Demo Company
Security Assessment Findings Report

Business Confidential

Date: Oct 7th, 2024
Project: 897-19
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Company (DC) 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 DC and TCMS.

TCMS 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

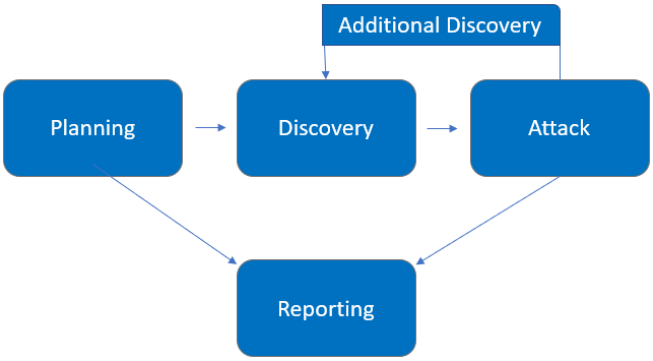
Name	Title	Contact Information
Demo Company		
John Smith	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.smith@demo.com
TCM Security		
Zidny Ilman N	Lead Penetration Tester	Email: zidnyilman224@gmail.com

Assessment Overview

From Oct 4th, 2024 to Oct 7th, 2024, DC engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), 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

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A TCMS engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

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.

Scope

Assessment	Details
External Penetration Test	10.15.42.245

Scope Exclusions

Per client request, TCMS did not perform any Denial of Service attacks during testing.

Client Allowances

DC did not provide any allowances to assist the testing.

Executive Summary

TCMS evaluated DC's external security posture through an external network penetration test from Oct 4th, 2024 to Oct 7th, 2024. By leveraging a series of attacks, TCMS found critical level vulnerabilities that allowed full internal network access to the DC headquarter office. It is highly recommended that DC address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Attack Summary

The following table describes how TCMS gained internal network access, step by step:

Step	Action	Recommendation
1	Executed nmap -sV, --top-ports, -sO, etc., to identify open ports and services on the target IP	Recommend restricting network access to open services or enhancing firewall configurations.
2	Accessed FTP using ftp 10.15.42.245 with anonymous login and found publicly accessible files	Limit anonymous FTP access and encrypt data stored on the server so it is accessible only by administrators.
3	Downloaded list.xyz containing sensitive data (username, email, password hash) and readme.txt	Improve file access permissions or encrypt sensitive files to prevent access by unauthorized users.
4	Used grep to find the bcrypt hash for *ethack* and attempted to crack it using *hashcat*	Increase password complexity and limit sensitive information access without additional encryption layers.

Security Strengths

SIEM alerts of vulnerability scans

During the assessment, the DC security team alerted TCMS engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the TCMS engineer's attacker IP address within minutes of scanning and was capable of blacklisting TCMS from further scanning actions.

Security Weaknesses

Missing Multi-Factor Authentication

TCMS leveraged multiple attacks against DC login forms using valid credentials harvested through open-source intelligence. Successful logins included employee e-mail accounts through Outlook Web Access and internal access via Active Directory login on the VPN. The use of multi-factor authentication would have prevented full access and required TCMS to utilize additional attack methods to gain internal network access.

Weak Password Policy

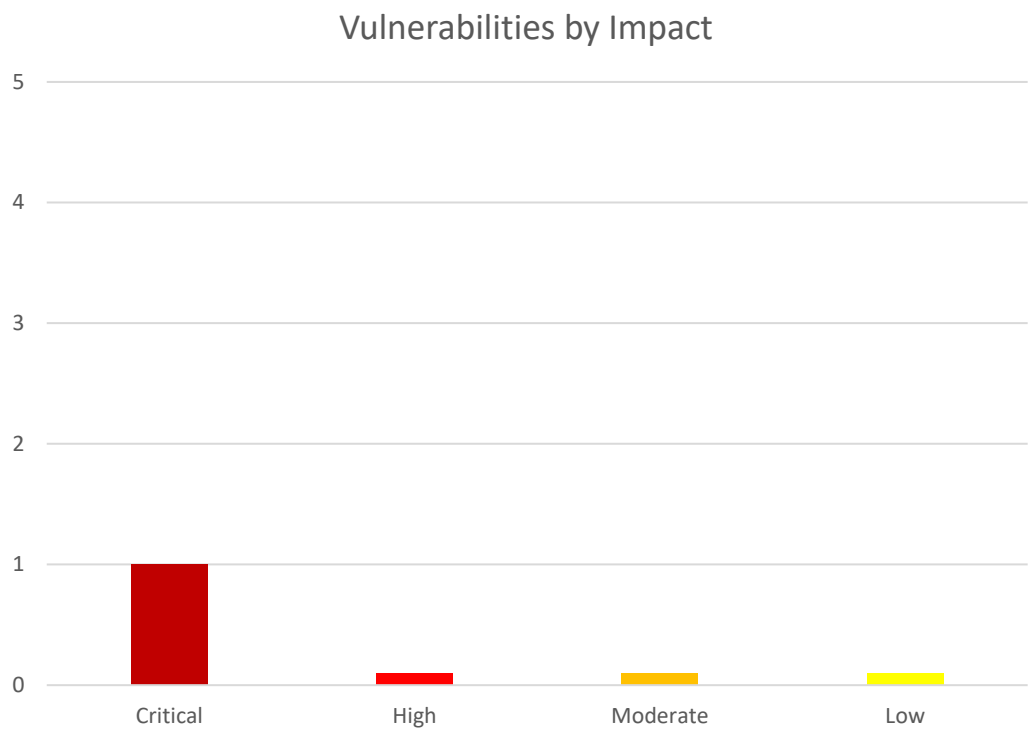
TCMS successfully performed password guessing attacks against DC login forms, providing internal network access. A predictable password format of Summer2018! (season + year + special character) was attempted and successful.

Unrestricted Logon Attempts

During the assessment, TCMS performed multiple brute-force attacks against login forms found on the external network. For all logins, unlimited attempts were allowed, which permitted an eventual successful login on the Outlook Web Access application.

Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



External Penetration Test Findings

Service Version Detection using Nmap

Description:	identifies open ports and attempts to determine the versions of services running on the target system at 10.15.42.245. This provides insight into potential service vulnerabilities.
System:	nmap -sV 10.15.42.245

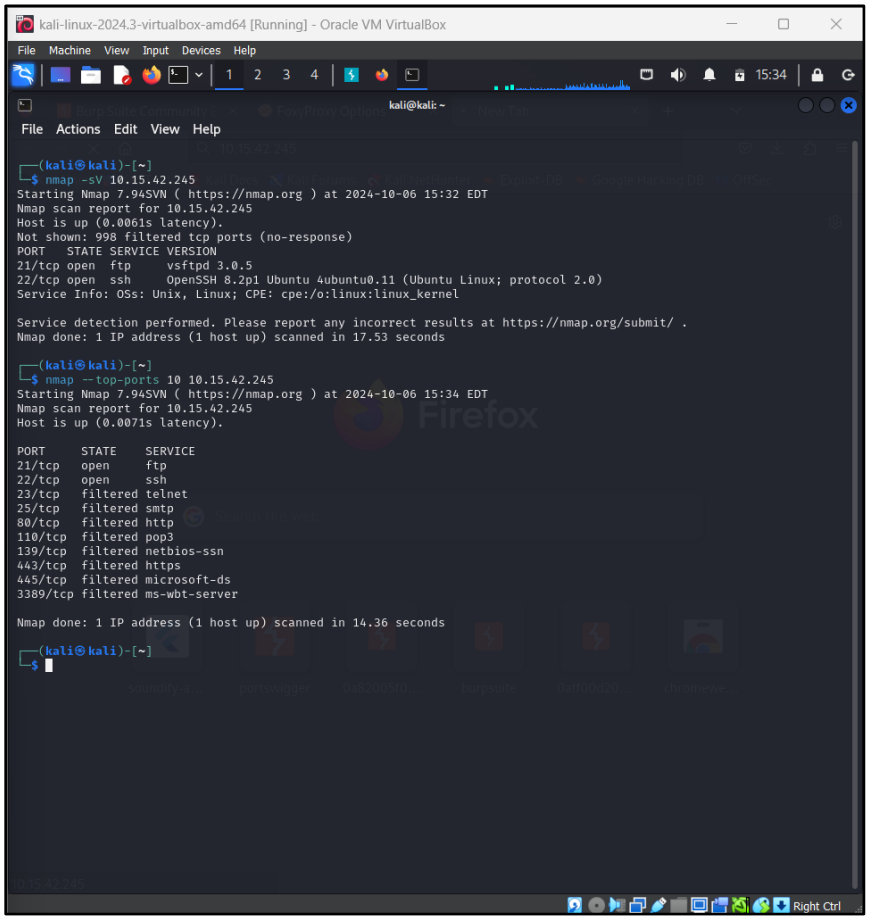
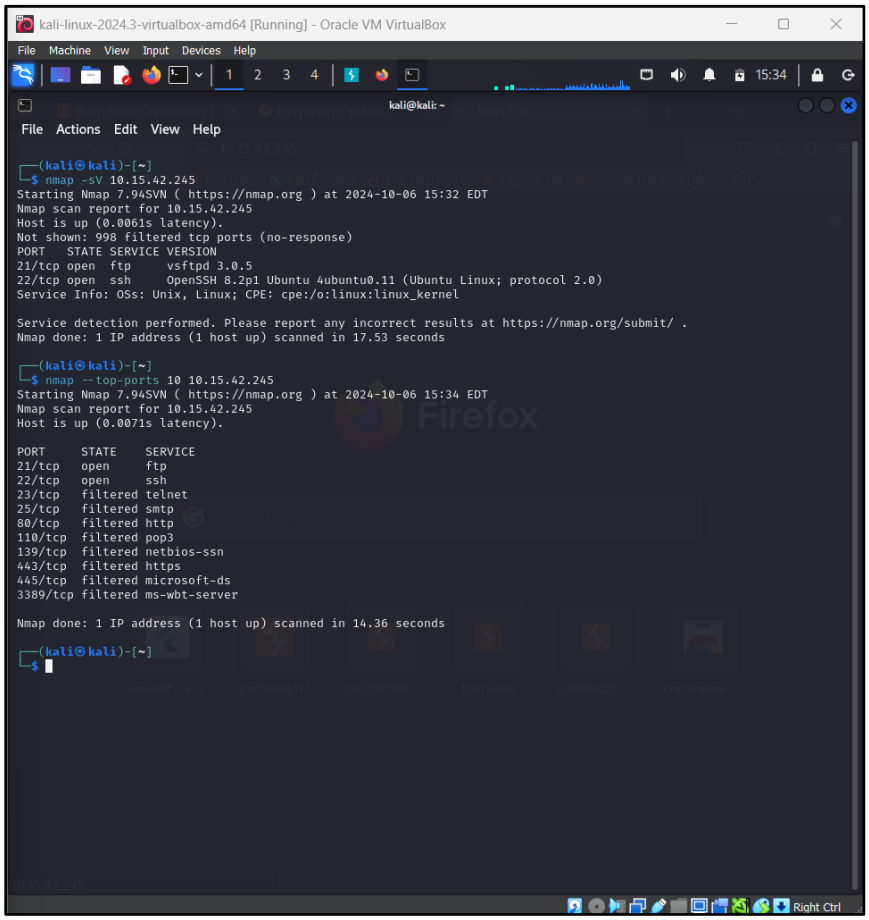


Figure 1: Sample list of breached user credentials

Top Ports Scan

Description:	Option limits scanning to the most common 10 ports, providing a quick overview of the high-traffic ports and services that might be exposed.
System:	nmap --top-ports 10 10.15.42.245

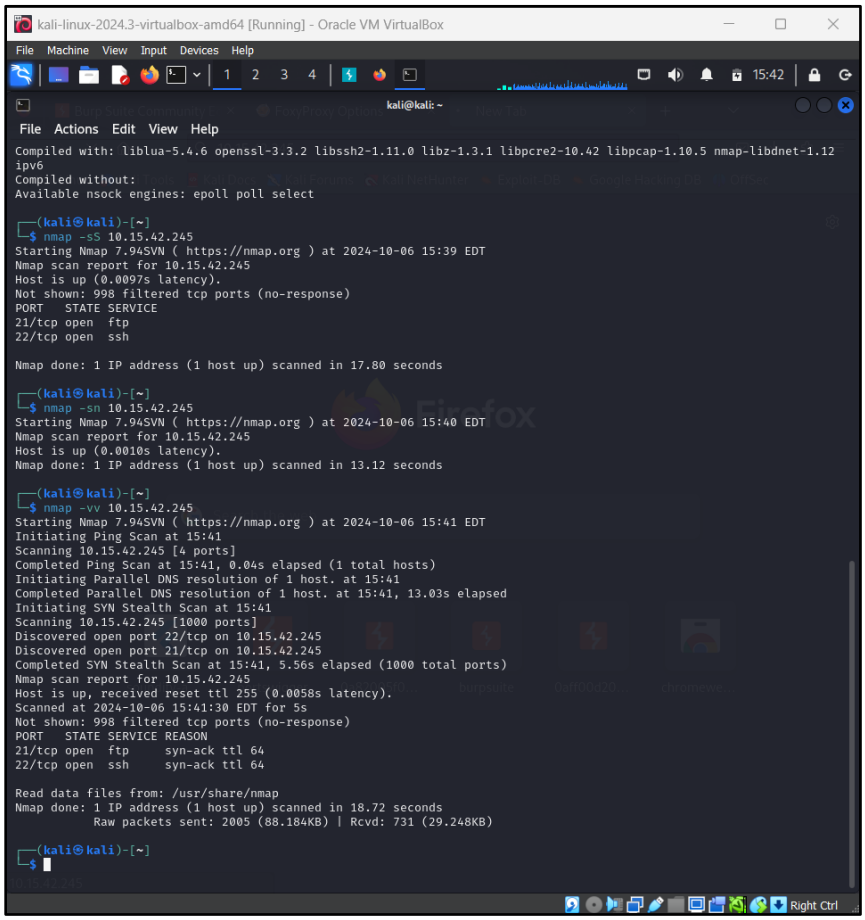


Version Scan with Verbose Output

Description:	The protocol scan identifies IP protocols in use by the target, enabling detection of non-standard protocols that might be active on the system.
System:	nmap -sO 10.15.42.245

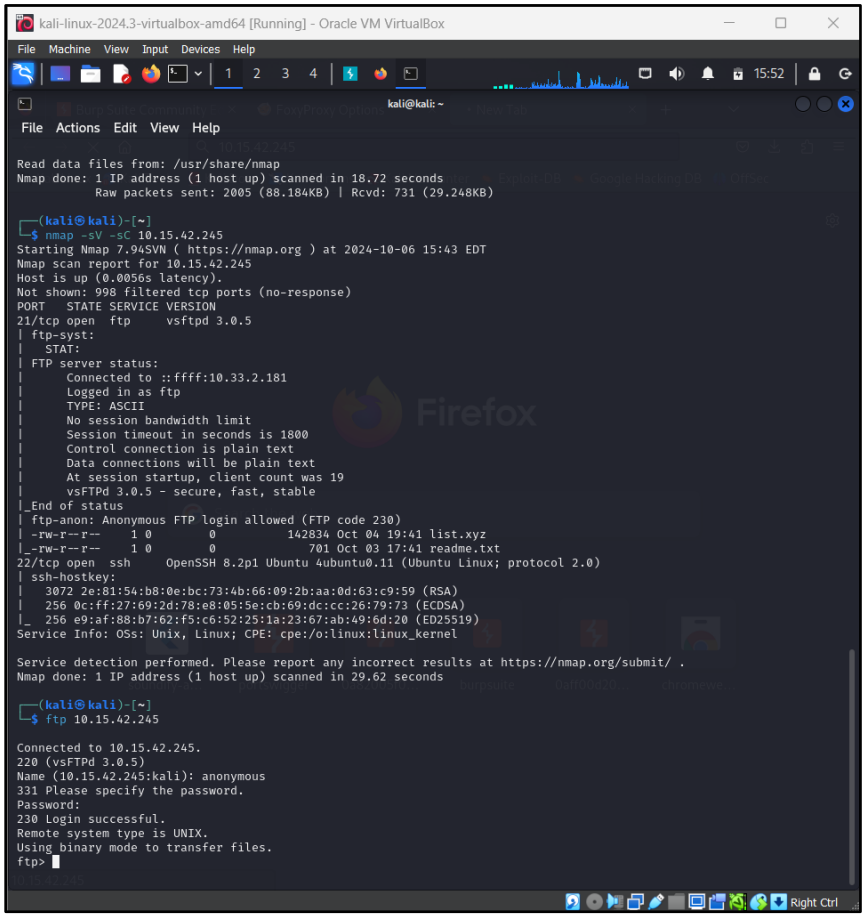
TCP SYN Scan, Double Verbose Scan

Description:	- TCP SYN scan provides a stealthier approach to identifying open ports without fully establishing connections, often bypassing simple firewall detection. - enhances the output, providing detailed live updates and helping with troubleshooting during the scan process.
System:	- nmap -sS 10.15.42.245 - nmap -vv 10.15.42.245



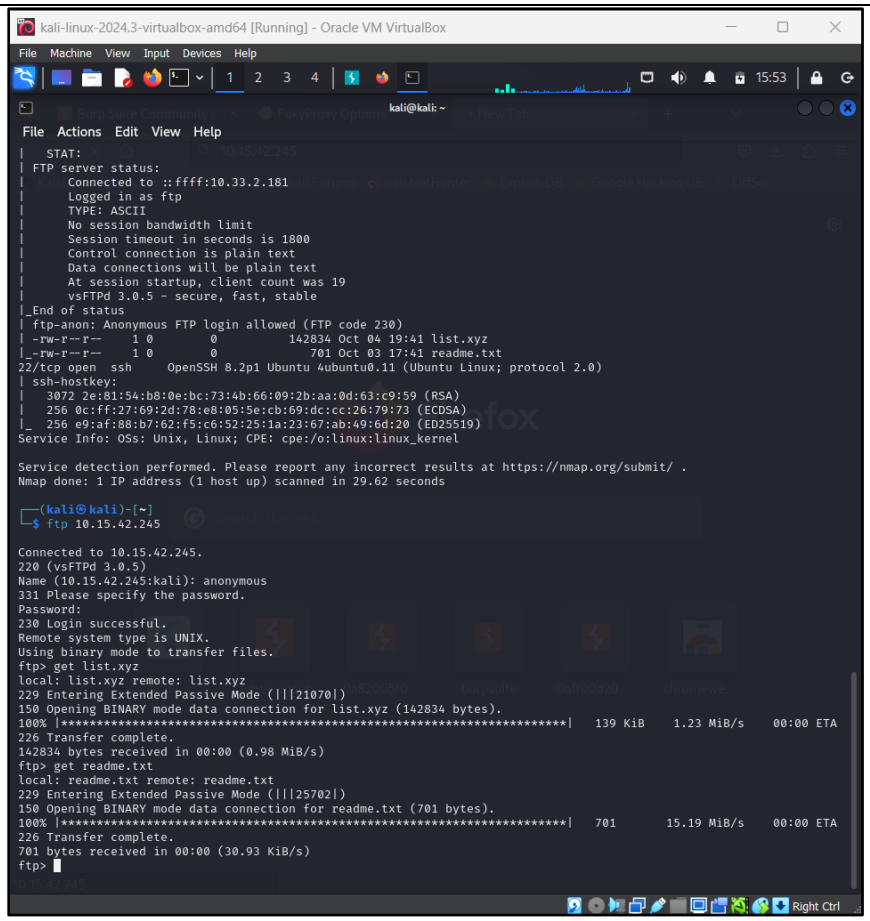
Comprehensive Scan with Default Scripts

Description:	The -sC option with -sV combines service version detection with default NSE (Nmap Scripting Engine) scripts to gather extensive information about the target, including detailed fingerprinting.
System:	nmap -sV -sC 10.15.42.245



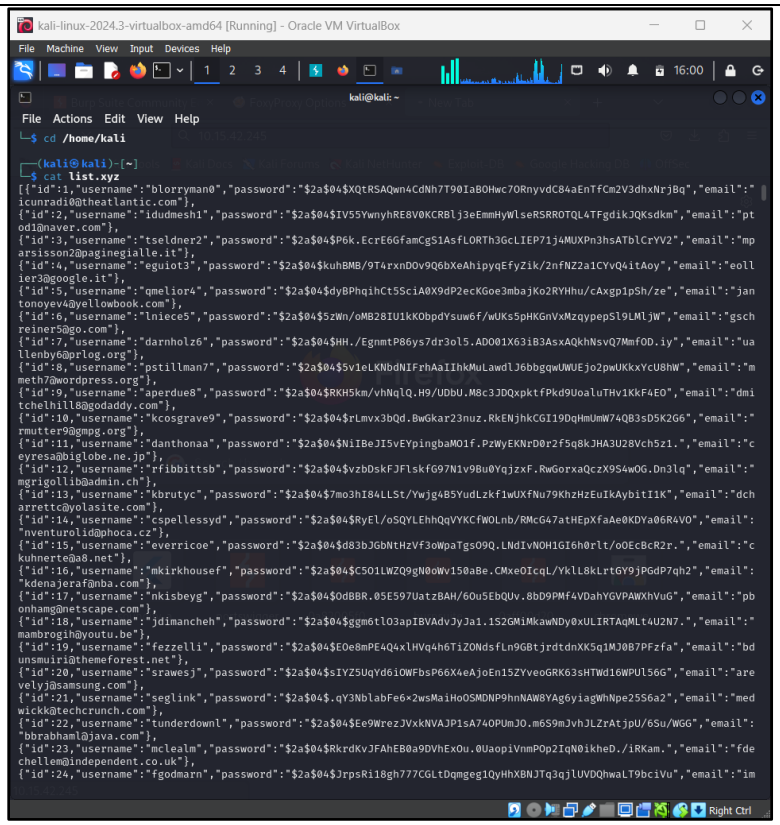
Accessing FTP Service

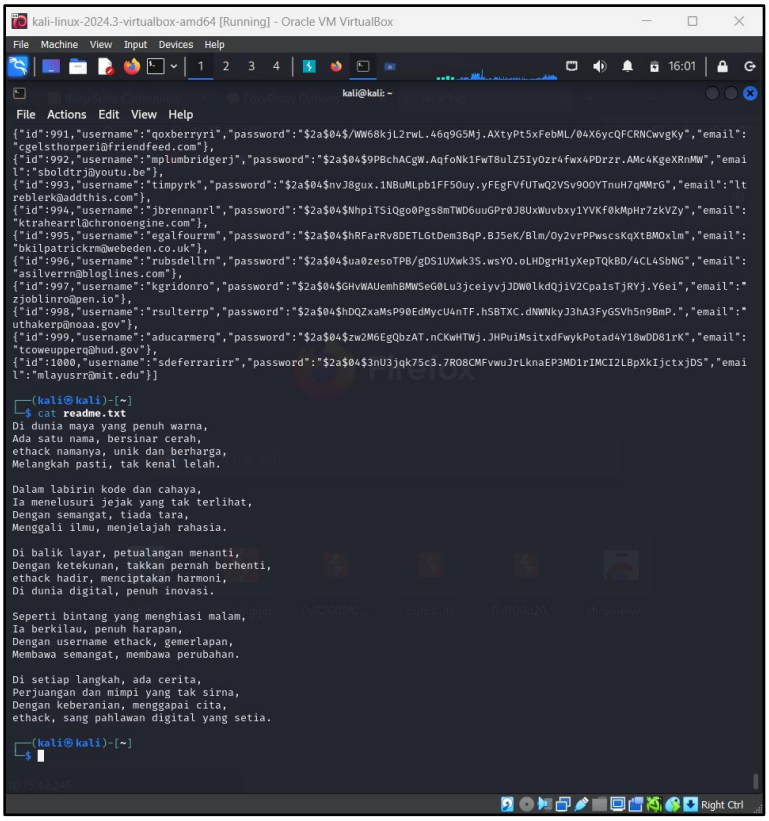
Description:	Using the FTP service with anonymous login, the identified files (list.xyz and readme.txt) are accessed and downloaded for further inspection.
System:	ftp 10.15.42.245

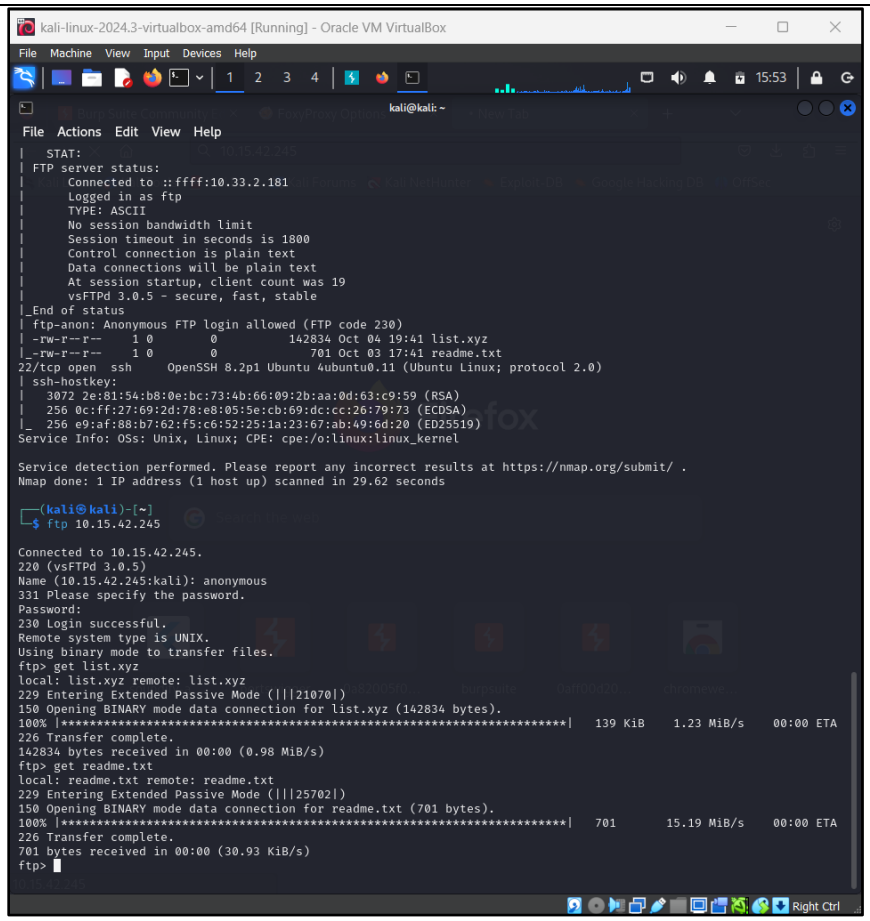


Analyzing list.xyz and readme.txt Files

Description:	The file list.xyz contains user information such as usernames, passwords, and emails. Meanwhile, readme.txt contains a hint or keyword, specifically mentioning the username “ethack” within a pantun.
System:	Cat list.xyz readme.txt







Extracting Information for ethack Username

Description:	The grep command is used to extract information specifically related to the "ethack" username from list.xyz, including a bcrypt password hash.
System:	grep "ethack" list.xyz

Remediation

Who:	IT Team
Vector:	Remote
Action:	Item 1: VPN and OWA login with valid credentials did not require Multi-Factor Authentication (MFA). TCMS recommends DC implement and enforce MFA across all external-facing login services.

Additional Reports and Scans (Informational)

TCMS provides all clients with all report information gathered during testing. This includes vulnerability scans and a detailed findings spreadsheet. For more information, please see the following documents:

- Demo Company-867-19 Full Findings.xslx
- Demo Company-867-19 Vulnerability Scan Summary.xslx
- Demo Company-867-19 Vulnerability Scan by Host.pdf

Last Page