Cybersecurity

Penetration Test Report

Rekall Corporation

Penetration Test Report

Faux Red Team, LLC
Robert Harris

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	Faux Red Team, LLC
Contact Name	Robert Harris
Contact Title	Penetration Tester

Document History

Version	Date	Author(s)	Comments
001	07/24/2022	Robert Harris	

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.

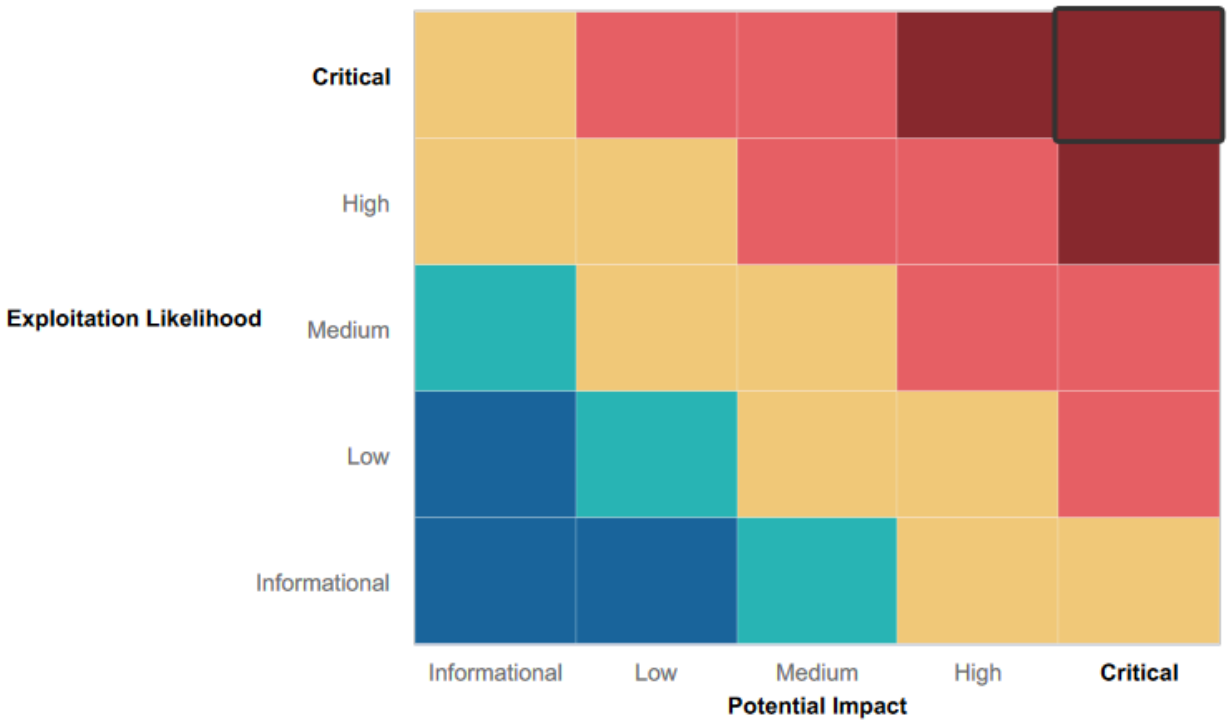
Executive Summary of Findings

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.

- Many exploits that have a high level of success do not pose a vulnerability because Rekall's infrastructure doesn't allow them.
- Common ports that pose critical weaknesses are not open to allow exploitation.
- The web application has basic restrictions on many of its pages that won't allow common exploits.
- Linux system vulnerabilities are not openly obvious and would require more determined reconnaissance to uncover.
- Majority of the Windows system is secure and prevents common vulnerabilities.

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.

- Many weaknesses and vulnerabilities discovered in Rekall's systems stem from poor username and password requirements/storage procedures.
- Upon further testing of the web application, discovered vulnerabilities that can expose critical information in Rekall's infrastructure.
- Some portions of the web application allow access to subdomains that shouldn't be accessible.
- Too many forms of input/types of characters are allowed in the web applications pages.
- Web application HTML storing critical login credentials.
- Rekall's Linux systems are vulnerable to a variety of known exploits that are more than two years old. These vulnerabilities then allow for more exploits to be discovered and used to expose even more critical information.
- Linux systems are not synchronized/streamlined to use the same applications as each other.
- Employee's compromising login credentials by using third party applications.
- Windows system allowing lower users too much connectivity capabilities and system application accessibility.

Executive Summary

We began our Penetration Test by assessing the security infrastructure of Rekall's web application. We discovered basic vulnerabilities that are common on many interactive websites such as Cross Site Scripting and Command Injection. Using Local File Inclusion we were able to upload a file containing a custom script, this could manipulate the web application in a variety of ways. We tested SQL Injection and Brute Force Attacks which allowed us to login using weak login credentials. Through Sensitive Data Exposure we were able to identify hidden pages that we accessed with PHP Injection by manipulation of the URL. With Directory Traversal we moved to pages that were not intended to be accessed by users. Using some of the previous login credentials we acquired, we altered the session ID to allow us Admin access. After we were finished assessing the web application it was clear many of the vulnerabilities would stem from poor login credential requirements.

We then moved to Rekall's Linux OS. After doing some reconnaissance on totalrecall.xyz, we found IP addresses and open ports. Using Nessus and aggressive nmap scans we found some critical vulnerabilities in software the OS was running. Using a vulnerability in Apache Tomcat we used Remote Code Execution to create a shell and gain root access. Which would lead to a variety of other critical vulnerabilities. We used a Shellshock exploit through an outdated version of Bash, giving us access to /etc/sudoers and /etc/passwd. Two vital locations on the Linux OS. A Nessus scan of 192.168.13.12 showed us that the OS is vulnerable to a Struts exploit that allowed us to pull a file from the system for later viewing. We used a Drupal exploit to create a shell and gain valuable information as well as logging in through SSH with weak user credentials, then using a sudo bypass exploit to escalate our privileges.

During our test of the Windows OS we gained initial access by acquiring a password hash from a third-party website during our reconnaissance phase, this gave us access through the front door. During an aggressive nmap scan we discovered the FTP port was open and allowed Anonymous users to login through it. From the port scan we found an exploit with Seattle Lab Mail that gave us access through the 110 pop3 port, allowing us to launch a shell. We acquired SYSTEM user access, then launched a tool called kiwi. This tool allowed us to dump the contents of a cache containing user credentials. Which we then cracked with a password cracking tool named "John the Ripper". During the cache dump we found credentials for an Administrator user, we then found what those credentials have access to. Using a PSExec exploit to create a shell, list users and acquire an Administrator password hash.

While reading this summary one could see this as an individual gaining access through a critical vulnerability and exposing a company's infrastructure, uncovering secrets and doing damage along the way. But in reality these are all separate medium to critical vulnerabilities. A malicious actor that wants to do harm to a company's systems doesn't need to know all of these vulnerabilities listed. In order to gain access, they only need to know one. In the following summaries details are given for the individual vulnerabilities and exploits. But the first step in protecting your company's infrastructure is the prevention of initial access. This is gained by having strong requirements for login credentials (username and password), healthy standards and expectations for credential confidentiality and implementing some form of two factor authentication.

Summary Vulnerability Overview

Vulnerability	Severity
Sensitive Data Exposure	Critical
SQL Injection	Critical
Brute Force Attack	Critical
Session Management	Critical
Apache Tomcat RCE (CVE-2017-12617)	Critical
Shellshock	Critical
Struts (CVE-2017-5638)	Critical
Sudo Blacklist Privilege Escalation (CVE-2019-14287)	Critical
SLMail exploit through 110/tcp pop3 Port	Critical
Kiwi tool and LSA Credential Dump	Critical
PSExec and SYSTEM Shell	Critical
Weak Login Credential Requirements/Third Party Vulnerabilities	Critical
Cross Site Scripting (XSS) stored	High
Local File Inclusion	High
Command Injection	High
PHP Injection	High
Directory Traversal	High
Drupal (CVE-2019-6340)	High
FTP Exfiltration Techniques	High
Cross Site Scripting (XSS) reflected	Medium
Open Source Exposed Data	Low

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

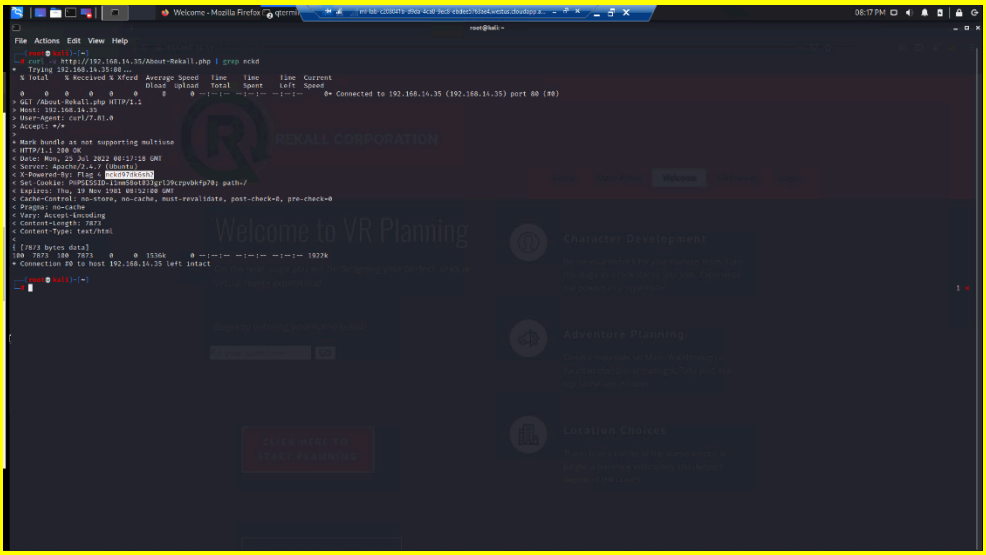
Scan Type	Total
Hosts	192.168.14.35 (Web App) 34.102.136.180 (.xyz) 192.168.13.0/24 (Linux) 172.22.117.0/24 (Windows)

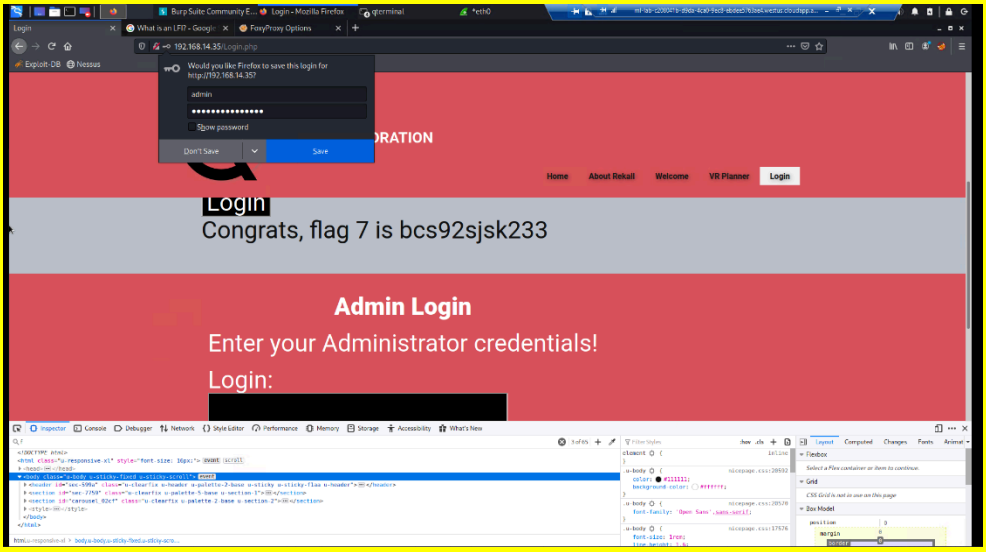
Ports	22/tcp sh 53/tcp domain 80/tcp http 88/tcp Kerberos-sec 135/tcp msrpc 139/tcp netbios-ssn 389/tcp ldap 445/tcp microsoft-ds? 464/tcp kpasswd5? 593/tcp ncacn_http 636/tcp tcpwrapped 3268/tcp ldap 3269/tcp tcpwrapped 3306/tcp mysql 5901/tcp vnc 6001/tcp X11 8009/tcp ajp13 8080/tcp http

Exploitation Risk	Total
Critical	12
High	7
Medium	1
Low	1

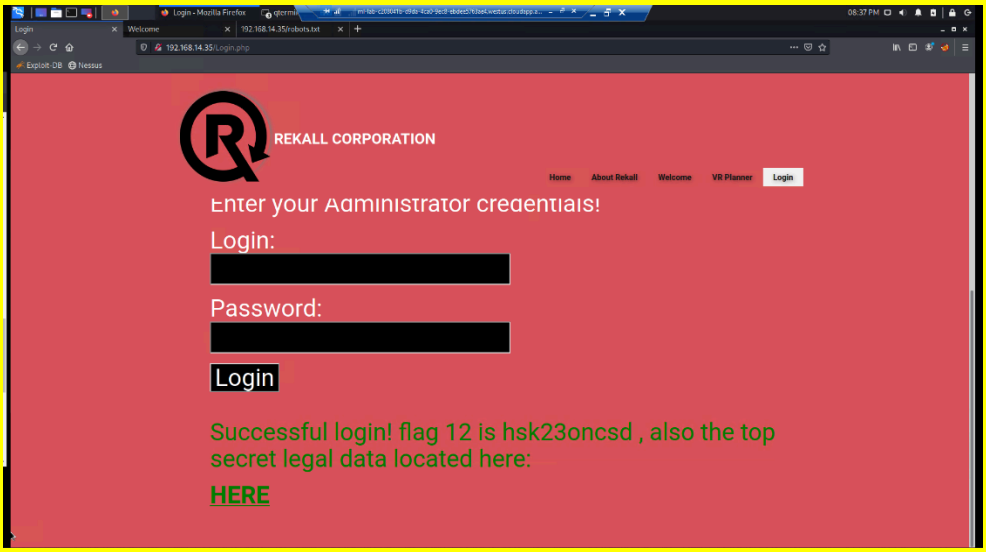
Vulnerability Findings

Vulnerability 1	Findings
Title	Sensitive Data Exposure
Type (Web app / Linux OS / WIndows OS)	Web App, Linux OS and Windows OS
Risk Rating	Critical
Description	Sensitive Data Exposure in general can have heavy ramifications if critical information is exposed. The example given here is simply a basic curl command, but the idea behind having sensitive data secured is an overarching theme for Cyber Security.

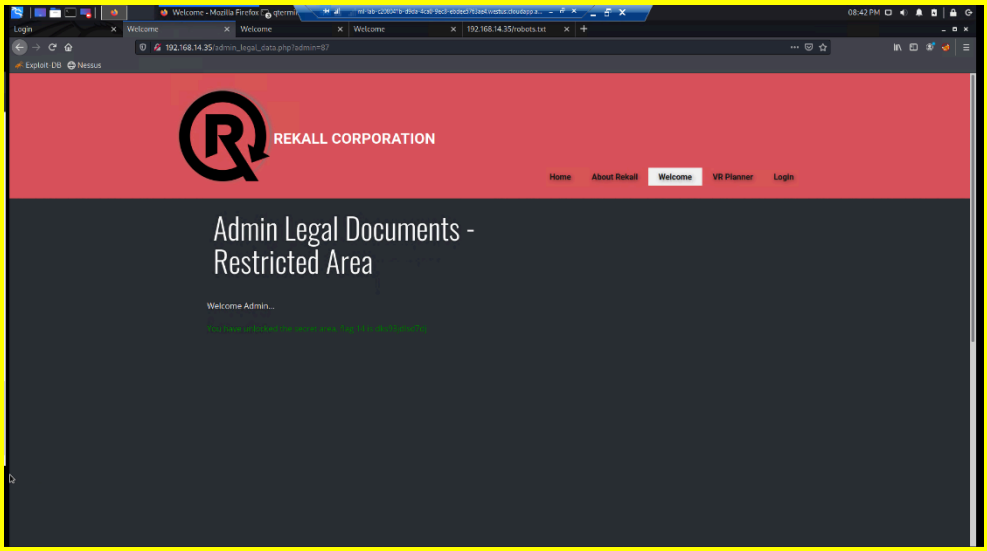
Images	
Affected Hosts	Web App, Rekall Infrastructure.
Remediation	Staying up to date on Cyber Security trends, capabilities and vulnerabilities.

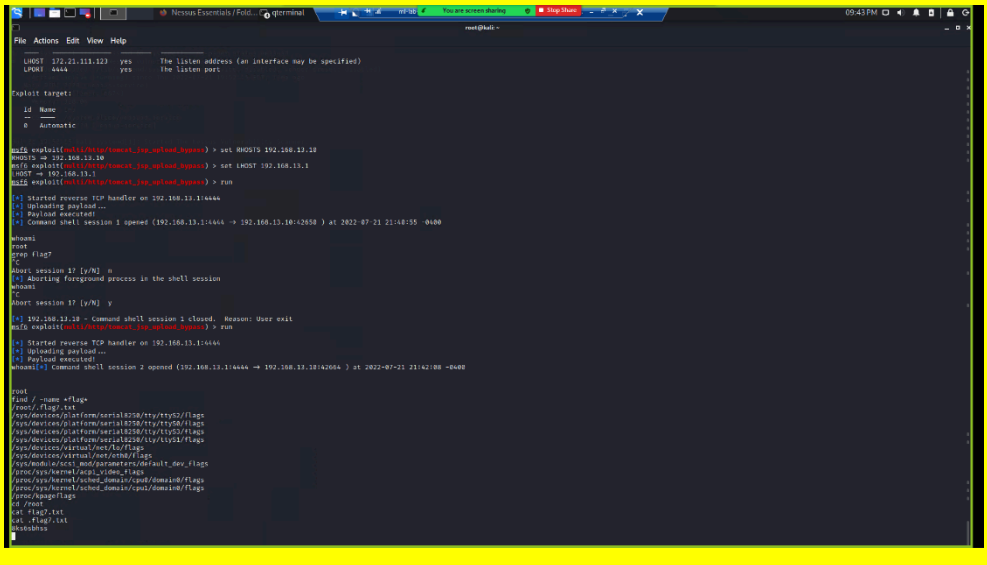
Vulnerability 2	**Findings**
Title	SQL Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	SQL Injection, depending on where and what it's intending to do, can allow a hostile actor to gain access to critical information. Such as (in this situation) login credentials.
Images	
Affected Hosts	Web App, Rekall Infrastructure.

Remediation	Input validation, prepared statements, stronger requirements for login credentials.

Vulnerability 3	Findings
Title	Brute Force Attack
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	Brute Force Attacks are a common act by hostile actors to acquire access by utilizing login credentials. Typically by inputting large amounts of possible user credential combinations.
Images	
Affected Hosts	Web App, Rekall Infrastructure.
Remediation	Stronger requirements for login credentials, two factor authentication, limiting login attempts until account lockout.

Vulnerability 4	Findings
Title	Session Management
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Critical
Description	By manipulating which session ID is being used (through URL manipulation or tools such as BurpSuite) a hostile actor can gain access to sensitive data, possibly with Admin privileges.

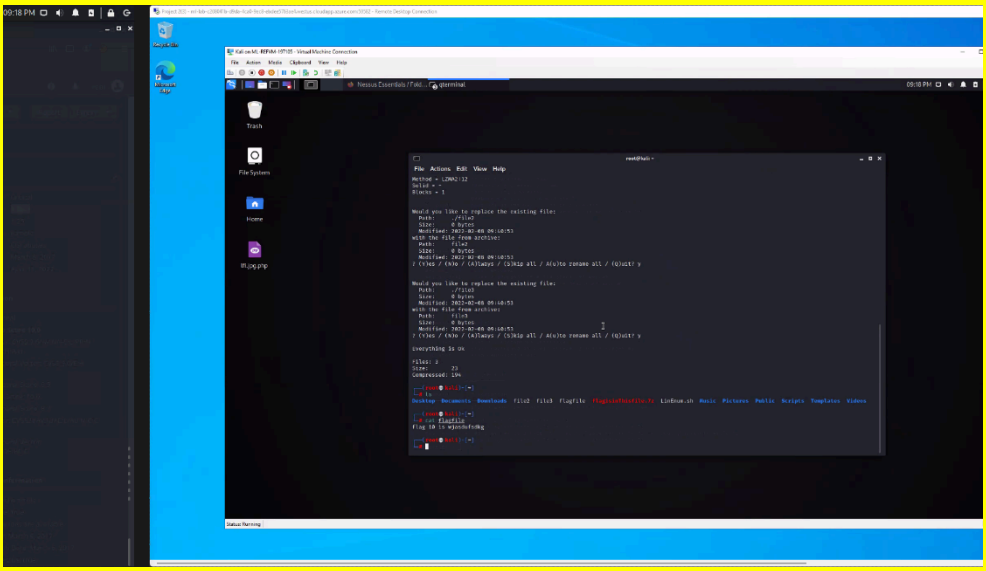
Images	
Affected Hosts	Web App, Rekall Infrastructure.
Remediation	Session ID regeneration, stronger requirements for login credentials, two factor authentication, limiting login attempts until lockout.

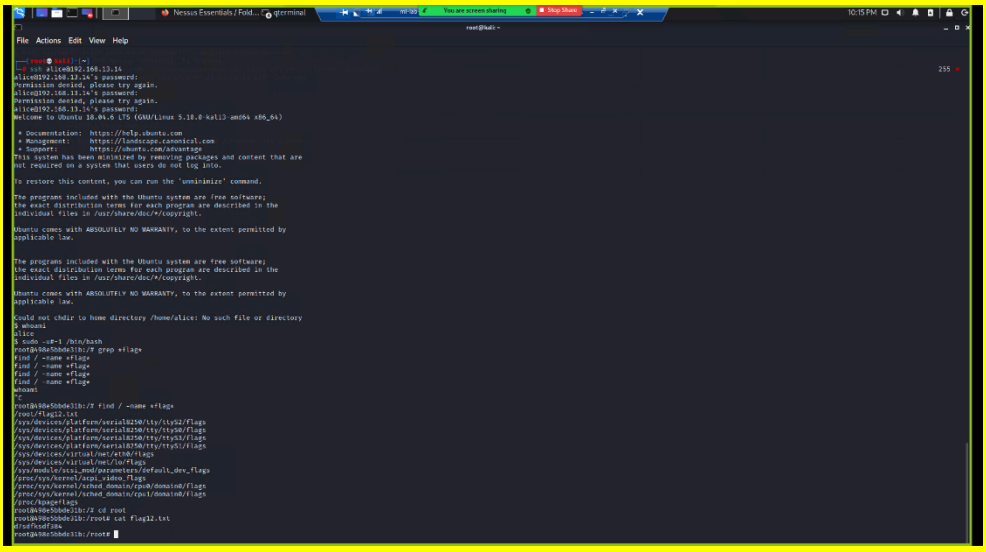
Vulnerability 5	**Findings**
Title	Apache Tomcat RCE (CVE-2017-12617)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Through the Apache Tomcat jsp_upload_bypass exploit we were able to gain access to the Linux system and create a shell with root privileges. From there many actions are possible, exposing the entire Rekall infrastructure.
Images	

Affected Hosts	Linux OS, Rekall Infrastructure.
Remediation	Keeping your operating systems up to date is crucial to prevent known vulnerabilities from affecting your infrastructure. Regular backups will also keep your systems safe from critical failures, malware or ransomware.

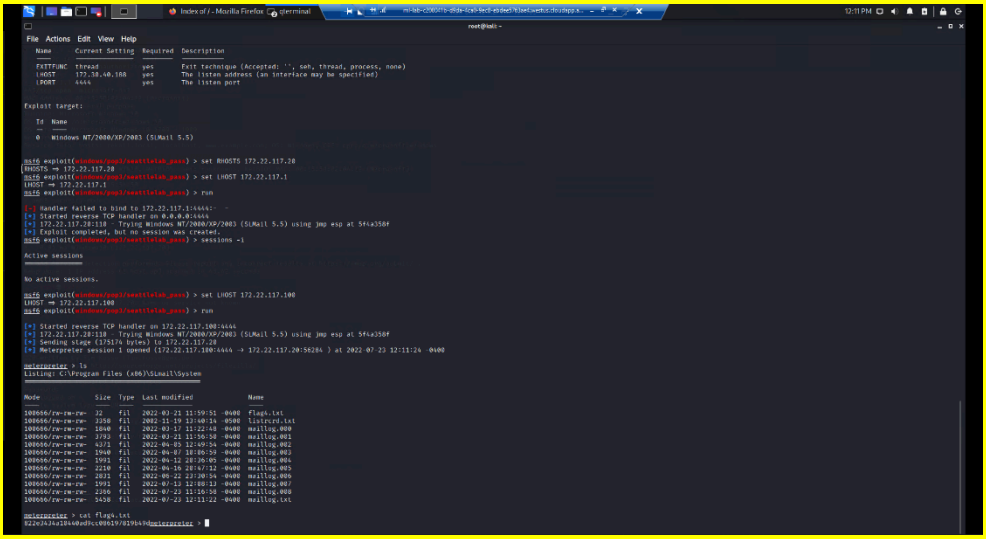
Vulnerability 6	Findings
Title	Shellshock
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Systems that have an outdated version of Bash can be vulnerable to the Shellshock exploit. Commands can be executed with higher privileges.
Images	
Affected Hosts	Linux OS, Rekall Infrastructure.
Remediation	Updating Bash should prevent this vulnerability from being an exploitable weakness

Vulnerability 7	Findings
Title	Struts (CVE-2017-5638)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Through the Nessus tool we discovered 192.168.13.12 was vulnerable to a Struts exploit. We then used Remote Code Execution to access and extract critical files.

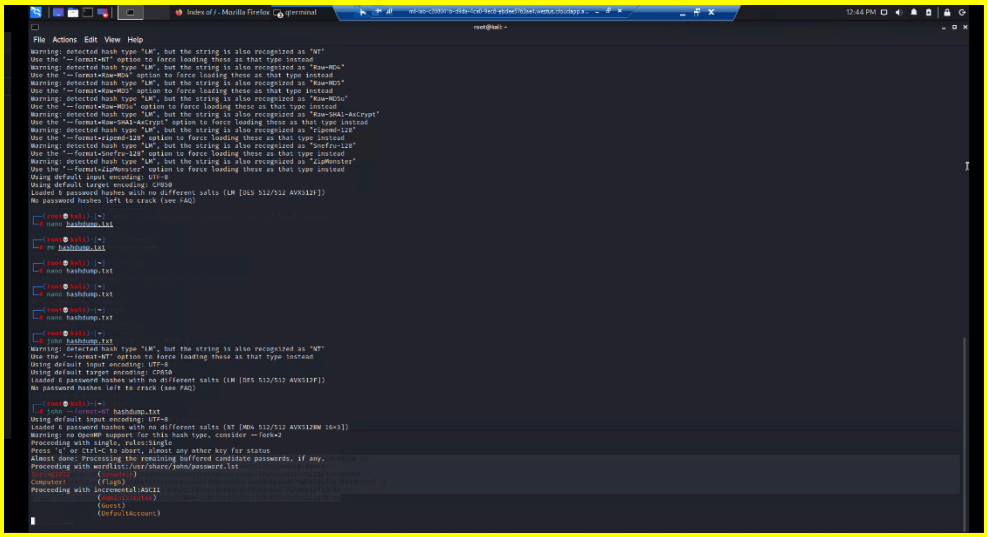
Images	
Affected Hosts	Linux OS, Rekall Infrastructure.
Remediation	Updating Apache Struts to the current version should fix this vulnerability.

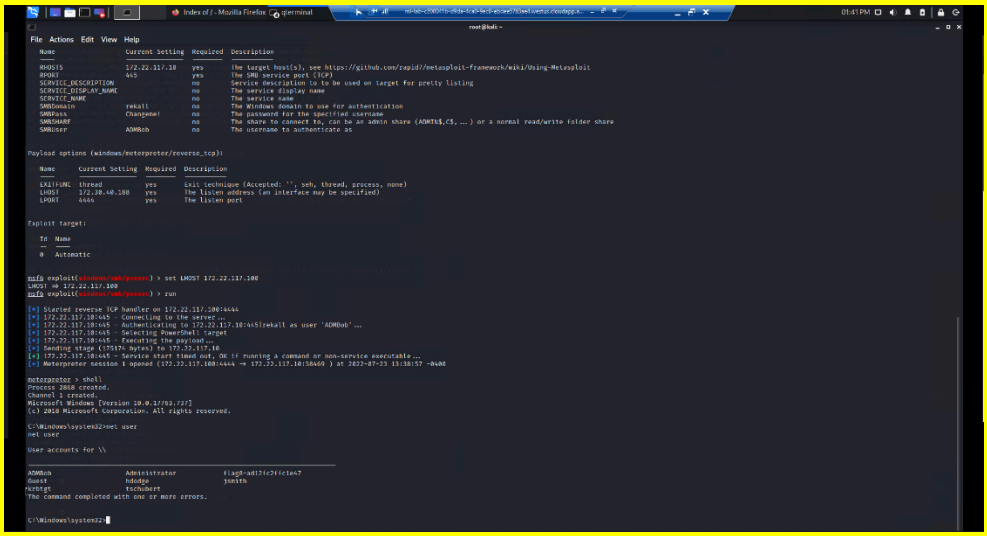
Vulnerability 8	**Findings**
Title	Sudo Blacklist Privilege Escalation (CVE-2019-14287)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	Critical
Description	Using SSH we connected to 192.168.13.14, using a previously discovered username we gained access by guessing the password. Then escalated our privileges with terminal commands.
Images	
Affected Hosts	Linux OS, Rekall Infrastructure.

Remediation	Stronger requirements for login credentials would remedy this vulnerability.

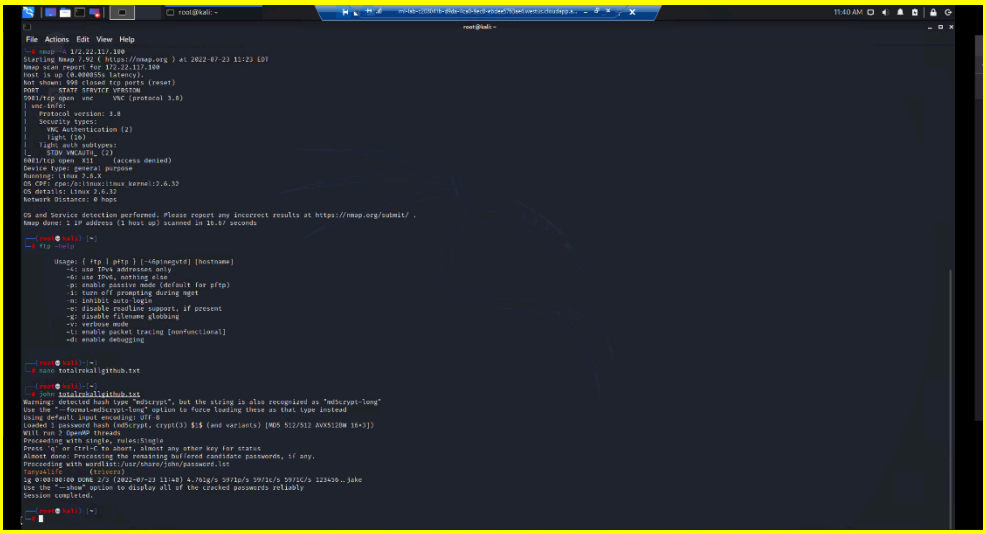
Vulnerability 9	Findings
Title	SLMail exploit through 110/tcp pop3 Port
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Through using a Seattle Lab Mail exploit we gained access to servers through the pop3 Port, allowing us to launch a shell.
Images	
Affected Hosts	Windows OS, Rekall Infrastrucure.
Remediation	Close or restrict unnecessary open ports.

Vulnerability 10	Findings
Title	Kiwi tool and LSA Credential Dump
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	After launching a shell on the Windows OS, we were able to load a tool called Kiwi. This tool allowed us to expose the hashes of users that we could then crack with password cracking software.

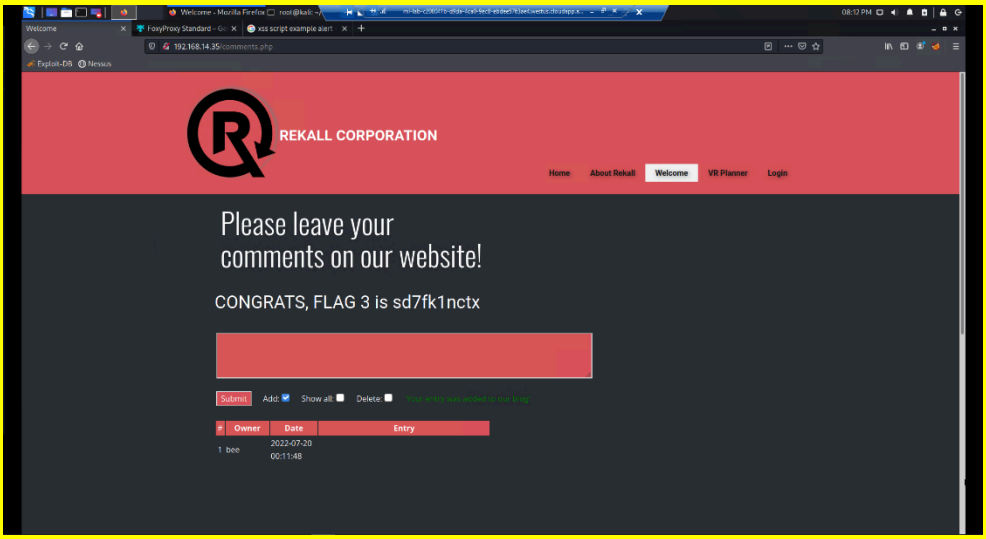
Images	
Affected Hosts	Windows OS, Rekall Infrastructure.
Remediation	Having stronger login credential requirements would stop this vulnerability from being exploited by preventing initial access of malicious actors.

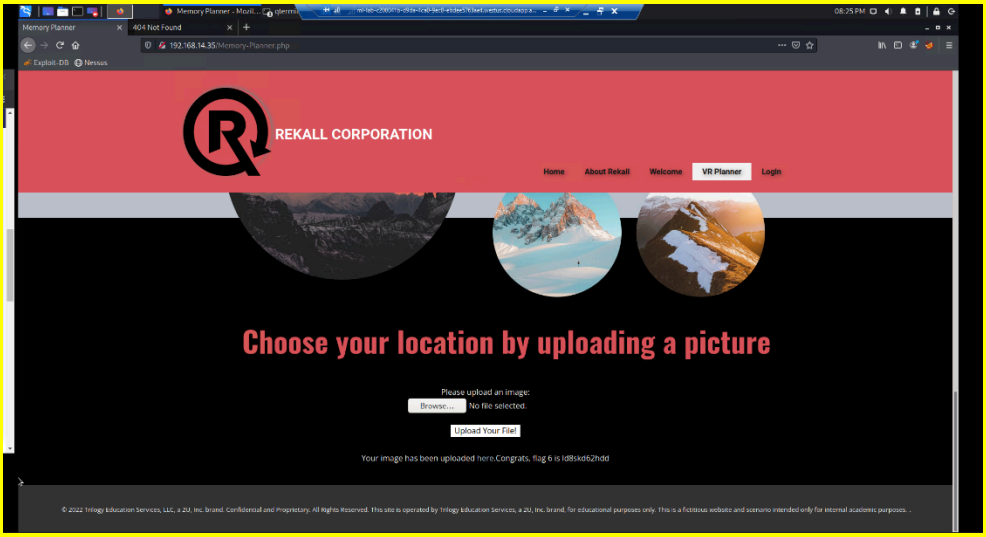
Vulnerability 11	**Findings**
Title	PSExec and SYSTEM shell
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	Using the kiwi tool on the shell we created we were able to credential dump the credentials of an Admin user. Then use a PSExec exploit to list the users in a SYSTEM shell.
Images	
Affected Hosts	Windows OS, Rekall Infrastructure.

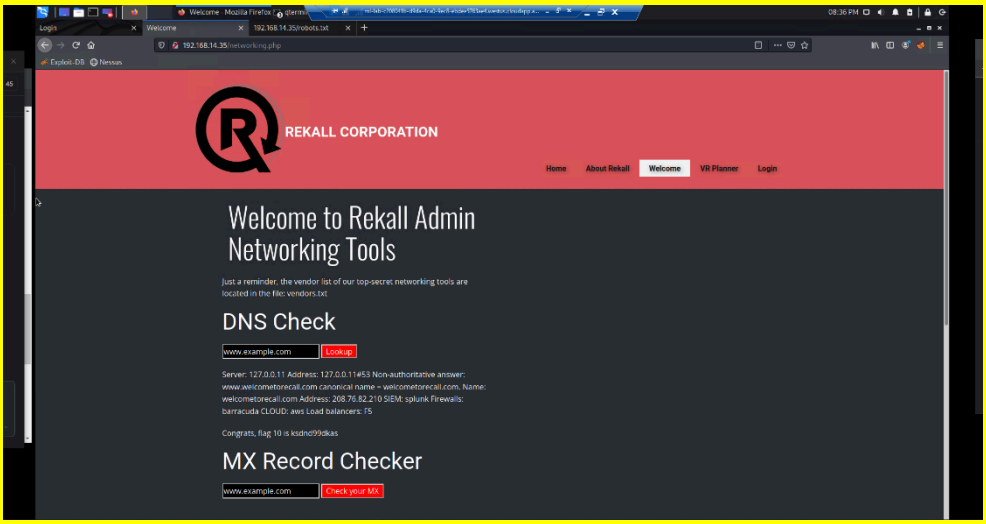
Remediation	Preventing initial access and stronger login credentials would mitigate the risk of this vulnerability.

Vulnerability 12	Findings
Title	Weak Login Credential Requirements/Third Party Vulnerabilities
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	Critical
Description	The initial access we gained to the Rekall systems came from finding a password hash on GitHub, a third-party website. Cracking this hash we found gave us a login username and password to begin our exploits.
Images	
Affected Hosts	Windows OS
Remediation	Stronger requirements for login credentials would stop this vulnerability. Also educating employees on how to properly handle login/logoff procedures and retaining login credential confidentiality.

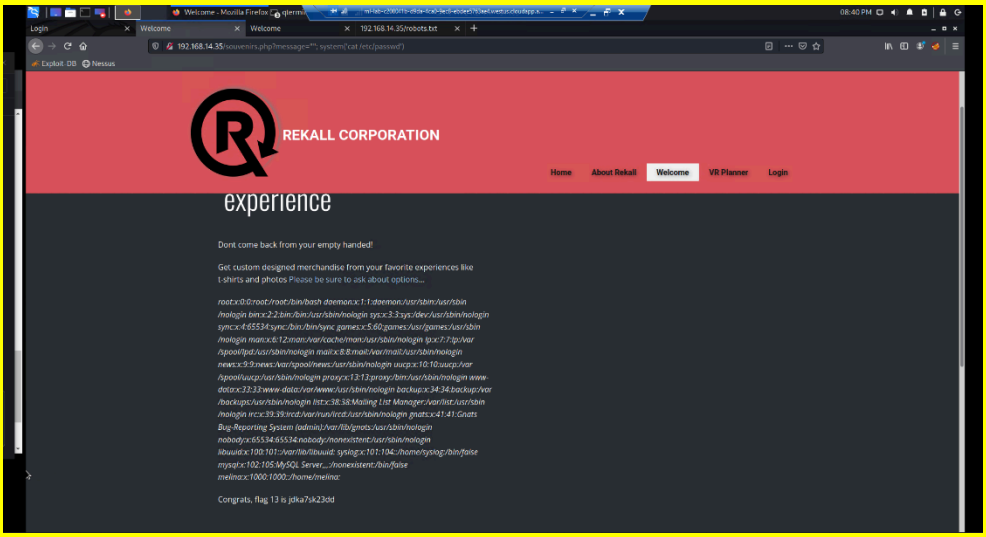
Vulnerability 13	Findings
Title	Cross Site Scripting (XSS) stored
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	Through inputting a script on the comments page we were able to manipulate the webpage.

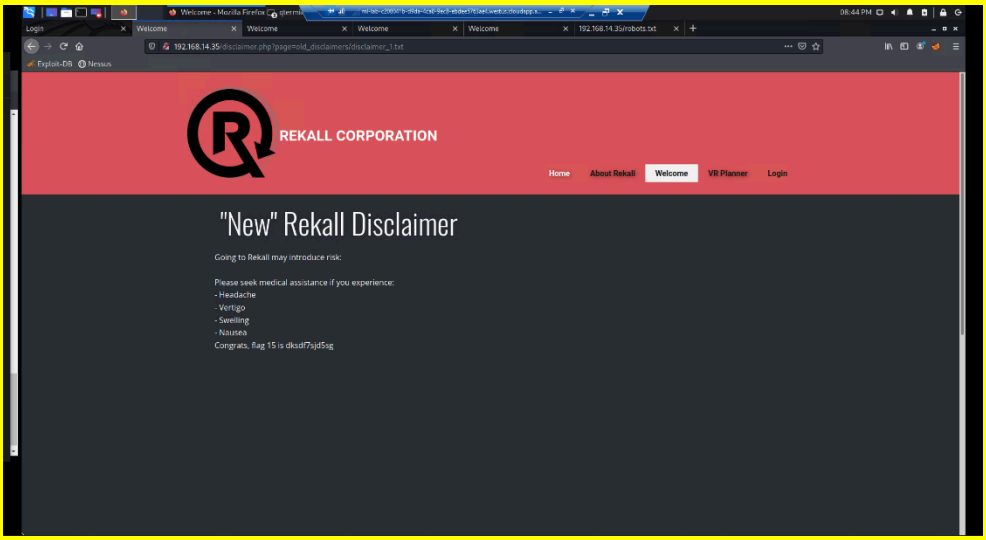
Images	
Affected Hosts	Web App
Remediation	Input validation and prepared statements can prevent this vulnerability.

Vulnerability 14	Findings
Title	Local File Inclusion
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	On the Memory-Planner page we were able to upload a custom script by renaming our file to bypass the requirements.
Images	
Affected Hosts	Web App
Remediation	Input validation and predefined characters would remedy this vulnerability.

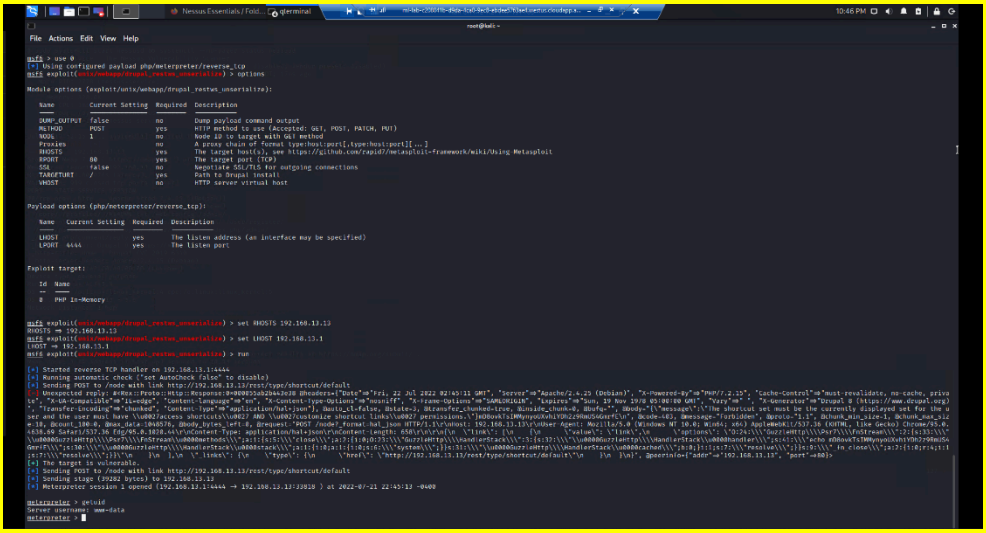
Vulnerability 15	Findings
Title	Command Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	By adding custom commands on the end of the inputted URL we were able to display confidential information.
Images	
Affected Hosts	Web App, Rekall Infrastructure.
Remediation	Input validation would not allow specific characters and invalid entries to be processed.

Vulnerability 16	Findings
Title	PHP Injection
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	After finding a hidden website with previous exploits we altered the URL to show this page's confidential information. Exposing valuable information.

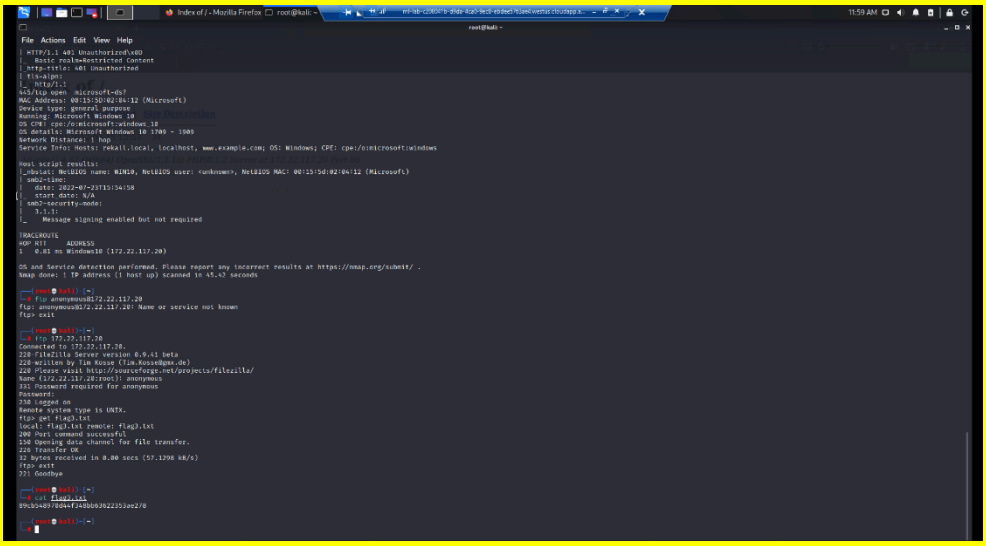
Images	
Affected Hosts	Web App, Rekall Infrastructure.
Remediation	If the Web App needs to have hidden pages, they shouldn't be allowed to be viewed by anyone with less than Administrator privileges.

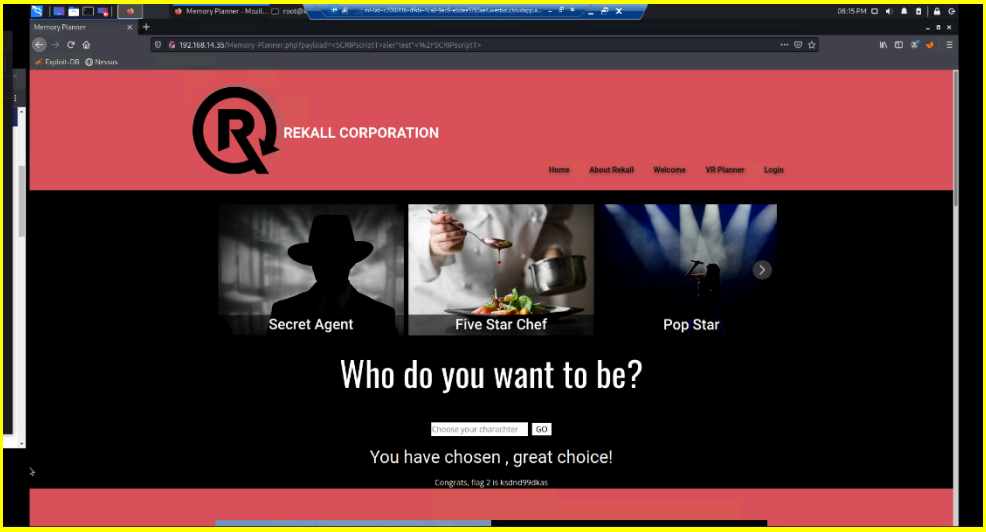
Vulnerability 17	Findings
Title	Directory Traversal
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	High
Description	After discovering directories through previous exploits we uncovered old disclaimers that could be viewed by altering the URL.
Images	
Affected Hosts	Web App

Remediation	Discarding unneeded portions of applications that could pose vulnerabilities is a good practice and could mitigate future risks.

Vulnerability 18	Findings
Title	Drupal (CVE-2019-6340)
Type (Web app / Linux OS / WIndows OS)	Linux OS
Risk Rating	High
Description	After running an aggressive nmap scan on 192.168.13.13 we discovered a vulnerability with Drupal. After launching a shell we gained server access.
Images	
Affected Hosts	Linux OS, Rekall Infrastructure.
Remediation	Updating software to current builds can mitigate risk to many known vulnerabilities.

Vulnerability 19	Findings
Title	FTP Exfiltration Techniques
Type (Web app / Linux OS / WIndows OS)	Windows OS
Risk Rating	High
Description	Upon aggressively scanning 172.22.117.20 we found port 21 FTP open, also showing us that Anonymous users are allowed to login.

Images	
Affected Hosts	Windows OS, Rekall Infrastructure.
Remediation	Increasing requirements for which users are allowed to use FTP port 21 would mitigate the risk of this exploit.

Vulnerability 20	**Findings**
Title	Cross Site Scripting (XSS) reflected
Type (Web app / Linux OS / WIndows OS)	Web App
Risk Rating	Medium
Description	On the Welcome and Memory-Planner pages we were able to enter custom scripts to manipulate the webpage.
Images	
Affected Hosts	Web App.

Remediation	Input validation would mitigate this risk.

Vulnerability 21	Findings
Title	Open Source Exposed Data
Type (Web app / Linux OS / WIndows OS)	Web App, Linux OS, Windows OS
Risk Rating	Low
Description	Anyone who is determined to do legitimate reconnaissance can find open source data on their intended target (IP addresses, open port scanning, SSL certificates, cookie information, etc.). Because it is so easily acquired, this is low risk but leads to medium, high and critical vulnerabilities.
Images	
Affected Hosts	Web App, Linux OS, Windows OS, Rekall Infrastructure.
Remediation	Be constantly aware of what information is being broadcasted about your company, product, systems and infrastructure. Be vigilant on determining which risks are necessary and which are unnecessary.

MITRE ATT&CK Matrix:
Successful Vulnerabilities are highlighted.