3.16.4 - root filesystem access via sambashare (Authenticated)	WebApps	Hardware	Henrik Pedersen
2017-05-29			✓	Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary Module Load (Metasploit)	Remote	Linux	Metasploit
2017-05-24			✓	Samba 3.5.0 - Remote Code Execution	Remote	Linux	steelo
2017-03-27			✓	Samba 4.5.2 - Symlink Race Permits Opening Files Outside Share Directory	Remote	Multiple	Google Security Research
2012-09-24			✓	Samba 3.5.11/3.6.3 - Remote Code Execution	Remote	Linux	kb
2015-04-13			✗	Samba < 3.6.2 (x86) - Denial of Service (PoC)	DoS	Linux_x86	sleepya
2010-02-04			✓	Samba 3.4.5 - Symlink Directory Traversal	Remote	Linux	kingcope
2010-02-04			✓	Samba 3.4.5 - Symlink Directory Traversal (Metasploit)	Remote	Linux	kingcope
2009-05-19			✓	Samba 3.3.5 - Format String / Security Bypass	Remote	Linux	Jeremy Allison
2013-08-22			✗	Samba 3.5.22/3.6.17/4.0.8 - nttrans Reply Integer Overflow	DoS	Linux	x90c
2005-05-24			✓	Sambar Server 5.x/6.0/6.1 - Server Referer Cross-Site Scripting	Remote	Windows	Jamie Fisher
2005-05-24			✓	Sambar Server 5.x/6.0/6.1 - logout RCredirect Cross-Site Scripting	Remote	Windows	Jamie Fisher
2005-05-24			✓	Sambar Server 5.x/6.0/6.1 - 'results.stm' indexname Cross-Site Scripting	Remote	Windows	Jamie Fisher
2004-06-01			✓	Sambar Server 6.1 Beta 2 - 'showini.asp' Arbitrary File Access	Remote	Windows	Oliver Karow
2004-06-01			✓	Sambar Server 6.1 Beta 2 - 'showperf.asp?title' Cross-Site Scripting	Remote	Windows	Oliver Karow

Showing 1 to 15 of 69 entries (filtered from 44,125 total entries) FIRST PREVIOUS 1 2 3 4 5 NEXT LAST

Phase 3: Exploitation

In this phase, already existing exploits for the vulnerable versions of services are explored using Metasploit.

Name of the Exploit	Tool
usermap_script	**msfconsole**

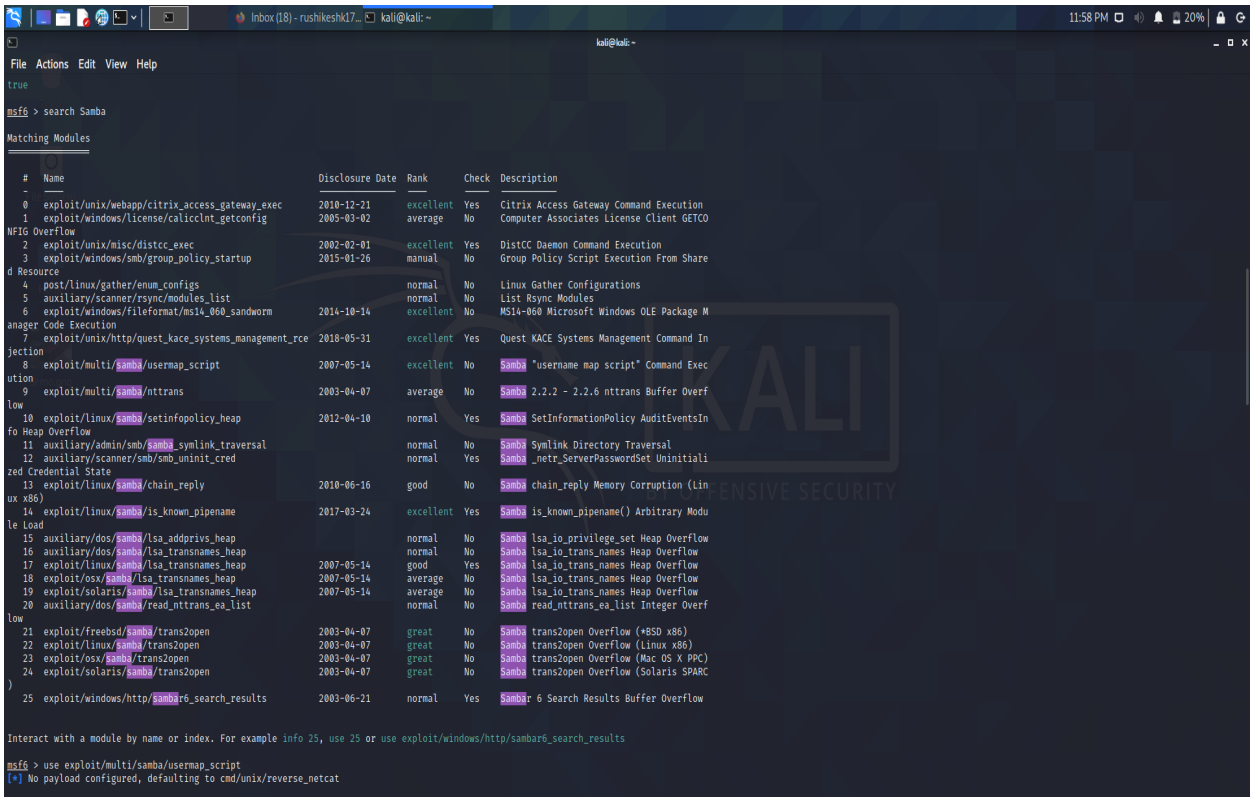
Service: Samba smbd

CVE 1:

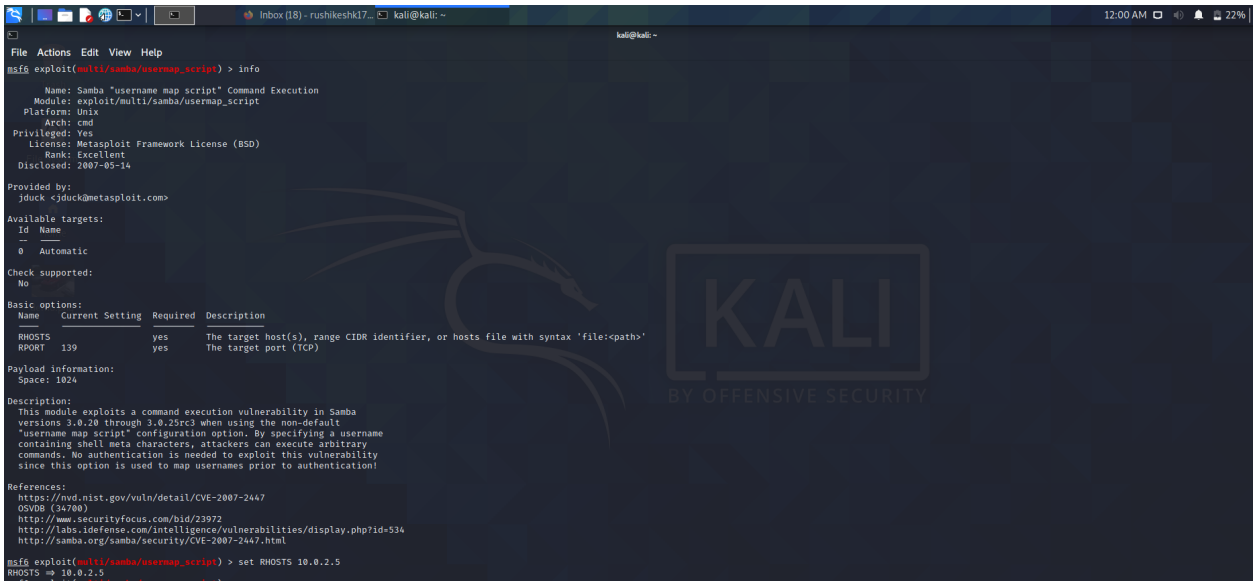
Tool used for exploitation: Metasploit

Steps Involved

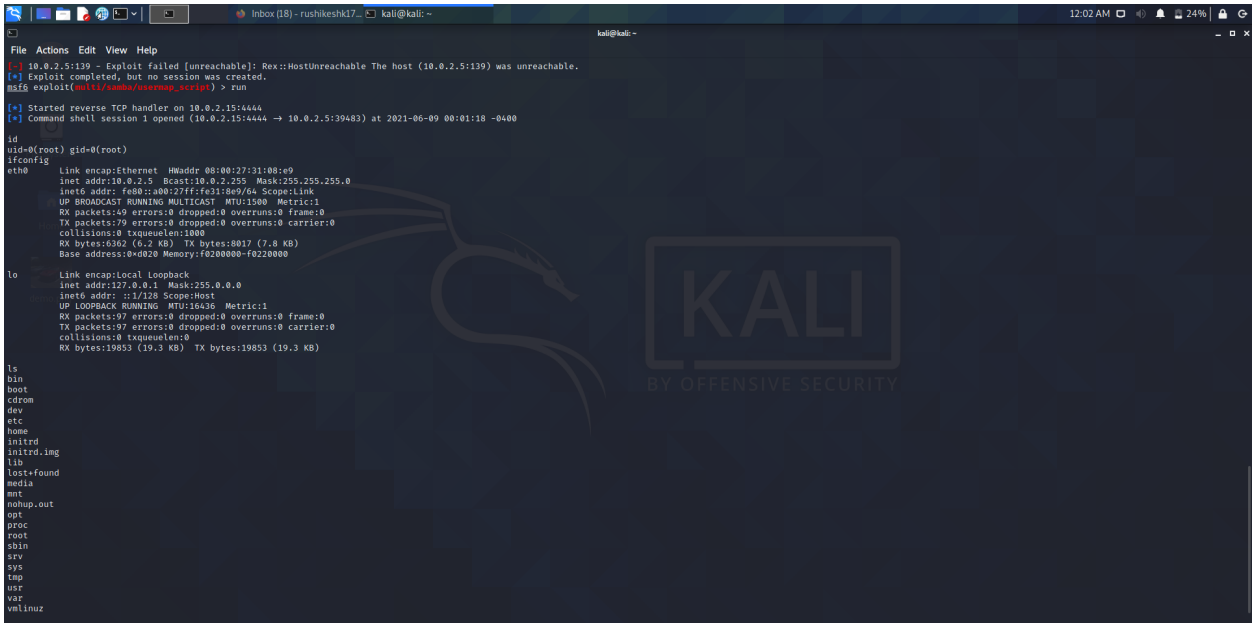
- Step 1: Search for the exploit **Samba** related to the vulnerability



- Step 2: use exploit/multi/samba/usermap_script
- Step 3: info
- Step 4: set RHOSTS <ip address of target machine> ## set RHOSTS 10.0.2.5



- Step5:run



Observations

- Got access to metasploit completely using samba

Summary

Phase	Technique	Tools	Commands (if any)
Reconnaissance	Port Scanning	nmap	
Vulnerability Assessment	Searching for CVEs	NVD Website	
Exploitation	Search for Exploits	Exploit-db	
Gaining Access	usermap_script	msfconsole	Search exploit,use,set,run

Problem Statement 2 | Brute Forcing SSH

Phase 1: Intelligence Gathering

Technique Used:

Port Scanning

A technique to know the Open Ports / Services running on the system

Network mapping

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses

Tools and Commands Used:

nmap (Network Mapper)

Nmap tool allows a user to quickly and thoroughly learn about the systems on a network. It has the ability to quickly locate ports & services associated with that host (system/machine).

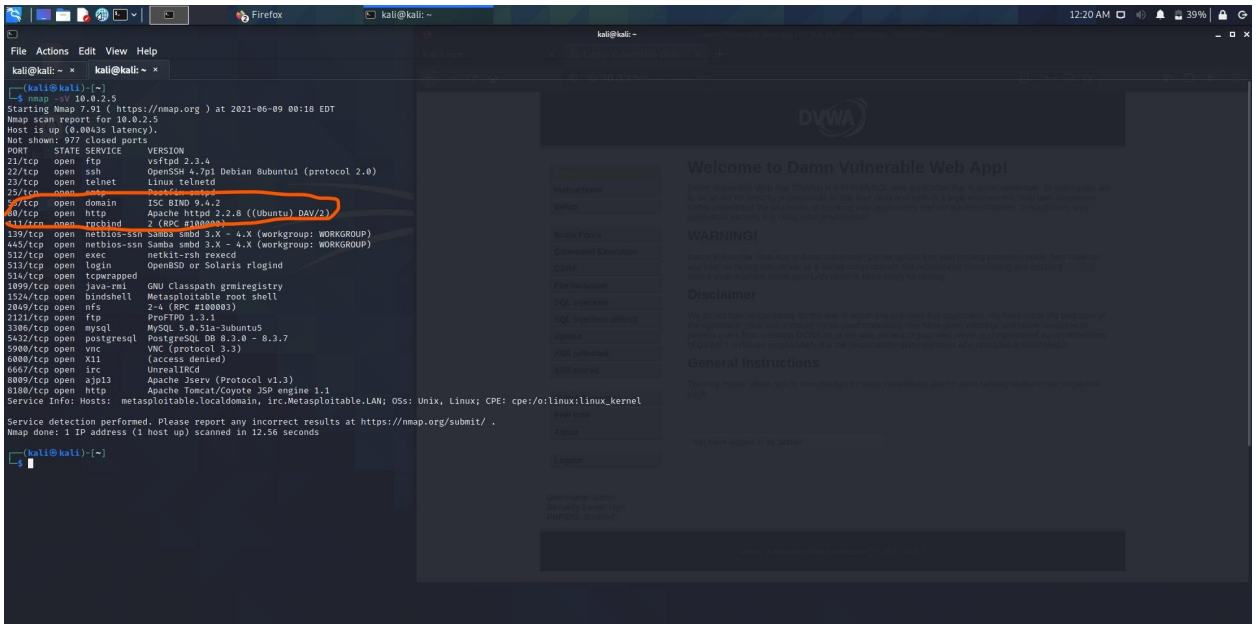
Syntax: `nmap [Flags] <IP Address>`

Command used

```
nmap -sV <target IP>
```

This command helps to know the open ports as well as service versions running on those ports

Output:



Observations:

- Service: **http**
- Version: **Apache HTTPd 2.2.8**
- Port:**80**

Phase 2: Vulnerability Assessment

DVWA is inbuilt with multiple vulnerabilities. But, for the scope of this lab, we will:

- Choose the Command Execution Vulnerability present in the DVWA.
- Set the DVWA Security Level to LOW. This implies that
    - The underlying code does not check if **$target** matches an **IP Address**.
    - There is **no filtering on special characters**.

- Simply put, Low-Security means easily exploitable.

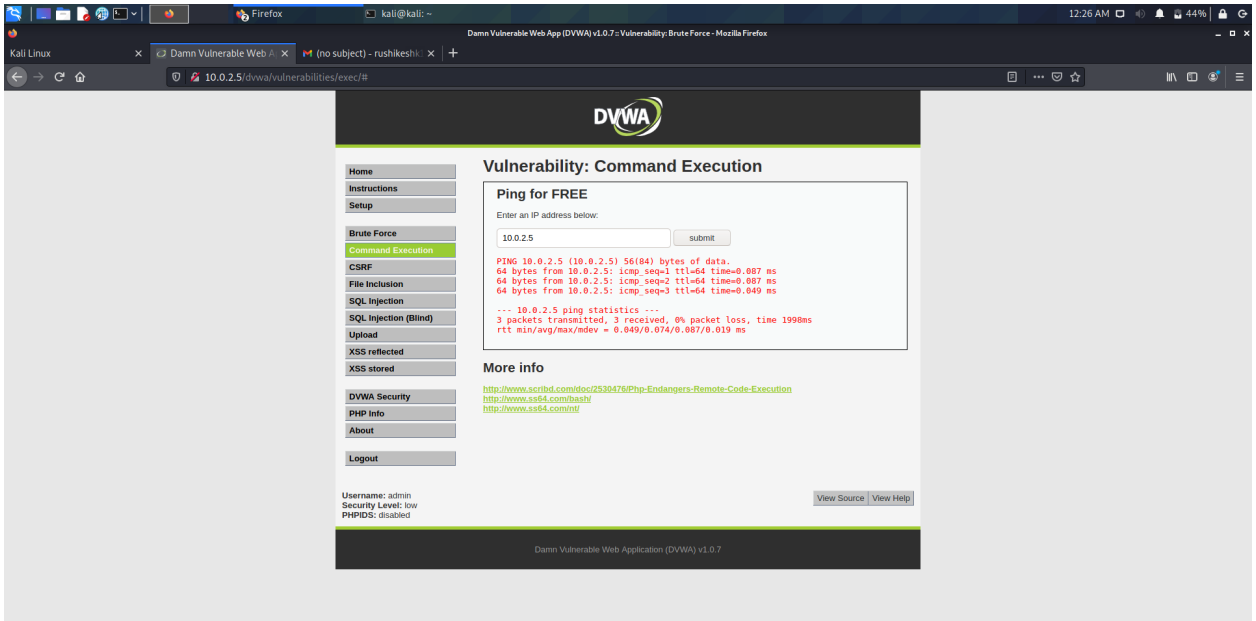
Changing DVWA Security Level to Low

- To change the DVWA Security level, navigate to the **DVWA Security tab** and change the security level to **Low**

Command Injection Overview:

Command injection (also known as shell injection) is a web security vulnerability that allows an attacker to execute arbitrary operating system (OS) commands on the server that is running an application

- Navigate to the Command Execution tab. You are provided with a free ping utility that allows us to ping any IP address.
- Enter the <Target IP Address>(10.0.2.5)



Phase 3: Exploitation

Hydra

Parallelized login cracker which supports numerous protocols (ftp, http, etc.) to attack

1.Very fast and Flexible

2.Helps in gaining unauthorized access to a system remotely

Syntax:

hydra [Options] <IP Address> <Protocol>

Tool	Command
hydra	**hydra -h or hydra -help,hydra -L <user file> -P <password file> <target IP> ftp -V**

In this phase, the service is exploited using the **hydra** to perform a brute force attack on

1.klog

2.sys

Observations

Username 1: **klog**

Wordlist used for exploitation:

Steps Involved

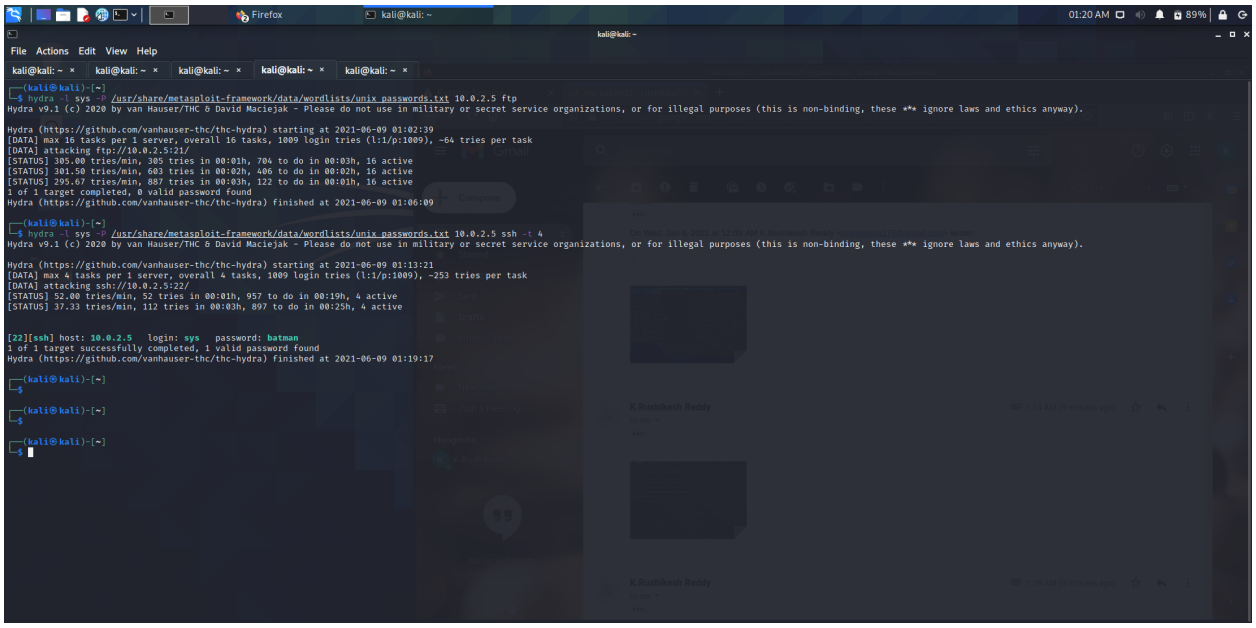
- Step1:hydra-lklog-P/usr/share/metasploit-framework/data/wordlists/adobe_top100_pass.txt <target IP> ftp

Username 2: **sys**

Wordlist used for exploitation:

Steps Involved

- Step1:hydra-lsys-P/usr/share/metasploit-framework/data/wordlists/unix_passwords.txt <target IP> ftp



Summary

Phase	Technique	Tools	Commands (if any)
Reconnaissance	Port Scanning	Nmap	
Vulnerability Assessment	Command Injection	Manual Assessment	
Exploitation	Brute Forcing	Hydra	hydra -h or hydra -help

Problem Statement 3 | OSINT

1. What is the Copyright Information identified in the image?
2. What are the Geolocation Coordinates?
3. What's the Location name?
4. Which device was the photo taken from (For example, Apple iPhone 11)
5. What's the target's real name?
6. The target seems to be the co-creator of a popular OSINT tool; what's the tool called?
7. What are the usernames identified in relation to the target?
8. What is the target's email address?
9. Does the target have a personal website? If yes, what is it?
10. Find out the target's Twitter handle and the year & month they joined Twitter.

1. Petruknisme,petruknisme.com

2.GPS Latitude : 27 deg 10' 26.01"
GPS Longitude : 78 deg 2' 31.44"

3.Agra

4.Model : iphone X

Make : Apple

5.Aan

6.Belati

7.@petruknisme(Twitter),

aancw (Aan)(Github)

petruknisme(hackthebox)

Contact @petruknisme - Telegram

Aan (petruknisme)(Hackerone)

8.dalang@petruknisme.com

9.yes,https://petruknisme.com/

10.https://twitter.com/petruknisme?lang=en

Joined september 2011

```
┌──(kali㉿kali)-[~/Desktop]
└─$ exiftool taj.png
ExifTool Version Number         : 12.16
File Name                       : taj.png
Directory                       : .
File Size                       : 6.1 MiB
File Modification Date/Time     : 2021:06:09 01:23:36-04:00
File Access Date/Time           : 2021:06:09 01:23:41-04:00
File Inode Change Date/Time     : 2021:06:09 01:23:36-04:00
File Permissions                : rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 4803
Image Height                    : 3181
Bit Depth                       : 8
Color Type                      : Palette
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Gamma                           : 2.2
SRGB Rendering                  : Perceptual
Profile CMM Type                : Little CMS
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 2012:01:25 03:41:57
Profile File Signature          : acsp
Primary Platform                : Apple Computer Inc.
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             :
Device Model                    :
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Little CMS
Profile ID                      : 0
Profile Description             : c2
Profile Copyright               : IX
Media White Point               : 0.9642 1 0.82491
Media Black Point               : 0.01205 0.0125 0.01031
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
Red Tone Reproduction Curve     : (Binary data 64 bytes, use -b option to extract)
Green Tone Reproduction Curve   : (Binary data 64 bytes, use -b option to extract)
Blue Tone Reproduction Curve    : (Binary data 64 bytes, use -b option to extract)
Pixels Per Unit X               : 2834
Pixels Per Unit Y               : 2834
Pixel Units                     : meters
Palette                         : (Binary data 414 bytes, use -b option to extract)
Model                           : iphone X
Make                            : Apple
City                            : agra
Application Record Version      : 4
Exif Byte Order                 : Big-endian (Motorola, MM)
X Resolution                    : 72
Y Resolution                    : 72
Resolution Unit                 : inches
Y Cb Cr Positioning             : Centered
Copyright                       : Petruknisme,petruknisme.com
GPS Version ID                  : 2.3.0.0
GPS Latitude                    : 27 deg 10' 26.01"
GPS Longitude                   : 78 deg 2' 31.44"
Image Size                      : 4803×3181
Megapixels                      : 15.3
GPS Position                    : 27 deg 10' 26.01", 78 deg 2' 31.44"

┌──(kali㉿kali)-[~/Desktop]
```

Conclusion

His name is Aan .He is a hacker