SmartInternz Long Term Internship

Team Leader: Potnuru Ramya , Sri Sivani college of engineering

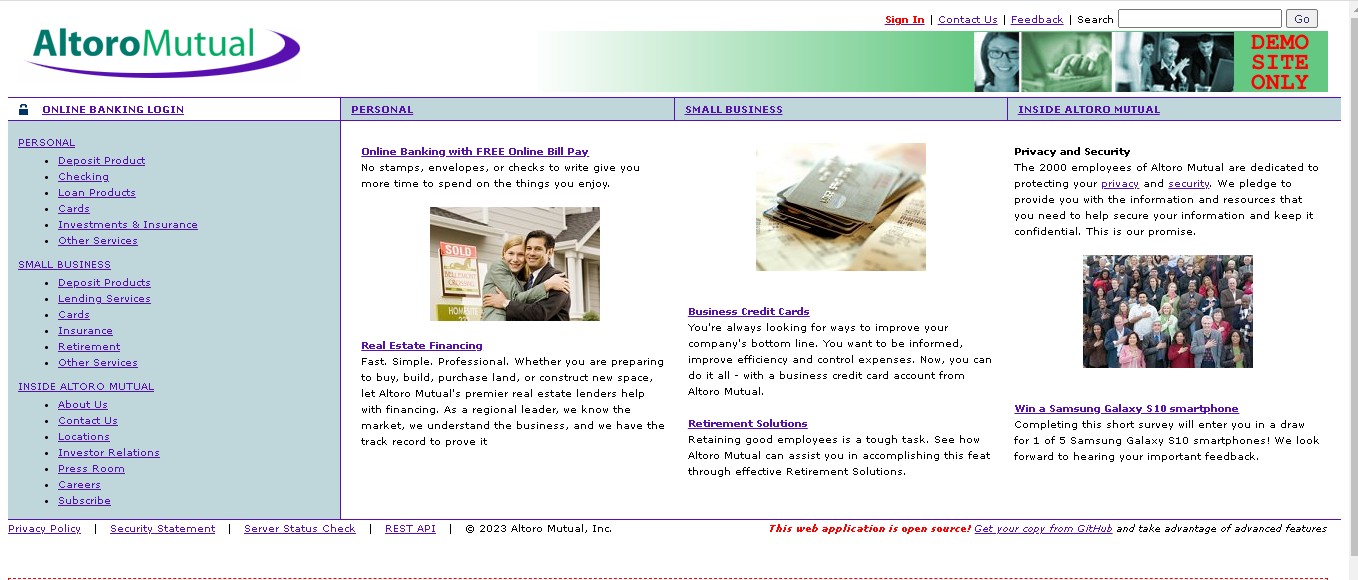
Team member:Bejjipurapu Mounika, Sri Sivani college of engineering

Team member:Dasu Sivasankaravaraprasad,Sri Sivani college of engineering

Team member:Jami Sai,Sri Sivani college of engineering Team member:Bouri Naveen, Sri Sivani college of engineering

**Malware Analysis and ngReverse Eineering**

AltoroMutual



Executive Summary

Executive summary of malware analysis and reverse engineering:

Malware analysis and reverse engineering are critical processes for understanding and countering malicious software threats. Malware analysis involves dissecting malware to uncover its functionality, behavior, and potential impact on systems. Reverse engineering is the process of deconstructing code to understand its inner workings.

These practices help cybersecurity experts identify vulnerabilities, create detection mechanisms, and develop effective countermeasures against evolving cyber threats. Successful malware analysis and reverse engineering contribute to safeguarding digital systems, data, and user privacy. Enhancing the overall security systems and networks.

Malware analysis and reverse engineering are critical processes for understanding and countering malicious software threats. Malware analysis involves dissecting malware to uncover its functionality, behavior, and potential impact on systems. Reverse engineering is the process of deconstructing code to understand its inner workings.

These practices help cybersecurity experts identify vulnerabilities, create detection mechanisms, and develop effective countermeasures against evolving cyber threats. Successful malware analysis and reverse engineering contribute to safeguarding digital systems, data, and user privacy.It refers to the practice of protecting computer systems, networks, and data from cyber threats, such as hacking, unauthorized access, data breaches, and other malicious activities. It involves a range of techniques and measures to safeguard digital assets and ensure the confidentiality, integrity, and availability of information in the digital world.

Overview

Malware analysis involves dissecting malicious software to understand its behavior, purpose, and potential impact. Reverse engineering is a key component of this process, aiming to decipher the code and logic of a program to reveal its innerworkings.

The primary objectives of the malware are as follows:

1. **Identify Vulnerabilities: The assessment aims to identify potential vulnerabilities in the**

network infrastructure, including unpatched software, misconfigurations, and open ports.

1. **Evaluate Security Controls: The effectiveness of existing security controls, such asfirewalls, intrusion detection systems (IDS), and access controls, is assessed to determinetheir ability to detect and prevent attacks.**
2. **Assess Network Architecture: The network architecture is reviewed to ensure propersegmentation, isolation of critical assets, and a robust perimeter defense.**
3. **Password Policy Evaluation: The assessment examines the strength of passwordpolicies and their adherence to industry best practices to prevent unauthorized access.**
4. **Physical Security Analysis: Physical security measures in place to protect networkinfrastructure and data centers are evaluated to prevent unauthorized physical access.**

Methodology:

The assessment follows a well-defined methodology, including the following steps

1. **Reconnaissance: Passive reconnaissance techniques are used to gather informationabout the network and its assets.**
2. **Vulnerability Scanning: Automated scanning tools are employed to identify potentialvulnerabilities in the network.**
3. **Manual Verification: The identified vulnerabilities are manually verified to eliminatefalse positives and prioritize critical issues.**
4. **Exploitation (with Authorization): Ethical exploitation of vulnerabilities is conducted todetermine the extent of potential damage if exploited maliciously.**
5. **Analysis and Reporting: The assessment findings are analyzed, and a detailed report isgenerated, including a list of vulnerabilities, risk severity, and actionable recommendations.**

Deliverables:

The assessment will provide the following deliverables:

1. **Network Vulnerability Assessment Report: A comprehensive report detailing theassessment methodology, findings, risk analysis, and actionable recommendations.**
2. **Executive Summary: A concise summary highlighting key findings and criticalvulnerabilities for executive stakeholders.**
3. **Remediation Plan: A roadmap outlining the prioritized actionsrequired to addressidentified vulnerabilities and improve network security.**

Information gathering:

Information gathering is a crucial phase in the cybersecurity and assessment process. Itinvolves collecting relevant data and intelligence about a target system, network, ororganization to understand its vulnerabilities and potential attack surfaces. Here aredifferent aspects of information gathering:

1. **Email Footprint Analysis:**

Email footprint analysis involves collecting information related to an organization's emailinfrastructure, such as email addresses, email servers, and email security measures. Thisanalysis helps in understanding how email communications are handled and identifyingpotential points of entry for attackers.

1. **DNS Information Gathering:**

DNS (Domain Name System) information gathering involves querying and analyzing DNSrecords to gather details about domain names, IP addresses, mail exchange servers, andother crucial information. It helps in understanding the network structure and identifyingpotential targets for cyberattacks.

1. **WHOIS Information Gathering:**

WHOIS information gathering involves querying the WHOIS database to retrieveregistration details of domain names and IP addresses.

This data includes contactinformation of domain owners and registrars, which can be valuable for understanding theownership and potential affiliations of a target domain.

1. **Information Gathering for Social Engineering Attacks:**

Social engineering attacks involve manipulating individuals into divulging sensitiveinformation or performing specific actions.

Information gathering for social engineering attacks includes researching potential targets' online presence, interests, and connectionsto craft convincing and personalized attack scenarios.

1. **Information Gathering for Physical Security Assessments:**

Physical security assessments involve gathering information about the physical premises,access controls, security measures, and personnel protocols of an organization. Thisassessment helps identify potential physical vulnerabilities and weaknesses in anorganization's security.

1. **Emerging Trends and Technologies in Information Gathering:**

As technology evolves, so do the methods of information gathering. Emerging trendsinclude the use of artificial intelligence and machine learning algorithms for autom data collection and analysis, advanced OSINT (Open-Source Intelligence) tools, and socialmedia analysis for gathering valuable intelligence.The result of the information gathering performed on Altoro Mutual (ip: 65.61.131.117)

domain name : testfire.net Email Footprint Analysis:

Tool used : the Harvester

The Harvester is a powerful open-source tool used for information gathering andreconnaissance in the field of cybersecurity. It is designed to gather data from varioussources, such as search engines, public databases, and social media platforms, to extractvaluable information about a target organization or individual. The tool primarily focuseson harvesting email addresses, subdomains, hostnames, and other related informationthat can be used for further analysis or exploitation.

Command used : theHarvester -d testfire.net -b allated Output:[\*] IPs found: 3

------------------- 65.61.137.117

[\*] No emails found. [\*] Hosts found: 41

---------------------

altoro.testfire.net:65.61.137.117 demo-analytics.testfire.net demo.testfire.net:65.61.137.117 demo2.testfire.net:65.61.137.117 evil.testfire.net:65.61.137.117 ftp.testfire.net:65.61.137.117 ftp.testfire.net:testfire.net

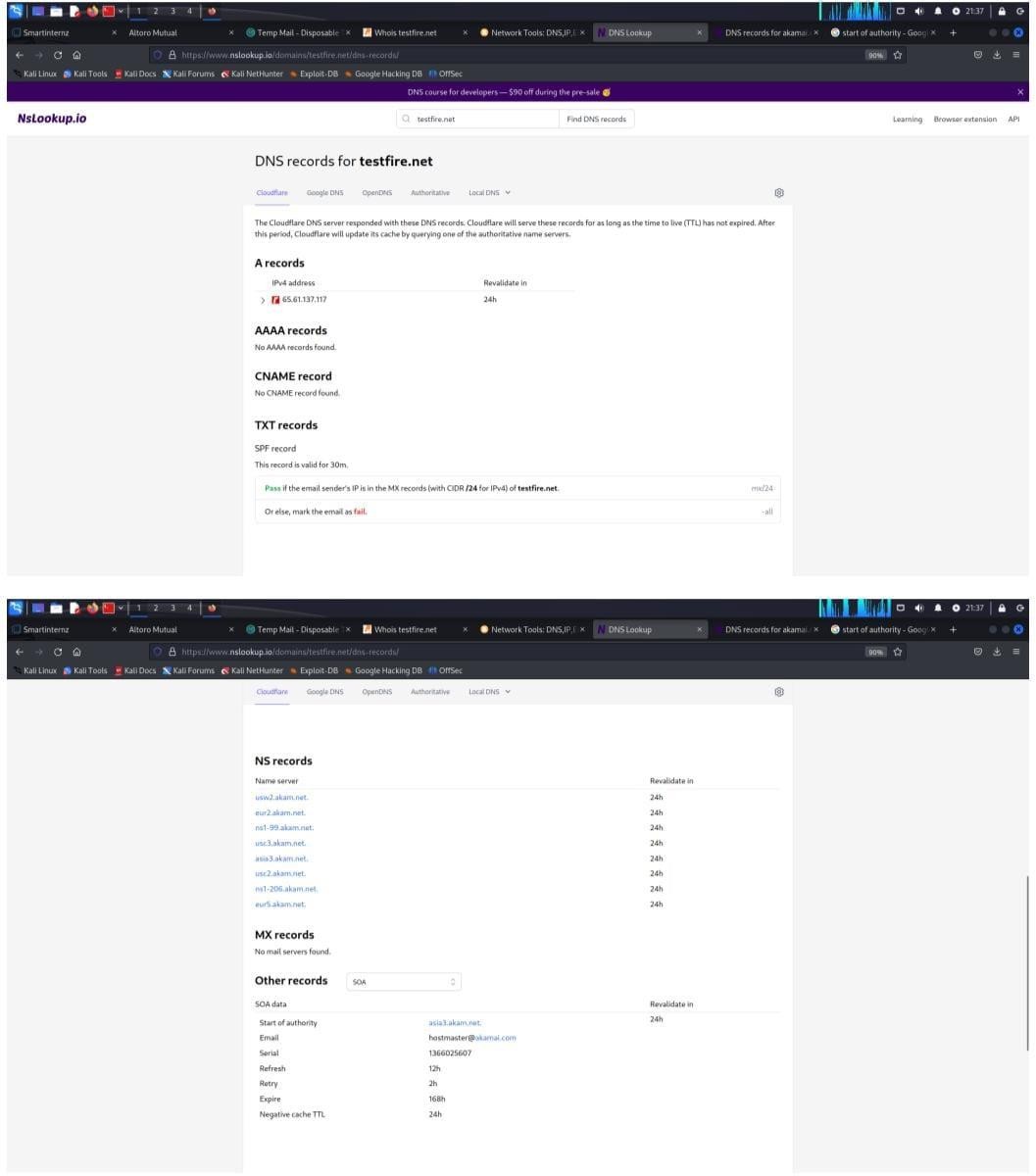
http---demo.testfire.net localhost.testfire.net:65.61.137.117 owtf.pydemo.testfire.net srchttpdemo.testfire.net [www.demo.testfire.net](http://www.demo.testfire.net/) www.testfire.net:testfire.net

www.testfire.net:testfire.net. www.testfire.net:65.61.137.117

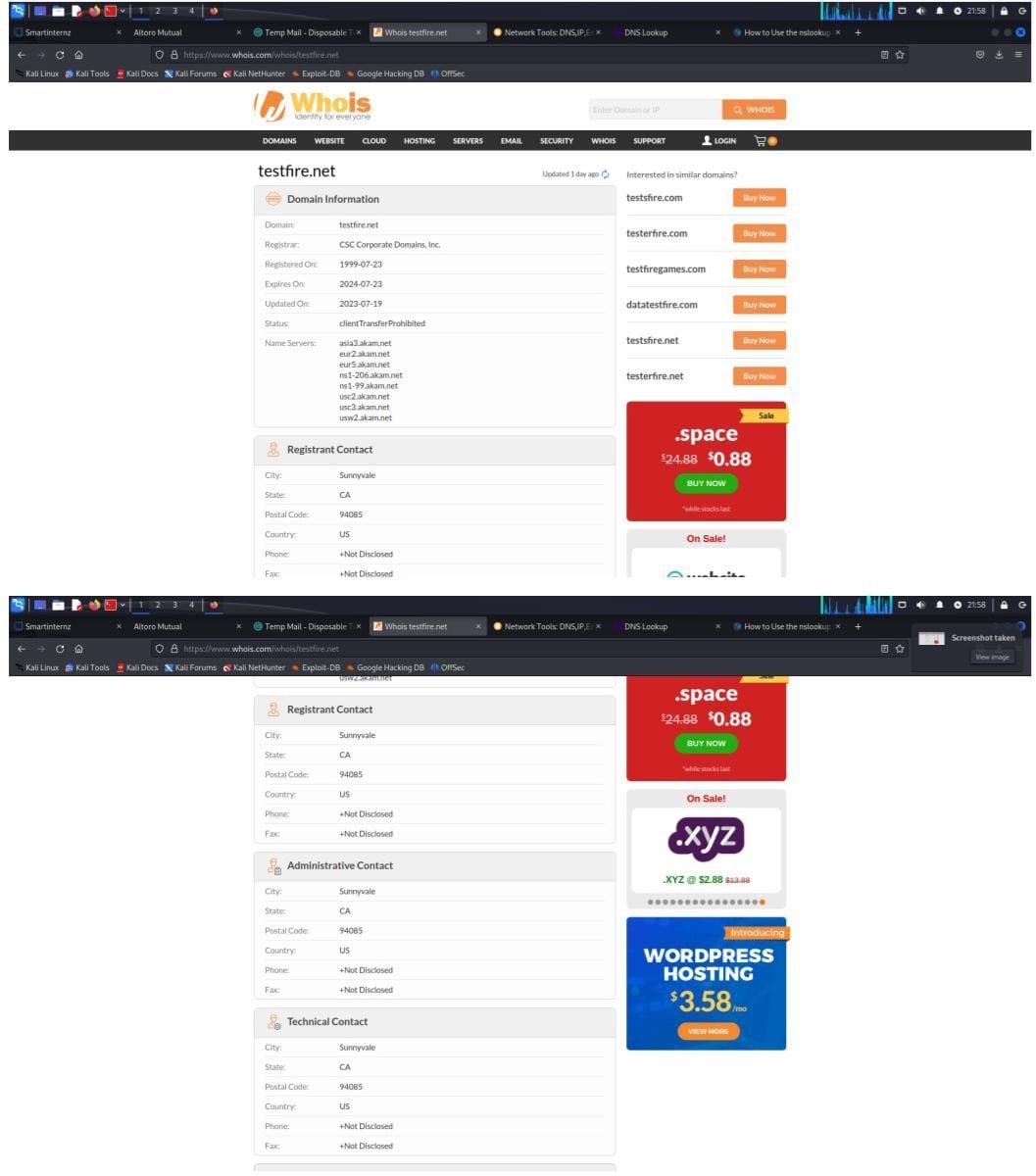
Result : No email found in Altoro Mutual

DNS INFORMATION GATHERING

Website link of Altoro Mutual Dns resulthttps[://ww](http://www.nslookup.io/domains/testfire.net/dns-records/)w[.ns](http://www.nslookup.io/domains/testfire.net/dns-records/)lo[okup.io/domains/testfire.net/dns-records/](http://www.nslookup.io/domains/testfire.net/dns-records/)



WHOIS INFORMATION GATHERING

Website of whois ip result link of Altoro Mutualhttps:[//w](http://www.whois.com/whois/testfire.net)ww[.whois.com/whois/testfire.net](http://www.whois.com/whois/testfire.net)

Vulnerability identification

Vulnerability paths and parameters refer to the specific routes and inputs that attackers can exploit to take advantage of vulnerabilities in software or systems. These paths and parameters vary depending on the nature of the vulnerability. Here are some common types:

1. **Injection Vulnerabilities: - SQL Injection\*: Attackers manipulate SQL queries by injecting malicious code through user inputs, exploiting poorly sanitized input fields.**

* **\*Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages viewed by other users, usually via input fields or URLs.**
* **Command Injection: Attackers execute arbitrary commands by injecting malicious commands into system commands.**

- XML External Entity (XXE): Attackers exploit XML parsing vulnerabilities by injecting malicious entities into XML input.

1. **Authentication and Session Management: - Session Fixation:Attackers set a user's session ID to a known value, effectively hijacking their session.**

Password Reset Token Leakage: Attackers exploit flaws that expose password reset tokens, allowing them to reset others' passwords.

1. **Insecure Direct Object References (IDOR): - Attackers access resources they shouldn't have access to by manipulating parameters (e.g., changing an ID in the URL).**
2. **Security Misconfigurations: - Attackers exploit improperly configured systems, services, or permissions to gain unauthorized access.**
3. **Cross-Site Request Forgery (CSRF): - Attackers trick users into performing unwanted actions on authenticated websites, exploiting the trust between the user and the website.**
4. **Sensitive Data Exposure: - Attackers exploit vulnerabilities that expose sensitive information, like passwords, credit card details, or personal data.**

Attackers manipulate users into disclosing sensitive information, often through deceptive emails or messages.These are just some examples of the types of vulnerability paths and parameters that attackers can exploit. Understanding these vulnerabilities helps in implementing proper security measures to prevent or mitigate potential attacks.

Vulnerabilities:Protocol Detection Synopsis

The remote service encrypts traffic using an older version of TLS. Description

The remote service accepts connections encrypted using TLS 1.0. TLS

1.0 has a number ofcryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newerversions of TLS like1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer functionproperly with major web browsers and major vendors.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POIterminals (and the SSL/TLS termination points to which they connect) that can be verified as notbeing susceptible to any known exploits.

See Also

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00 Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. Risk Factor Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N) CVSS v2.0 Base Score

6.1 (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N) References

XREF CWE:327

Plugin Information

Published: 2017/11/22, Modified: 2023/04/19 Plugin

Output

TLSvL is enabledand the server support at least one cipher

Additional DNS Hostnames Synopsis

Nessus has detected potential virtual hosts. Description

Hostnames different from the current hostname have been collected by miscellaneous plugins.Nessus has generated a list of hostnames that point to the remote host. Note that these are onlythe alternate hostnames for vhosts discovered on a web server.

Different web servers may be hosted on name-based virtual hosts.

See Also https://en.wikipedia.org/wiki/Virtual\_hosting Solution

If you want to test them, re-scan using the special vhost syntax, such as :

[www.example.com](http://www.example.com/)[192.0.32.10] Risk Factor None

Plugin Information

Published: 2010/04/29, Modified: 2022/08/15 Plugin Output tcp/0

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common PlatformEnumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible

CPE based on the information available from the scan.

See Also <http://cpe.mitre.org/>

https://nvd.nist.gov/products/cpe Solution n/a

Risk Factor None Plugin Information

Published: 2010/04/21, Modified: 2023/07/27 Plugin Output tcp/0

Business Impact

Additional DNS Hostnames Synopsis:The Nessus vulnerability scan has detected potential virtual hosts with different hostnames pointing to the remote host

Impact:1. Resource Allocation

1. **Security Implications**
2. **Website Reputation and Trust**
3. **Search Engine Optimization (SEO) Recommended Actions:**
4. **Review Virtual Host Configuration**
5. **Monitor Resource Usage**
6. **Implement Security Measures**
7. **Monitor Website Reputation**
8. **Address SEO Concerns**

Common Platform Enumeration (CPE) Synopsis:The Nessus scan has enumerated Common Platform Enumeration (CPE) names that match the remotesystem.

Impact:

1. **Vulnerability Identification and Management**
2. **Asset Inventory and Visibility**
3. **Regulatory Compliance**

Common Platform Enumeration (CPE)

Synopsis:The Nessus scan has enumerated Common Platform Enumeration(CPE) names that match the remotesystem.

Impact:

1. **Vulnerability Identification and Management**
2. **Asset Inventory and Visibility**
3. **Regulatory Compliance**
4. **Vendor Support and Updates**
5. **Risk Assessment and Mitigation**

Recommended Actions:1. Regular Scanning and Enumeration

1. **Patch Management**
2. **Vulnerability Monitoring**
3. **Asset Inventory and Lifecycle Management**
4. **Compliance Reporting**

SSL Cipher Block Chaining Cipher Suites Supported Synopsis:

The plugin identifies that the remote service supports the use of SSL Cipher Block Chaining (CBC)ciphers. CBC mode is a cryptographic technique.

Impact:

1. **Data Confidentiality**
2. **Vulnerability to Padding Oracle Attacks**
3. **Compliance and Security Standards**
4. **Mitigation Strategies Recommended Actions:**
5. **SSL/TLS Configuration Review**
6. **Regular Software Updates**
7. **Vulnerability Assessments**
8. **Monitoring and Logging**

Nessus SYN scanner Synopsis:The Nessus SYN scanner is capable of determining which TCP ports are open on a target system.

Impact:

1. **Network Visibility**
2. **Vulnerability Identification**
3. **Firewall Resilience Assessment**
4. **Network Load and Performance Recommended Actions:**
5. **Responsible Scanning**
6. **Firewall Hardening**
7. **Vulnerability Remediation**
8. **Monitoring and Incident Response OS Identification Synopsis:**

The plugin performs OS identification using various remote probes, such as TCP/IP, SMB, HTTP,NTP, SNMP, etc.

Impact:

1. **System Profiling**
2. **Vulnerability Assessment**
3. **Security Posture Evaluation**
4. **Network Hardening**
5. **Compliance and Regulatory Requirements: Recommended Actions:**
6. **Asset Inventory and Documentation**
7. **Patch Management**
8. **Security Control Customization**
9. **Network Segmentation Device Type Synopsis:**

The Nessus scan has identified the remote device type based on the remote operating system.

Impact:

1. **Device Profiling**
2. **Security Policy Implementation**
3. **Network Visibility**
4. **Incident Response**
5. **Change Management and Patching Recommended Actions:**
6. **Accurate Device Identification**
7. **Network Segmentation**
8. **Security Policy Tuning**
9. **Incident Response Planning**

RANSOMWARE it is a malicious software or computer virus, upon triggering which will encrypt the files and data in the disk and asks for ransom(money) in exchange to decrypt the data.

HOW SIMPLE RANSOMWARE MADE WITH PYTHON:

First a private public key pair is generated using libraries which supports algorithm rsa Then generated public key and private key is encoded with base64 so that reverse engineers and malware analysist can’t easily find the keys. Then a recursive function will scan the directories and files and encrypt those data with public key and delete those original files Based on malware author this malware can have GUI with countdown and other graphic interface with payment gateway embedded can be included.

Detailed instruction for vulnerability:

Vulnerabilities are weaknesses or flaws in software, systems, or processes that could be exploited by attackers to compromise security. They can range from coding errors to misconfigurations, and understanding them is crucial for effective cybersecurity. Defining vulnerabilities involves identifying specific weaknesses and assessing their potential impact on the system's integrity, confidentiality, or availability. Regular vulnerability assessments and penetration testing help organizations identify and address these vulnerabilities to mitigate potential risks.

Identifying vulnerabilities involves searching for weaknesses in software, systems, or processes that could be exploited by attackers. These can be categorized into different types, such as:

1. **Software Vulnerabilities: These include flaws in code, like buffer overflows, SQL injection, and cross-site scripting (XSS).**
2. **Configuration Vulnerabilities: Result from incorrect settings or configurations, like leaving default passwords or open ports.**
3. **Design Vulnerabilities: Arise from poor system or application design, making it easier for attackers to exploit.**
4. **Human Vulnerabilities: Stem from social engineering or human error, like sharing passwords or falling for phishing attacks.**
5. **Physical Vulnerabilities: Relate to the physical environment, such as lack of physical security or unprotected hardware.**
6. **Policy and Process Vulnerabilities: Result from inadequate security policies or processes within an organization.**
7. **Zero-Day Vulnerabilities: Previously unknown vulnerabilities that attackers can exploit before they are patched.**
8. **Network Vulnerabilities: Arise from weaknesses in network infrastructure, like insecure protocols or weak encryption.**

Naming vulnerabilities often involves giving them a specific identifier, commonly referred to as a "CVE" (Common Vulnerabilities and Exposures) number. This unique identifier helps security professionals and researchers refer to vulnerabilities consistently across different platforms and discussions. For instance, the identifier "CVE-2023-12345" would be associated with a particular vulnerability.

Import base64 import os from Crypto.PublicKey import RSA

from Crypto.Cipher import PKCS1\_OAEP, AES '''

with open('public.pem', 'rb') as f: public = f.read() print(base64.b64encode(public))

'''

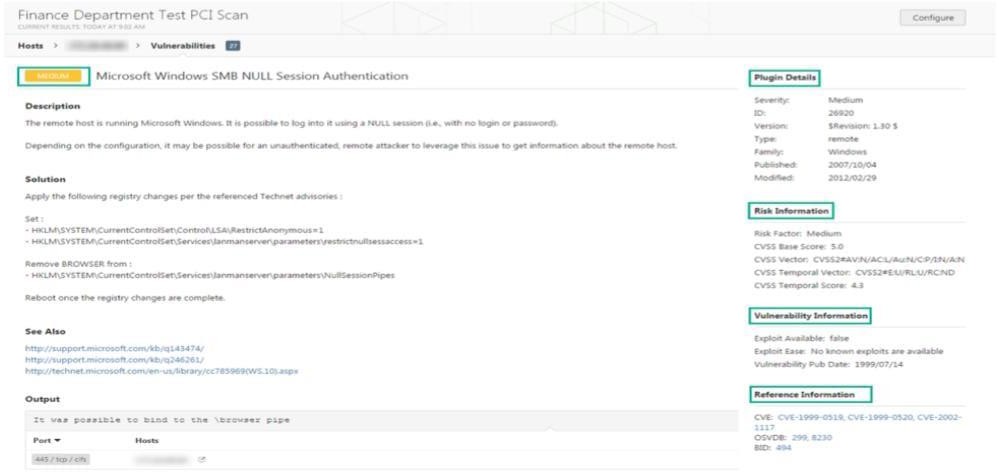
To view vulnerabilities:

1. **In the top navigation bar, click Scans.**
2. **Click the scan for which you want to view results.**
3. **Do one of the following:**

* **Click a specific host to view vulnerabilities found on that host.**
* **Click the Vulnerabilities tab to view all vulnerabilities.**

1. **(Optional) To sort the vulnerabilities, click an attribute in the table header row to sort by thatattribute.**
2. **Clicking on the vulnerability row will open the vulnerability details page, displaying plugin**

information and output for each instance on a host.



Reporting Your Results

Chances are your job isn’t done yet. You need to report your findings to your team.

Scan results can be exported in several file formats. Some of these report formats arecustomizable, while others are designed to be imported into another application or product, suchas Microsoft Excel or Tenable.sc. For an explanation of the various report formats and the purpose of each, see the Nessus User Guide. Comprehensive and detailed reporting is crucial for several reasons:

1. **Informed Decision-Making: Detailed reports provide a thorough understanding of data, enabling informed decisions based on accurate insights.**
2. **Transparency: Comprehensive reporting promotes transparency by showcasing the full scope of information, which builds trust with stakeholders.**
3. **Problem Identification: Detailed reports help identify trends, outliers, and issues, allowing for timely corrective actions.**
4. **Performance Evaluation: Comprehensive reporting allows for an accurate assessment of performance, helping organizations gauge success and areas for improvement.**
5. **Communication: Detailed reports facilitate effective communication among teams, departments, and pa…**

To Export a Scan Report:

1. **Start from a scan's results page**
2. **In the upper-right corner, click Export.**
3. **From the drop-down box, select the format in which you want to export the scan results.**
4. **Click Export to download the report.**

Recommendations:

Based on the assessment results, the following recommendations are suggested to improve the security of the "altoroMutual" system:

1. **Disable TLS version 1.0 and enable support for TLS 1.2 and 1.3 to enhance encryption securityand comply with industry standards.**
2. **Investigate and verify the additional DNS hostnames to ensure that they are legitimate and donot pose security risks.**
3. **Monitor the open TCP ports identified by the Nessus SYN scanner to prevent any potentialsecurity issues or unauthorized access.**
4. **Review and understand the CPE information to identify any potential vulnerabilities associatedwith hardware and software products on the host.**
5. **Address SSL/TLS-related vulnerabilities, such as replacing certificates signed with weakhashing algorithms, verifying root Certification Authority certificates, and enabling recommended cipher suites.**
6. **Regularly update and patch the system to address any known vulnerabilities and improveoverall security.**
7. **Implement proper network security controls, including firewalls and intrusiondetection/prevention systems, to protect against potential threats.**

It is essential to address these vulnerabilities promptly to enhance the security posture of the"altoroMutual" system and safeguard sensitive data and communications. Regular vulnerabilityassessments and security best practices should be followed to ensure ongoing protectionagainst potential threats.