Ethical Hacking
Security Assessment Findings Report

Information Technology

Date: Juny 1th, 2024
Project: DC-001
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Corp and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Demo Corp and TCMS.

Demo Corp may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

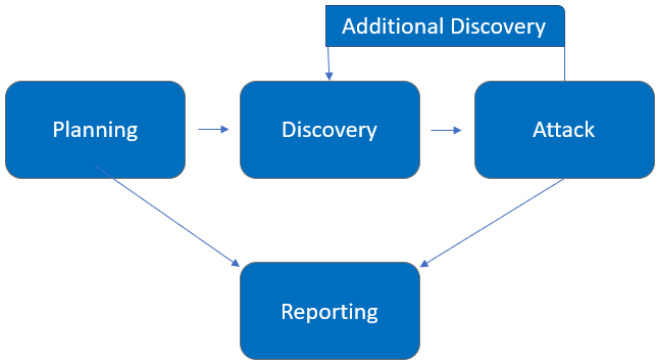
Name	Title	Contact Information
Demo Corp		
Subkhan Masudi	5027221044	Email: akutuban2@gmail.com

Assessment Overview

From May 31nd, 2024 to June 1th, 2024, All testing performed is based on the Information Security Testing and Assessment Technical Guide module, OWASP ZAP Testing Guide, and customized testing frameworks.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Assessment Components

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Jay's Bank Application Penetration Testing	167.172.75.216

Scope Exclusions

Per client request, TCMS did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Demo Corp.

Client Allowances

Demo Corp provided TCMS the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

TCMS evaluated Demo Corp's internal security posture through penetration testing from May 31nd, 2021 to June 1th, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for ten
(10) business days.

Testing Summary

The network assessment evaluated Demo Corp's internal network security posture. From an internal perspective, the TCMS team performed vulnerability scanning against all IPs provided by Demo Corp to evaluate the overall patching health of the network. The team also performed common Active Directory based attacks, such as Link-Local Multicast Name Resolution (LLMNR) Poisoning, SMB relaying, IPv6 man-in-the-middle relaying, and Kerberoasting. Beyond vulnerability scanning and Active Directory attacks, the TCMS evaluated other potential risks, such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

The TCMS team discovered that LLMNR was enabled in the network (Finding IPT-001), which permitted the interception of user hashes via LLMNR poisoning. These hashes were taken offline and cracked via dictionary attacks, which signals a weak password policy (Finding IPT-005). Utilizing the cracked passwords, the TCMS team gained access to several machines within the network, which indicates overly permissive user accounts.

With machine access, and the use of older operating systems in the network (Finding IPT-009), the team was able to leverage WDigest (Finding IPT-003) to recover cleartext credentials to accounts. The team was also able to dump local account hashes on each machine accessed. The TCMS team discovered that the local account hashes were being re-used across devices (Finding IPT-002), which lead to additional machine access through pass-the-hash attacks.

Ultimately, the TCMS team was able to leverage accounts captured through WDigest and hash dumps to move laterally throughout the network until landing on a machine that had a

Domain Administrator credential in cleartext via WDigest. The testing team was able to use this credential to log into the domain controller and compromise the entire domain. For a full walkthrough of the path to Domain Admin, please see Finding IPT-025.

In addition to the compromise listed above, the TCMS team found that users could be impersonated through delegation attacks (Finding IPT-004), SMB relay attacks were possible due to SMB signing being disabled (Finding IPT-007), and IPv6 traffic was not restricted, which could lead to LDAPS relaying and domain compromise (Finding IPT-006).

The remainder of critical findings relate to patch management as devices with critical out-of-date software (Finding IPT-008), operating systems (Finding IPT-009), and Microsoft RCE vulnerabilities (Findings IPT-010, IPT-011, IPT-012, IPT-013), were found to be present within the network.

The remainder of the findings were high, moderate, low, or informational. For further information on findings, please review the Technical Findings section.

Tester Notes and Recommendations

Testing results of the Demo Corp network are indicative of an organization undergoing its first penetration test, which is the case here. Many of the findings discovered are vulnerabilities within Active Directory that come enabled by default, such as LLMNR, IPv6, and Kerberoasting.

During testing, two constants stood out: a weak password policy and weak patching. The weak password policy led to the initial compromise of accounts and is usually one of the first footholds an attacker attempts to use in a network. The presence of a weak password policy is backed up by the evidence of our testing team cracking over 2,200 user account passwords, including a majority of the Domain Administrator accounts, through basic dictionary attacks.

We recommended that Demo Corp re-evaluates their current password policy and considers a policy of 15 characters or more for their regular user accounts and 30 characters or more for their Domain Administrator accounts. We also recommend that Demo Corp explore password blacklisting and will be supplying a list of cracked user passwords for the team to evaluate. Finally, a Privilege Access Management solution should be considered.

Weak patching and dated operating systems led to the compromise of dozens of machines within the network. We believe the number of compromised machines would have been significantly larger, however the TCMS and Demo Corp teams agreed it was not necessary to attempt to exploit any remote code execution (RCE) based vulnerabilities, such as MS17-010 (Finding IPT-012), as the domain controller had already been compromised and the teams did not want to risk any denial of service through failed attacks.

We recommend that the Demo Corp team review the patching recommendations made in the Technical Findings section of the report along with reviewing the provided Nessus

scans for a full overview of items to be patched. We also recommend that Demo Corp improve their patch management policies and procedures to help prevent potential attacks within their network.

On a positive note, our testing team triggered several alerts during the engagement. The Demo Corp Security Operations team discovered our vulnerability scanning and was alerted when we attempted to use noisy attacks on a compromised machine. While not all attacks were discovered during testing, these alerts are a positive start. Additional guidance on alerting and detection has been provided for findings, when necessary, in the Technical Findings section.

Overall, the Demo Corp network performed as expected for a first-time penetration test. We recommend that the Demo Corp team thoroughly review the recommendations made in this report, patch the findings, and re-test annually to improve their overall internal security posture.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools (Nessus)
2. Mimikatz detected on some machines
3. Service accounts were not running as domain administrators
4. Demo Corp local administrator account password was unique to each device The following identifies the key weaknesses identified during the assessment:

1. Password policy found to be insufficient
2. Critically out-of-date operating systems and weak patching exist within the network
3. Passwords were observed in cleartext due to WDigest
4. LLMNR is enabled within the network
5. SMB signing is disabled on all non-server devices in the work
6. IPv6 is improperly managed within the network
7. User accounts can be impersonated through token delegation
8. Local admin accounts had password re-use and were overly permissive
9. Default credentials were discovered on critical infrastructure, such as iDRACs
10. Unauthenticated share access was permitted
11. User accounts were found to be running as service accounts
12. Service accounts utilized weak passwords
13. Domain administrator utilized weak passwords

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

0	0	0	0	0
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Analisis Network (Nmap)	Low	Implement network segmentation to limit the impact of network scans. Use Intrusion Detection Systems (IDS) to detect unauthorized scanning. Regularly audit and update firewall rules to prevent unauthorized access.
SQLMap Injection	Moderate	Use prepared statements and parameterized queries to prevent SQL injection. Employ input validation and sanitization techniques. Regularly update and patch database systems and applications. Implement web application firewalls (WAF) to block malicious SQL queries.

Vulnerability: Authentication Bypass via Brute Force (Hydra)	High	Implement account lockout mechanisms after a number of failed login attempts. Use multi-factor authentication (MFA) to enhance security. Enforce strong password policies and regularly update passwords. Monitor login attempts and implement logging and alerting for suspicious activity.
Burp Suite	High	Conduct regular web application security assessments and fix identified vulnerabilities. Implement secure coding practices to prevent common web vulnerabilities. Use Content Security Policy (CSP) and other security headers to protect web applications. Regularly update and patch web servers, frameworks, and libraries.

Technical Findings

Internal Penetration Test Findings

Reconnaissance Nmap IP

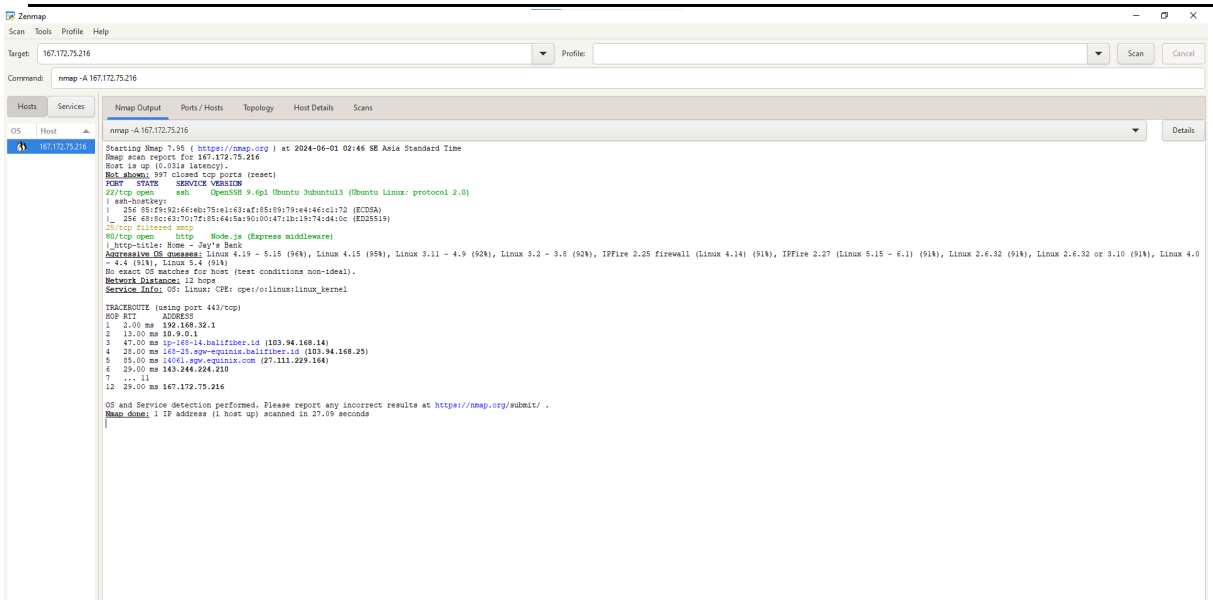
Description:	Nmap (Network Mapper) is an open-source tool for network exploration and security auditing. It is designed for quickly scanning large networks but also works well against single hosts.
Risk:	Using Nmap without authorization can be considered suspicious activity or even illegal. Aggressive scanning can cause overload or crashes on some network systems.
System:	Windows
Tools Used:	Nmap
References:	https://nmap.org/

Evidence

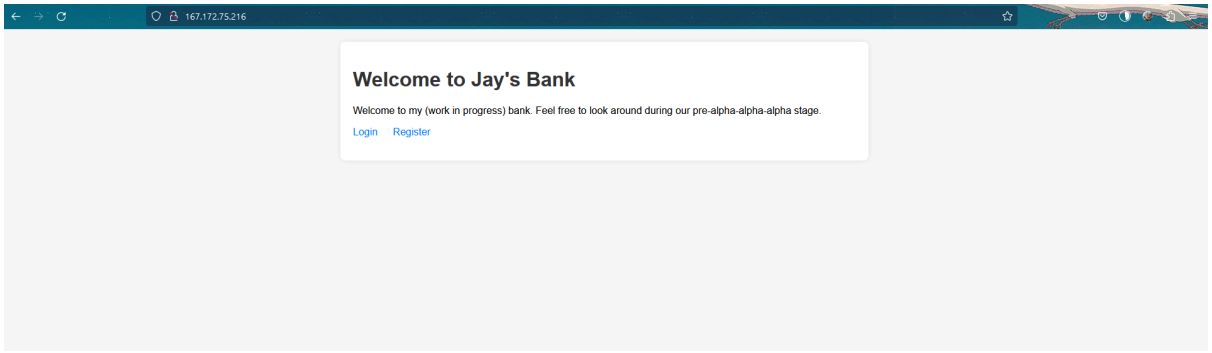
Pengujian Reconnaissance terhadap IP Address 167.172.75.216 menggunakan Nmap berhasil menemukan beberapa port

1. Siapkan Nmap pada windows / linux
2. Jalankan perintah nmap untuk melakukan Reconnaissance pada ip :
   nmap -A 167.172.75.216

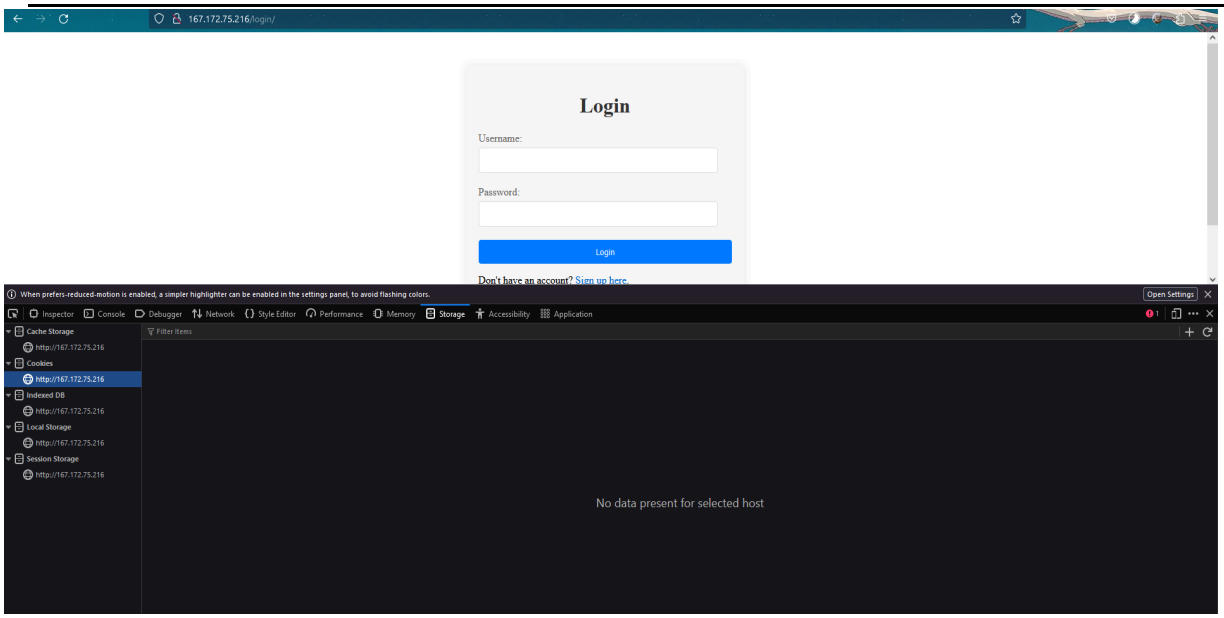
3. Hasil:
   dari nmap menemukan hasil seperti ini, dengan menggunakan **nmap -A 167.172.75.216**



4. ketika mencoba membuka **port 80** muncul **login page/ register**



5. jika hanya menggunakan **inspect f12** pada browser tidak menemukan cookie yg terbuka



Remediation

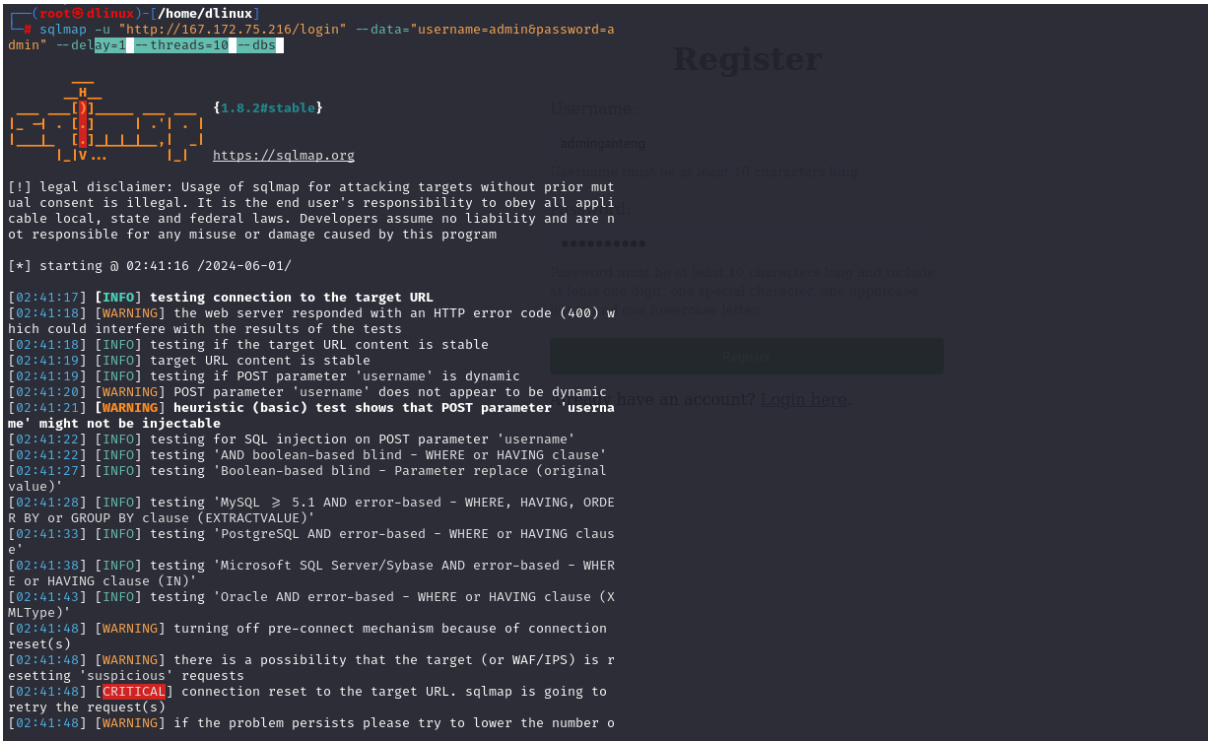
- Implement network segmentation to limit the impact of network scans.
- Use Intrusion Detection Systems (IDS) to detect unauthorized scanning.
- Regularly audit and update firewall rules to prevent unauthorized access.

SQL Injection (SQLMap)

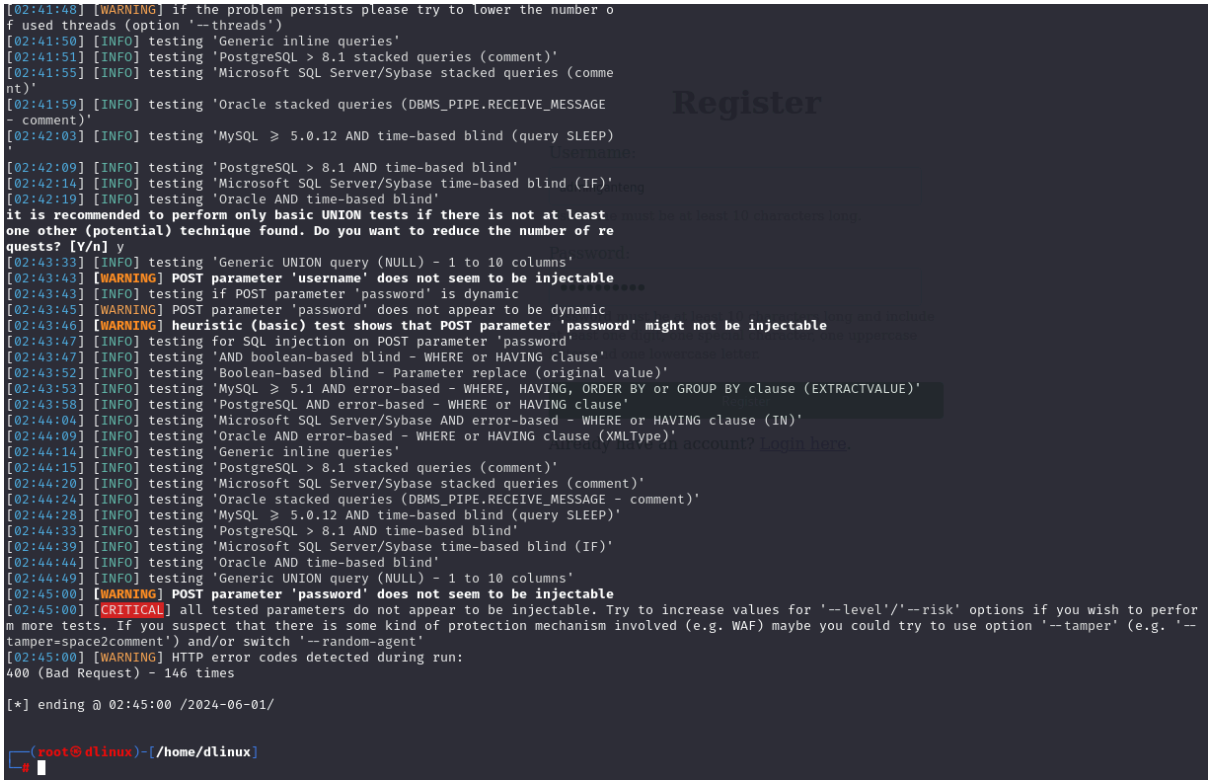
Description:	SQLMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications. The tool can exploit vulnerabilities to take over database servers.
Risk:	Exploiting SQL injection vulnerabilities can lead to unauthorized access to sensitive data, data modification, or even complete control of the database server. Using this tool without permission can violate legal and ethical cybersecurity standards.
System:	Windows, Linux
Tools Used:	SQLMap
References:	SQLMap Official Website "The Web Application Hacker's Handbook" by Dafydd Stuttard and Marcus Pinto

Evidence

mencoba untuk melakukan SQLMap Injection menggunakan command “ sqlmap -u "http://167.172.75.216/login" --data="username=admin&password=admin" --delay=1 --threads=10 --dbs



”



Remediation

- Use prepared statements and parameterized queries to prevent SQL injection.
- Employ input validation and sanitization techniques.
- Regularly update and patch database systems and applications.
- Implement web application firewalls (WAF) to block malicious SQL queries.

Vulnerability: Authentication Bypass via Brute Force (Hydra)

Description:	Hydra is a versatile brute force tool that supports various network protocols. It is used to attempt different username and password combinations to gain unauthorized access to a system.
Risk:	- Brute force attempts can lead to account lockouts or increased security monitoring. - Brute force activity is often illegal without explicit permission.
System:	Windows, Linux
Tools Used:	THC-Hydra
References:	THC-Hydra GitHub

Evidence

Pengujian **brute force** menggunakan **Hydra** berhasil menemukan kombinasi username dan password yang valid untuk username `admin`.

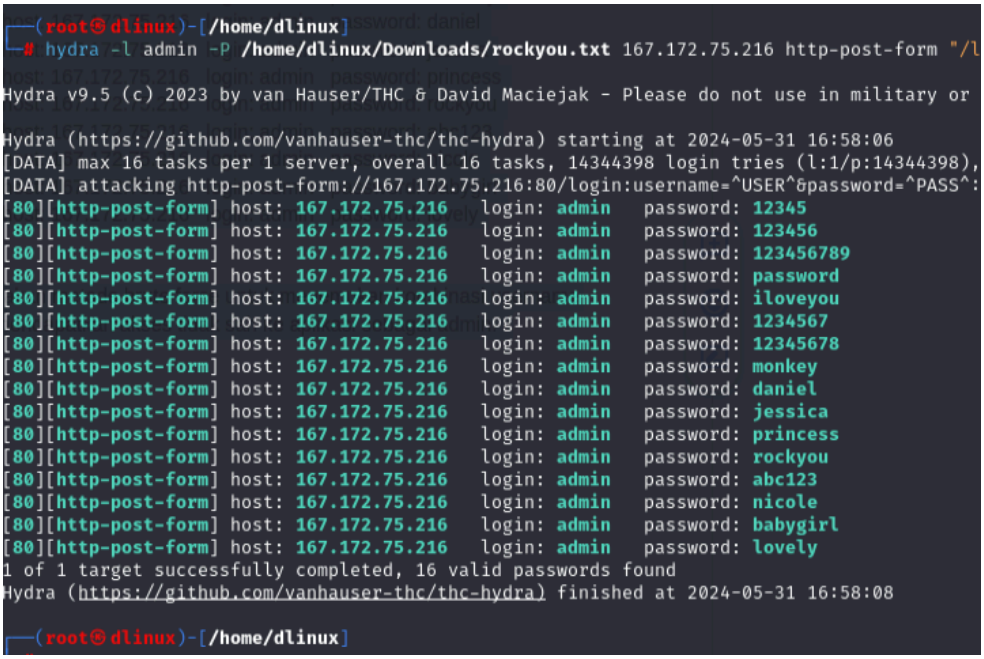
1. Siapkan file password (`**rockyou.txt**`) yang berisi daftar password umum yang digunakan untuk brute force.
2. Jalankan perintah **Hydra** berikut untuk melakukan brute force pada form login:

   hydra -l admin -P /home/dlinux/Downloads/rockyou.txt 167.172.75.216 http-post-form "/login:username=^USER^&password=^PASS^:F=Invalid username or password"

3. Hasil:
   Hydra menemukan 16 password valid untuk username `admin`:

   [80][http-post-form] host: 167.172.75.216 login: admin password: **12345**
   [80][http-post-form] host: 167.172.75.216 login: admin password: **123456**
   [80][http-post-form] host: 167.172.75.216 login: admin password: **123456789**
   [80][http-post-form] host: 167.172.75.216 login: admin password: **password**
   [80][http-post-form] host: 167.172.75.216 login: admin password: **iloveyou**
   [80][http-post-form] host: 167.172.75.216 login: admin password: **1234567**
   [80][http-post-form] host: 167.172.75.216 login: admin password: **12345678**
   [80][http-post-form] host: 167.172.75.216 login: admin password: **monkey**
   [80][http-post-form] host: 167.172.75.216 login: admin password: **daniel**
   [80][http-post-form] host: 167.172.75.216 login: admin password: **jessica**

[80][http-post-form] host: 167.172.75.216 login: admin password: **princess**
[80][http-post-form] host: 167.172.75.216 login: admin password: **rockyou**
[80][http-post-form] host: 167.172.75.216 login: admin password: **abc123**
[80][http-post-form] host: 167.172.75.216 login: admin password: **nicole**
[80][http-post-form] host: 167.172.75.216 login: admin password: **babygirl**
[80][http-post-form] host: 167.172.75.216 login: admin password: **lovely**



Dampak Potensial:
Penyerang dapat menggunakan metode brute force untuk menemukan kombinasi **username** dan **password** yang valid, mendapatkan akses tidak sah ke aplikasi sebagai **admin**.

Remediation

- Implement account lockout mechanisms after a number of failed login attempts.
- Use multi-factor authentication (MFA) to enhance security.
- Enforce strong password policies and regularly update passwords.
- Monitor login attempts and implement logging and alerting for suspicious activity.

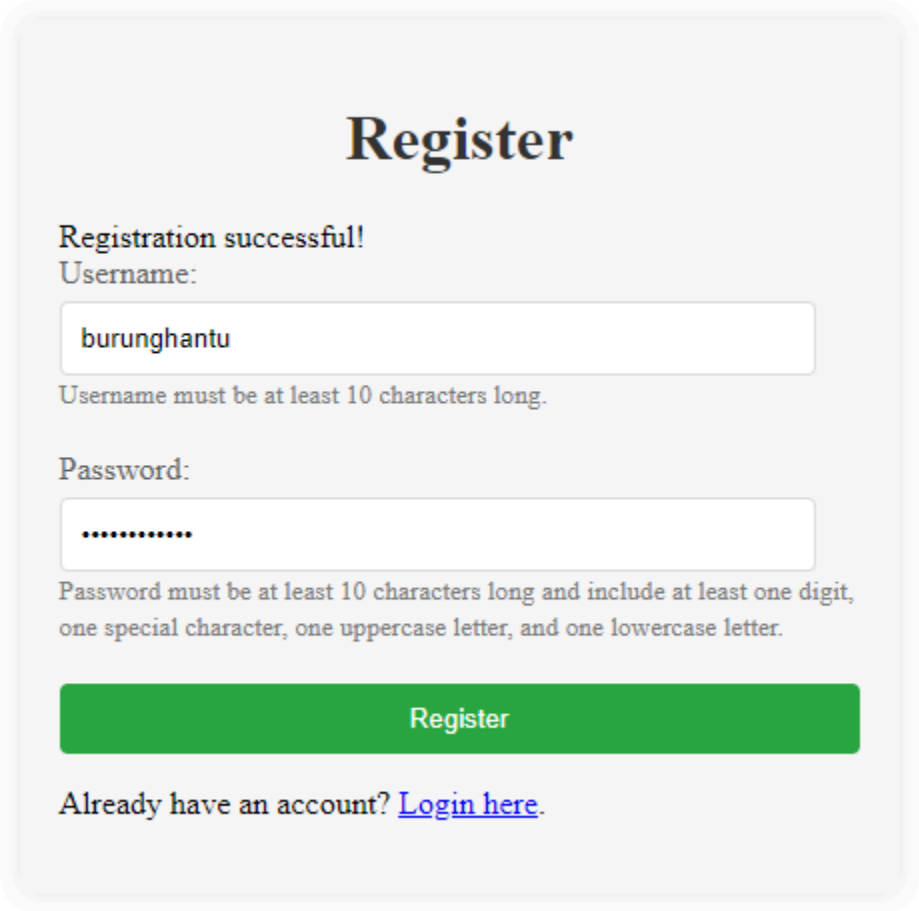
Burp Suite

Description:	Burp Suite is a platform for web application security testing. It includes various tools that work together to support the entire testing process, from mapping

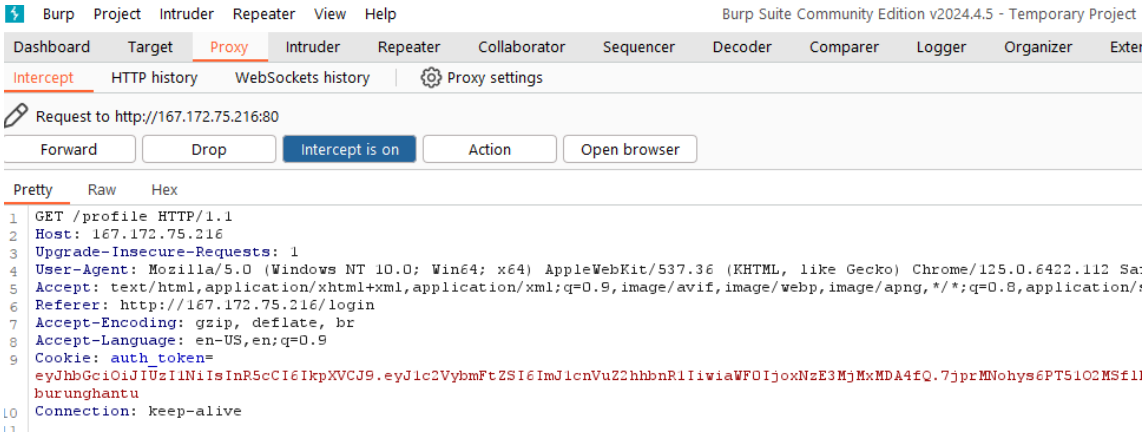
	and analyzing an application's attack surface to finding and exploiting security vulnerabilities.
Risk:	The tool can be used to find security weaknesses that can be exploited for unauthorized access or data compromise. Using Burp Suite without authorization can be considered illegal.
System:	Web applications that utilize cookies for session management
Tools Used:	Windows, linux
References:	Burp Suite Official Website

Evidence

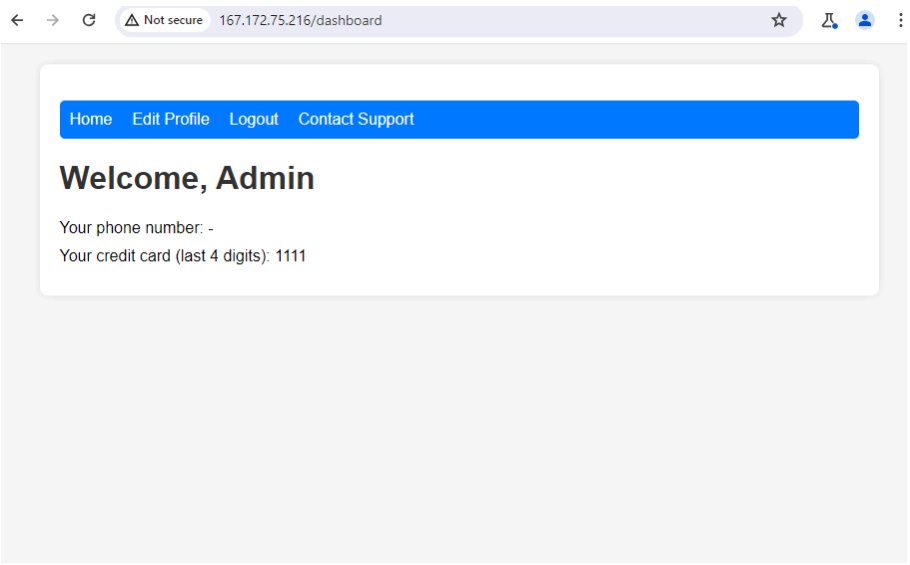
Pengujian **Burp Suite** menggunakan Aplikasi Burp Suite Windows berhasil untuk masuk kedalam laman ip.

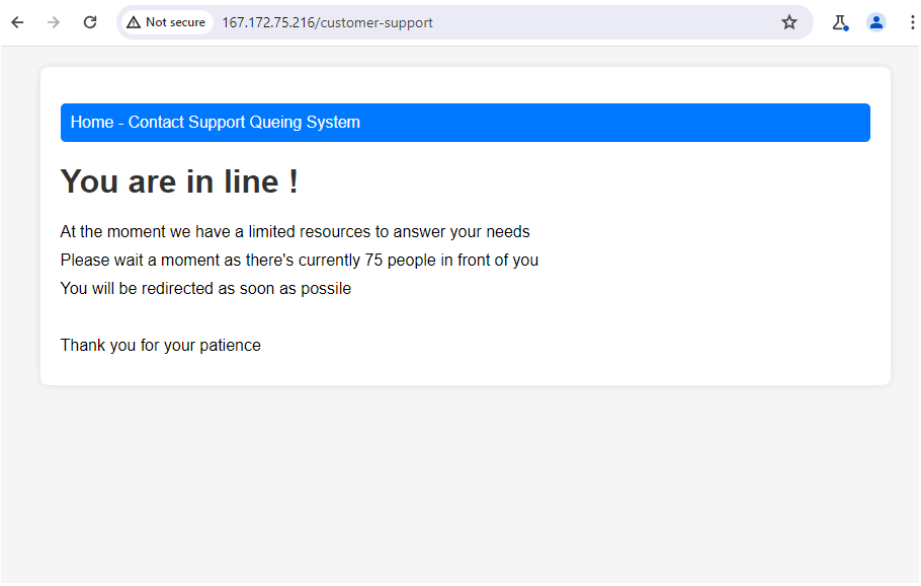


ditemukan juga auth token cookies saat di cek di proxy



sukses untuk masuk ke dashboard admin dan juga bisa check untuk contact support





Remediation

- Conduct regular web application security assessments and fix identified vulnerabilities.
- Implement secure coding practices to prevent common web vulnerabilities.
- Use Content Security Policy (CSP) and other security headers to protect web applications.
- Regularly update and patch web servers, frameworks, and libraries.

Additional Scans and Reports

TCMS provides all clients with all report information gathered during testing. This

includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by TCM Security.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled “Additional Scans and Reports”.

Last Page