ET NetSec

Penetration Testing Findings Report

Table of Contents

Confidentiality Statement

The information provided by this document is the exclusive property of Contoso, herein known as “the client,” and ET NetSec. This document contains proprietary and confidential information that the client and ET NetSec may share with auditors under non-disclosure agreements in order to demonstrate penetration test compliance.

Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both the client and ET NetSec.

Disclaimer

A penetration test is considered a snapshot in time. Consequently, the findings and/or recommendations reflect the information gathered only during the assessment.

Engagements with the target that are limited by time do now fully allow for a full evaluation of all security controls. ET NetSec prioritized the assessment to identify the weakest security controls an attacker would exploit. As such, ET NetSec recommends conducting similar security assessments on a yearly basis.

Contact Information

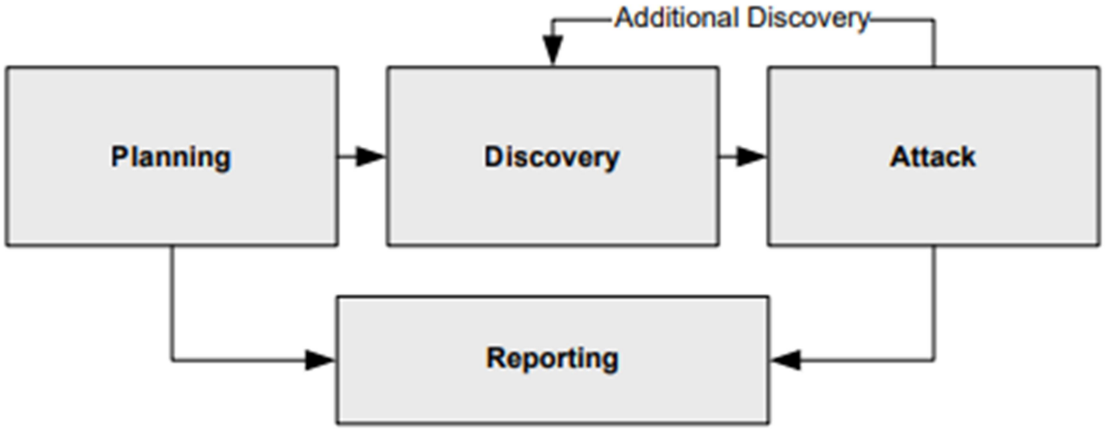
Name	Title	Contact Information
Contoso		
Sean Flynn	VP, Information Technology	Office: (407) 345-8080
ET NetSec		
Emmanuel Tarantino	Director of Security	Office: (305) 302-3443

Assessment Summary

ET NetSec will engage the client in order to evaluate the security of its infrastructure and compare it to industry standard and best practices. All testing performed is based on the National Institute of Standards and Technology (NIST) Technical Guide to Information Security Testing and Assessment, which can be found on NIST's website, https://csrc.nist.gov/publications/detail/sp/800-115/final.

The four pillars of the penetration testing ET NetSec will base its approach are:

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



Assessment Components

External Penetration Testing

The purpose of an external penetration test is to emulate the role of an attacker attempting to gain access to an internal network without resources from inside the network. A security professional from ET NetSec attempts to gather information through open-source intelligence, which can range from employee information, common password practices, and any information that can be leveraged against external systems to gain internet network access. Additionally, ET NetSec will perform network scanning and enumeration in order to identify potential vulnerabilities that may be exploitable.

Severity Ratings

The Common Vulnerability Scoring System (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. ET NetSec will use the following scores throughout the document to assess vulnerability and risk impact.

Severity	CVSS 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

The following IP addresses were included in the scope of the external penetration testing.

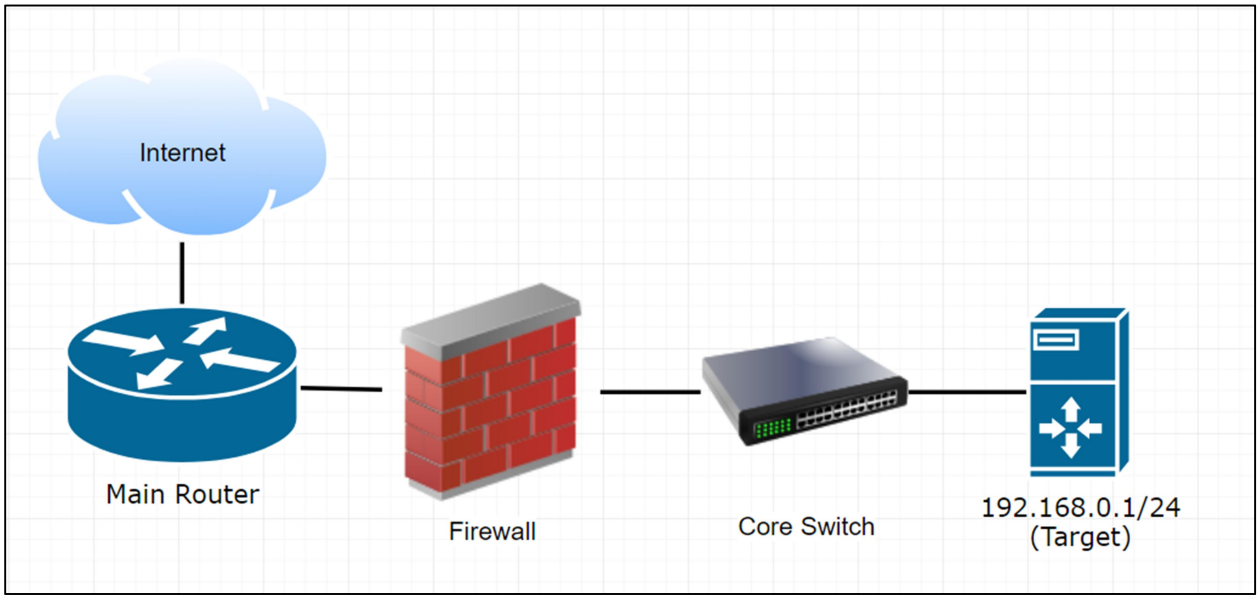
Assessment	IP Range
External Penetration Test	192.168.0.1/24

Scope Exclusions

Per the client's request, ET NetSec did not perform any Denial of Service attacks during testing.

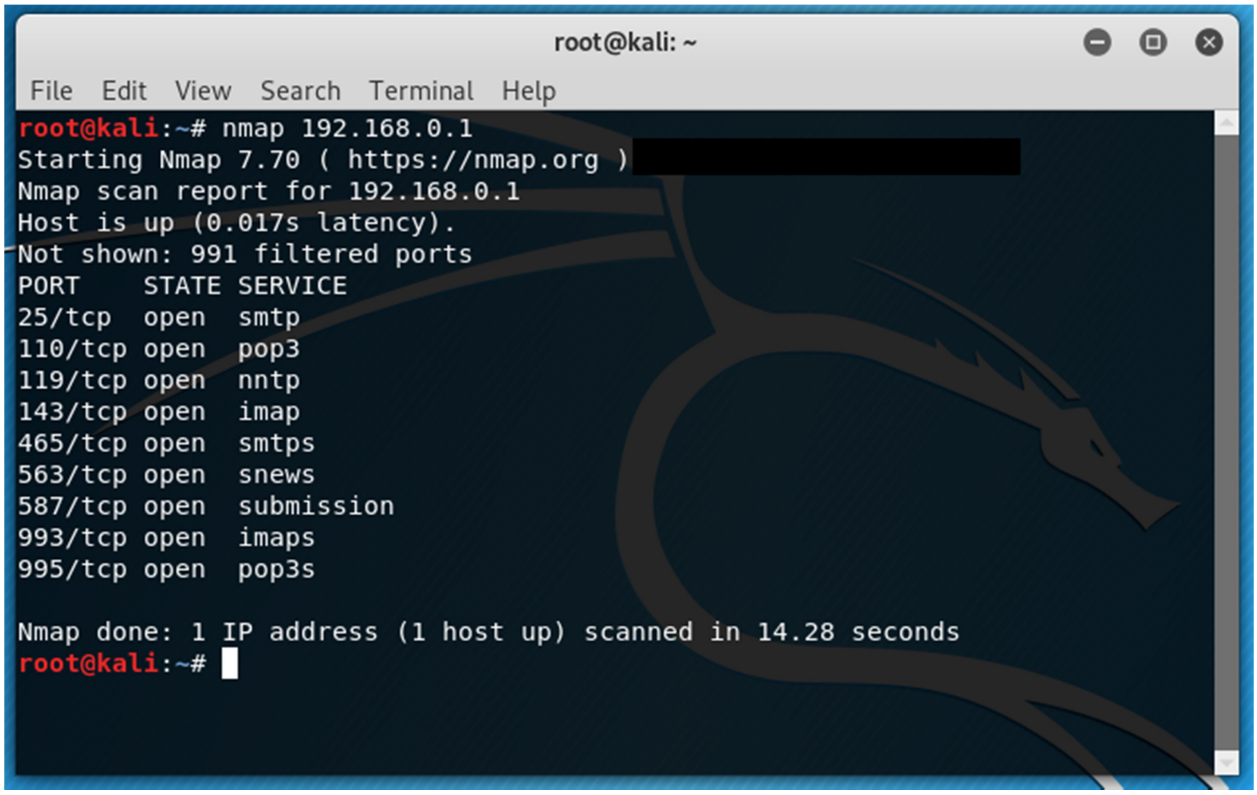
Executive Summary

Network Topology



Port Scanning

ET NetSec engineers used a port scanner to probe the provided host by the client.



Below is list and explanation of all ports open on the scanned machine, detailing the services each port is responsible for.

PORT	SERVICE
25	Simple Mail Transfer Protocol (SMTP), used for email routing between mail servers.
110	Post Office Protocol, version 3 (POP3).
119	Network News Transfer Protocol (NNTP), retrieval of newsgroup messages.
143	Internet Message Access Protocol (IMAP), management of electronic mail messages on a server.
465	URL Rendezvous Directory for SSM (Cisco protocol). Authenticated Simple Mail Transfer Protocol (SMTP) over Transport Layer Security/Secure Sockets Layer (TLS/SSL) (SMTPS).
563	The Network News Transfer Protocol (NNTP) over Transport Layer Security/Secure Sockets Layer (TLS/SSL) (NNTPS).
587	Email message submission (SMTP).
993	Internet Message Access Protocol over TLS/SSL (IMAPS).
995	Post Office Protocol 3 over TLS/SSL (POP3S).

Security Strengths

Strong User Password Policy

ET NetSec was unsuccessful in a password guessing attack against the client using predictable password formats, such as “Spring2020!” (season + year + special character) or commonly used passwords, such as “Password123!”.

Security Weaknesses

Open Ports

ET NetSec was able to perform a scan of open ports on the client’s system. The open ports can be used as attack vectors. It is recommended to close all unused ports.

Multi-Factor Authentication

Although the password guessing attack was unsuccessful due to strong password policy, ET NetSec strongly encourages incorporating a multi-factor authentication. By using multi-factor authentication, an attacker would not be able to leverage otherwise acquired information to gain internal network access.

Unrestricted Logon Attempts

During the assessment, ET NetSec was allowed to brute-force password guessing attacks. Although unsuccessful, it is strongly recommended to incorporate a lockout period when a user tries to login unsuccessfully after a number of attempts. For all logins, unlimited attempts were allowed, which may eventually allow an attacker to login.

Remediation

Who:	IT Team/CEO
Vector:	Remote
Action:	Item 1: The system contains a large number of open ports. These ports could be used to leverage vulnerabilities by an attacker. ET NetSec recommends closing all unused ports. Item 2: The client does not require Multi-Factor Authentication. ET NetSec recommends implementing Multi-Factor Authentication on all devices, or at the very least external-facing devices. Item 3: The system permitted unlimited login attempts. ET NetSec recommends restricting logon attempts before the account is locked out for a period of time. At which point the IT Team can unlock after verifying with the user, or the account will unlock on its own after the allowed time has elapsed. Additionally, ET NetSec recommends that the client: ▪ Train employees on how to create a proper password. ▪ Check employee credentials against known breached passwords. ▪ Discourage employees from using work e-mails and usernames as login credentials to other services unless absolutely necessary. ▪ Stay up to date on all security updates and system patching.

ET NetSec

Penetration Testing Findings Report

End of Report