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	SecurityOne
Contact Name	Penetration Tester
Contact Title	Reuben Baulch

Document History

Version	Date	Author(s)	Comments
001	3/10/2022	Reuben Baulch	-

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 IP addresses are listed below.

Web application

192.168.14.35

Linux servers

192.168.13.1
192.168.13.10
192.168.13.11
192.168.13.12
192.168.13.13

Windows servers

192.168.14.35
192.168.13.10
172.22.117.20

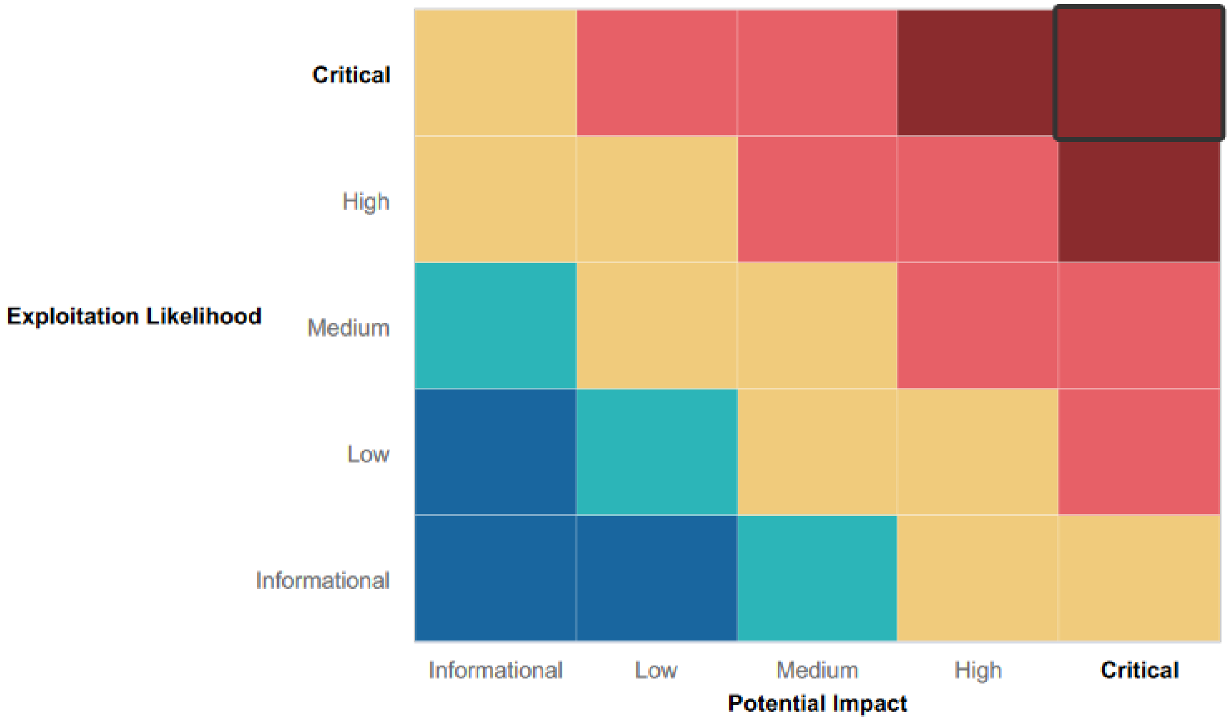
Executive Summary of Findings

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.

- Web application was filtering for malicious code injection (input sanitisation)
- Web app only allows jpg extensions in file name for picture uploads
- Web app filters for command injections such as && and ;

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.

- Web application is vulnerable to local file inclusion
- Web application is vulnerable to local file XSS
- Web application login page is vulnerable to SQL injection
- Admin credentials found in source code
- Sensitive data being exposed in robots.txt
- Obtained user credentials through command injection
- PHP injection allowed for misuse of admin tools on the web application
- Able to abuse session management using Burpsuite
- 192.168.13.10 was successfully exploited using Apache Tomcat exploit
- 192.168.13.11 was successfully exploited using a shellshock exploit
- 192.168.13.12 was successfully exploited using a Apache struts exploit
- 192.168.13.13 was successfully exploited using a Drupal exploit
- Able to SSH into 192.168.13.13 and escalate to root privileges
- Able to transfer files from the 172.22.117.20 host using FTP
- Exploited 172.22.117.20 with the pop3 exploit
- Able to move laterally using the PsExec exploit

Executive Summary

SecurityOne was contracted by Rekall to conduct a penetration test in order to determine its exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against Rekall with the goals of:

1. Identifying if a remote attacker could penetrate ReKall's defenses
2. Determining the impact of a security breach on the confidentiality of the company's private data and appropriate remediations to the vulnerabilities identified.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the techniques and recommendations outlined in the Mitre attack framework with all tests and actions being conducted under controlled conditions.

Upon conducting an all round penetration test on Rekall, SecurityOne found numerous vulnerabilities that could expose the corporation to attack. Overall, the security position of Rekall was in a critical condition, with a wide range of issues being identified in Rekalls web application, linux and windows servers.

The critical state of Rekall's security can easily be turned around with some effective planning and action in a timely manner which will be discussed as remediation to the vulnerabilities listed under vulnerability findings below. While Rekall's shortcomings have resulted in a poor security position, there were some positives that should continue to be implemented into the future. These were the strengths that SafeSecurity identified above.

Summary Vulnerability Overview

Vulnerability	Severity
Web application is vulnerable to local file inclusion	**Critical**
Web application is vulnerable to local file XSS	**Critical**
Web application login page is vulnerable to SQL injection	**Critical**
Admin credentials found in source code	**High**
Sensitive data being exposed in robots.txt	**Medium**
Obtained user credentials through command injection	**Critical**
PHP injection allowed for misuse of admin tools on the web application	**High**
Able to abuse session management using Burpsuite	**Critical**
192.168.13.10 was successfully exploited using Apache Tomcat exploit	**Critical**
192.168.13.11 was successfully exploited using a shellshock exploit	**Critical**
192.168.13.12 was successfully exploited using a Apache struts exploit	**Critical**

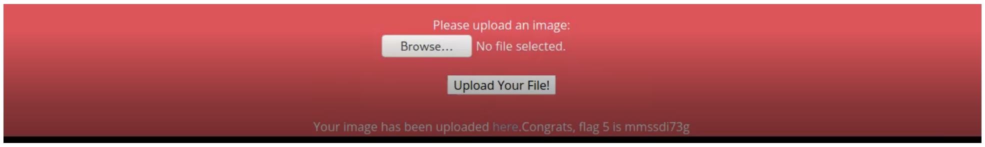
192.168.13.13 was successfully exploited using a Drupal exploit	**Critical**
Able to SSH into 192.168.13.13 and escalate to root privileges	**Critical**
Able to transfer files from the 172.22.117.20 host using FTP	**High**
Exploited 172.22.117.20 with the pop3 exploit	**Critical**
Able to move laterally using the PsExec exploit	**Critical**

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

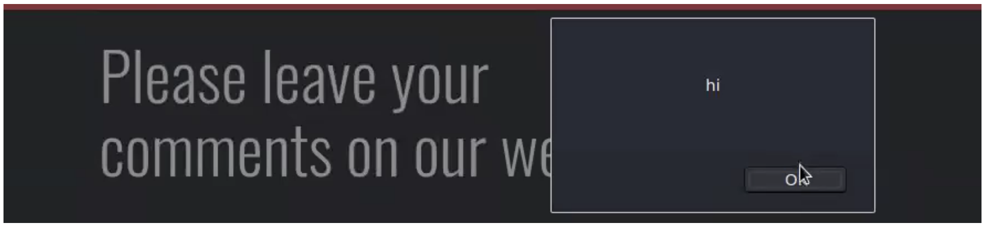
Scan Type	Total
Hosts	5
Ports	21, 25, 79, 80, 106, 110, 135, 139, 443, 445, 53, 88, 389, 445, 464, 593, 636, 3268, 3269

Exploitation Risk	Total
Critical	12
High	3
Medium	1
Low	0

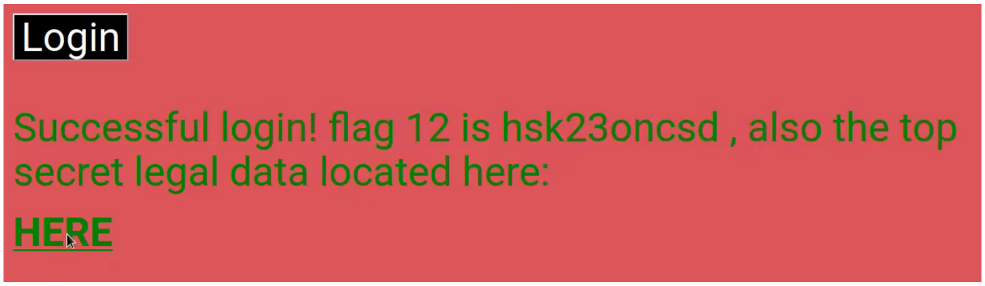
Vulnerability Findings

Vulnerability 1	Findings
Title	Web application is vulnerable to local file inclusion
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	The Rekall web application can execute malicious scripts included in files that are uploaded.
Images	 Please upload an image: No file selected. Your image has been uploaded here.Congrats, flag 5 is mmssdi73g

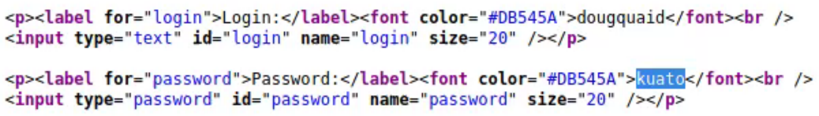
Affected Hosts	192.168.14.35
Remediation	● Don't include files on a web server that can be compromised. Use a database instead ● save your file paths in a secure database and give an ID for every single one, this way users only get to see their ID without viewing or altering the path ● use verified and secured whitelist files and ignore everything else

Vulnerability 2	**Findings**
Title	Web application is vulnerable to local file XSS
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Attackers can inject client side scripts in to the web application to reveal sensitive data
Images	 Please leave your comments on our we hi
Affected Hosts	192.168.14.35
Remediation	● Whenever accepting any data, ensure the format of the data is what you expect. In effect, this whitelists data to ensure that the application does not accept any code. ● make sure any dynamic content coming from the data store cannot be used to inject JavaScript on a page

Vulnerability 3	**Findings**
Title	Web application login page is vulnerable to SQL injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Malicious SQL statements can be inserted into an entry field for execution and reveal sensitive data

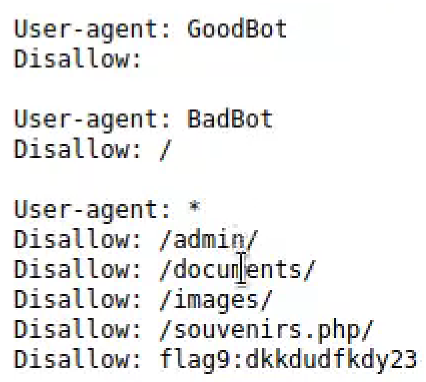
Images	 Login Successful login! flag 12 is hsk23oncsd , also the top secret legal data located here: HERE
Affected Hosts	192.168.14.35
Remediation	● Use Allow-list Input Validation such as a drop down to prevent sql queries being injected into the web application ● Check that supplied fields like email addresses match a regular expression ● Ensure that numeric or alphanumeric fields do not contain symbol characters.

Vulnerability 4	**Findings**
Title	Admin credentials found in source code
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**High**
Description	Upon viewing page source, there are user credential located in the source code that allow the user to login as an administrator

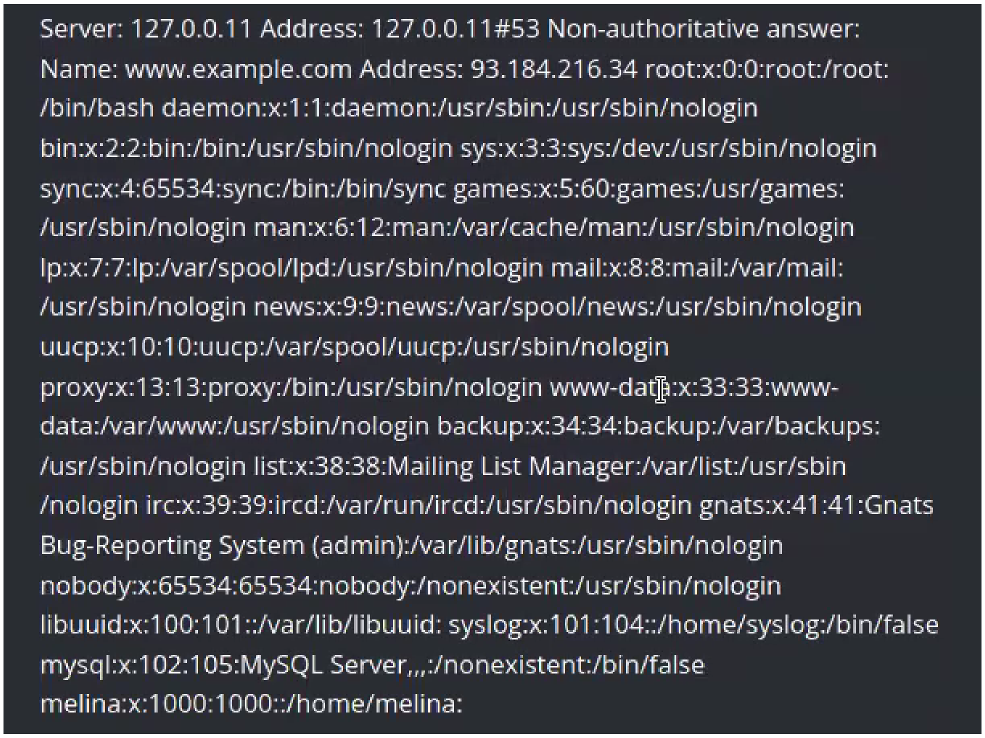
Images	
	`<p><label for="login">Login:</label><font color="#DB545A">dougquaid</font><br />`
	`<input type="text" id="login" name="login" size="20" /></p>`
	`<p><label for="password">Password:</label><font color="#DB545A">kuato</font><br />`
	`<input type="password" id="password" name="password" size="20" /></p>`

Affected Hosts	192.168.14.35
Remediation	● User passwords should never be hard coded and usually also not be stored on the server or a database. ● Should use so-called salt and hashing and only store the hash in a database ● Make sure access to this DB is as limited as possible ● Set up two-factor authentication instead of basic authentication to prevent dictionary attacks from being successful. ● Reset the users password.

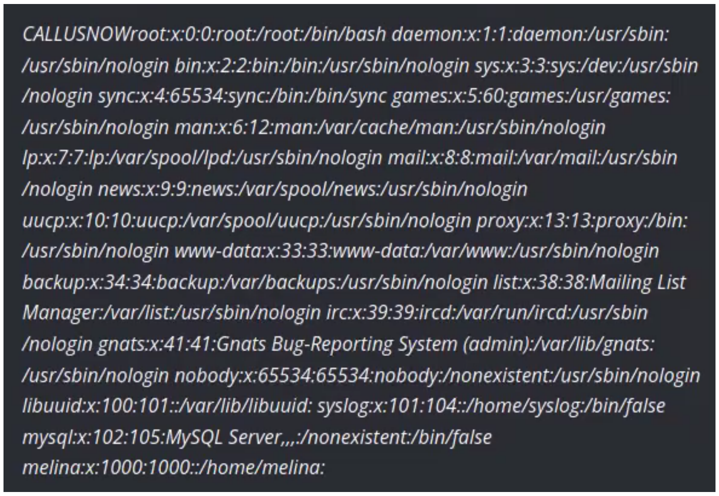
Vulnerability 5	**Findings**
Title	Sensitive data being exposed in robots.txt
Type (Web app / Linux OS / WIndows OS)	Web app

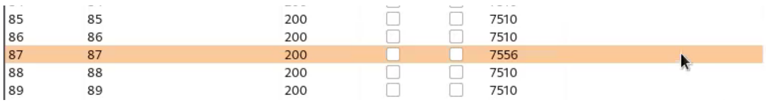
Risk Rating	**Medium**
Description	Google dorking for Rekall’s website highlights robots.txt which contains a directory that displays sensitive user information to the public.While robots.txt is not inherently dangerous, attackers can use it to identify restricted or private areas of a website. This assists in mapping out the site's contents
Images	 User-agent: GoodBot Disallow: User-agent: BadBot Disallow: / User-agent: * Disallow: /admin/ Disallow: /documents/ Disallow: /images/ Disallow: /souvenirs.php/ Disallow: flag9:dkkdudfkdy23
Affected Hosts	192.168.14.35
Remediation	● Be aware of what is displayed and assume that attackers will play close attention to the locations identified in the file. ● Use no index instead of disallow for pages that need to be private and not publicly accessible

Vulnerability 6	**Findings**
Title	Obtained user credentials through command injection
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Can execute arbitrary operating system (OS) commands on the server that is running an application, and typically fully compromise the application and all its data.

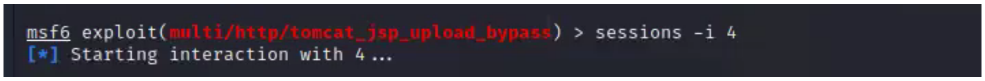
Images	 Server: 127.0.0.11 Address: 127.0.0.11#53 Non-authoritative answer: Name: www.example.com Address: 93.184.216.34 root:x:0:0:root:/root: /bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync 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:
Affected Hosts	192.168.14.35
Remediation	● Avoid system calls and user input—to prevent threat actors from inserting characters into the OS command. ● Set up input validation—to prevent attacks like XSS and SQL Injection. ● Create a white list—of possible inputs, to ensure the system accepts only pre-approved inputs.

Vulnerability 7	Findings
Title	PHP injection allowed for misuse of admin tools on the web application
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	High
Description	An attacker takes advantage of a script that contains system functions/calls to read or execute malicious code on a remote server. This is synonymous to having a backdoor shell and under certain circumstances can also enable privilege escalation

Images	 CALLUSNOWroot: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:
Affected Hosts	192.168.14.35
Remediation	● Avoid Using Weak Sanitization Methods.Whenever you accept user input, you must make sure it is valid, store and process it in such a way that it does not enable attacks against the application. ● avoid error output that could be used by an attacker to identify sensitive environment information related to your PHP application and web server.

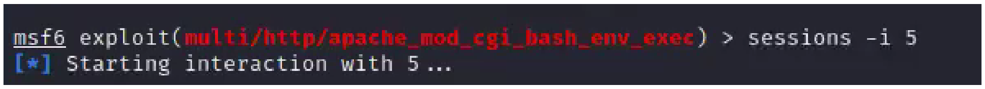
Vulnerability 7	Findings
Title	Able to abuse session management using Burpsuite
Type (Web app / Linux OS / WIndows OS)	Web app
Risk Rating	**Critical**
Description	Session Fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application.
Images	 85 85 200 □ □ 7510 86 86 200 □ □ 7510 87 87 200 □ □ 7556 88 88 200 □ □ 7510 89 89 200 □ □ 7510
Affected Hosts	192.168.14.35
Remediation	● The session ID must be unpredictable (random enough) to prevent guessing attacks, where an attacker is able to guess or predict the ID of a valid session through statistical analysis techniques ● Regenerate session key after authentication to prevent hackers from exploiting the session ID generated during login

Vulnerability 7	Findings
Title	192.168.13.10 was successfully exploited using Apache Tomcat exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	By exploiting a vulnerability in Apache Tomcat, a hacker can upload a backdoor and get a shell

Images	
	`msf6 exploit(multi/http/tomcat_jsp_upload_bypass) > sessions -i 4`
	`[*] Starting interaction with 4 ...`

Affected Hosts	192.168.13.10
Remediation	● Make sure Apache Tomcat is updated to the latest version.

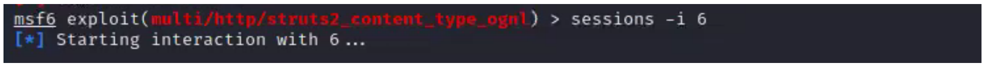
Vulnerability 7	Findings
Title	192.168.13.11 was successfully exploited using a shellshock exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	Shellshock is a computer bug that exploits the vulnerability in the UNIX command execution shell-bash to facilitate hackers to take control of the computer system remotely and execute arbitrary code

Images	
	`msf6 exploit(multi/http/apache_mod_cgi_bash_env_exec) > sessions -i 5`
	`[*] Starting interaction with 5 ...`

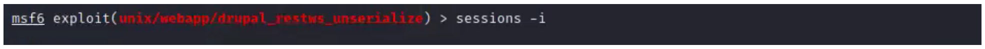
Affected Hosts	192.168.13.11
Remediation	● Make sure the bash shell is completely patched and up to date ● By sanitizing user input and removing un-needed characters, developers can disrupt an attack before it takes place.

Vulnerability 7	Findings
Title	192.168.13.12 was successfully exploited using a Apache struts exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**

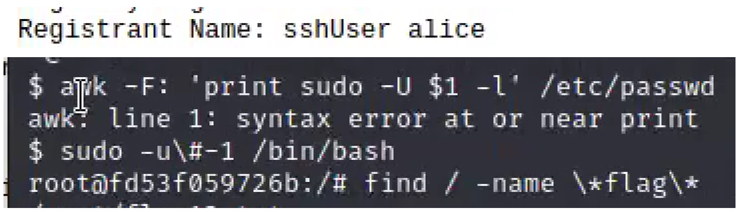
Description	Apache Struts is an open source framework used for building Java web applications. Successful exploitation of this vulnerability could allow for remote code execution.

Images	
	`msf6 exploit(multi/http/struts2_content_type_ognl) > sessions -i 6`
	`[*] Starting interaction with 6 ...`

Affected Hosts	192.168.13.12
Remediation	● Make sure Apache Struts is updated to the latest version.

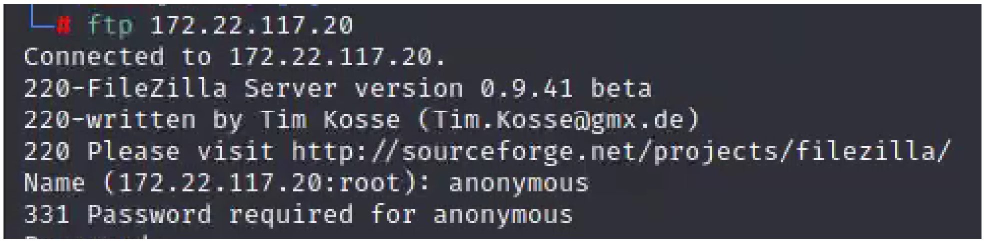
Vulnerability 7	**Findings**
Title	192.168.13.13 was successfully exploited using a Drupal exploit
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	A critical exploit that takes advantage of vulnerabilities in Drupal that allow for critical remote code execution
Images	 `msf6 exploit(unix/webapp/drupal_restws_unserialize) > sessions -i`
Affected Hosts	192.168.13.13
Remediation	● Make sure Drupal is updated to the latest version.

Vulnerability 7	**Findings**
Title	Able to SSH into 192.168.13.13 and escalate to root privileges
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	**Critical**
Description	SecurityOne was able to find the ssh user Alice using a WHOIS lookup. This allowed for the ssh into host 192.168.13.13 using the user Alice. In doing this, SecurityOne was able to escalate to root privileges.

Images	
	`Registrant Name: sshUser alice`
	`$ awk -F: 'print sudo -U $1 -l' /etc/passwd`
	`awk: line 1: syntax error at or near print`
	`$ sudo -u\#-1 /bin/bash`
	`root@fd53f059726b:/# find / -name \*flag\*`

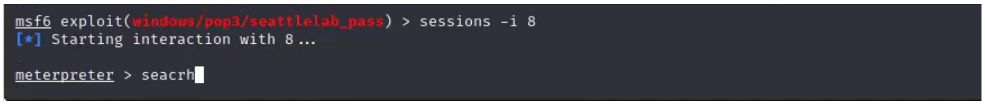
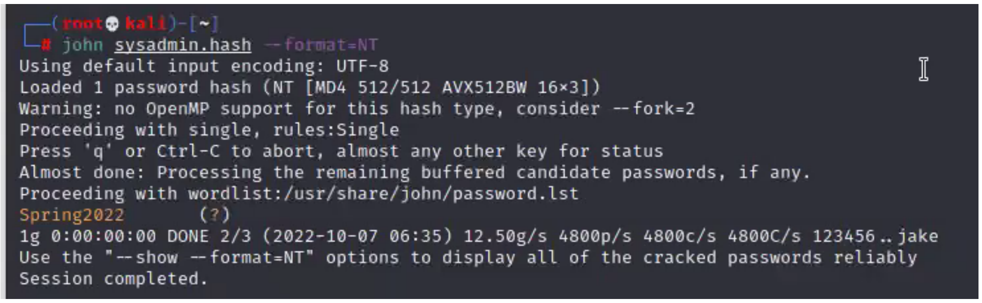
Affected Hosts	192.168.13.1
Remediation	- Remove user credentials that can be found on the internet - manage the privileged accounts and ensure that they are all secure, used according to the best practices, and not exposed. - Analyzing user behavior can discover if there are compromised identities. - Urge all employees to delete files with passwords stored on them and consider using a password manager instead - Create company policies around how employees are required to store their passwords - Establish account lockout for for a sudden spike in failed logins and force all employees to change their passwords with new strong ones - Implement strong password policies

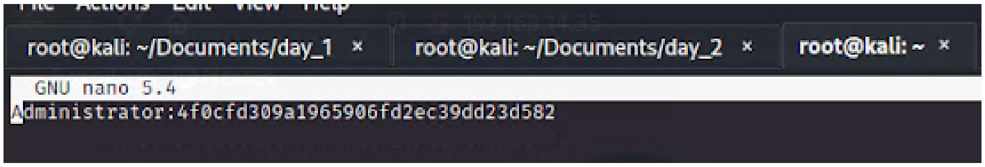
Vulnerability 7	**Findings**
Title	Able to transfer files from the 172.22.117.20 host using FTP
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Moving to attacking windows servers, SecurityOne was able to transfer files from the 172.22.117.20 host using ftp.

Images	
	`└─# ftp 172.22.117.20`
	`Connected to 172.22.117.20.`
	`220-FileZilla Server version 0.9.41 beta`
	`220-written by Tim Kosse (Tim.Kosse@gmx.de)`
	`220 Please visit http://sourceforge.net/projects/filezilla/`
	`Name (172.22.117.20:root): anonymous`
	`331 Password required for anonymous`

Affected Hosts	172.22.117.20
Remediation	- Update ftp to the latest version - Consider closing port 21 if ftp is not a necessity. Ftp is insecure and should no longer be used. SFTP is a more secure alternative

Vulnerability 7	**Findings**
Title	Exploited 172.22.117.20 with the pop3 exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical

Description	SecurityOne was also able to further exploit 172.22.117.20 with the pop3 exploit, which allowed for the discovery of plain text passwords for users such as sysadmin.
Images	 msf6 exploit(windows/pop3/seattlelab_pass) > sessions -i 8 [*] Starting interaction with 8 ... meterpreter > seacrh  ┌──(root💀kali)-[~] └─# john sysadmin.hash --format=NT Using default input encoding: UTF-8 Loaded 1 password hash (NT [MD4 512/512 AVX512BW 16×3]) 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 Almost done: Processing the remaining buffered candidate passwords, if any. Proceeding with wordlist:/usr/share/john/password.lst Spring2022 (?) 1g 0:00:00:00 DONE 2/3 (2022-10-07 06:35) 12.50g/s 4800p/s 4800c/s 4800C/s 123456..jake Use the "--show --format=NT" options to display all of the cracked passwords reliably Session completed.
Affected Hosts	172.22.117.20
Remediation	● Make sure pop3 is up to date and running the latest version ● Consider using IMAP which is more secure

Vulnerability 7	**Findings**
Title	Able to move laterally using the PsExec exploit
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	**Critical**
Description	SecurityOne was able to use a psexec exploit along with the user ADMBod to move laterally to the host 172.22.117.10. Here, the admin password could be cracked.
Images	 File Actions Edit View Help root@kali: ~/Documents/day_1 root@kali: ~/Documents/day_2 root@kali: ~ GNU nano 5.4 Administrator:4f0cfd309a1965906fd2ec39dd23d582
Affected Hosts	172.22.117.10
Remediation	● Make sure PsExec is fully patched and up to date ● Limit credential reuse by making sure that passwords in the network are not on the breach password list ● Manage local administrator passwords so that they are not the same across the network ● Limit credential reuse by making sure that passwords in the network are not on the breach password list ● Manage local administrator passwords so that they are not the same across the network