**SmartInternLongTermVirtualInternship**

## An Internship Report Submitted In Partial Fulfillment of The Requirements for the Award of Degree of

**BACHELOR OF TECHNOLOGY**

## In

**MECH – MECHANICAL ENGINEERING**

**Submittedby:**

**BIDDIKA PALGUNA RAO 20W61A0304**

**SIRIPURAM BHUJANGA RAO 20W61A0327**

**VIBUDHI VAMSI 20W61A0331**

**THOTA AVINASH 21W65A0322**



**Department of Mechanical Engineering**

**SRI SIVANI COLLEGE OF ENGINEERING**

**Approved By AICTE & Affiliated to JNTUGV**

**Chilakapalem Jn., Srikakulam 532402**

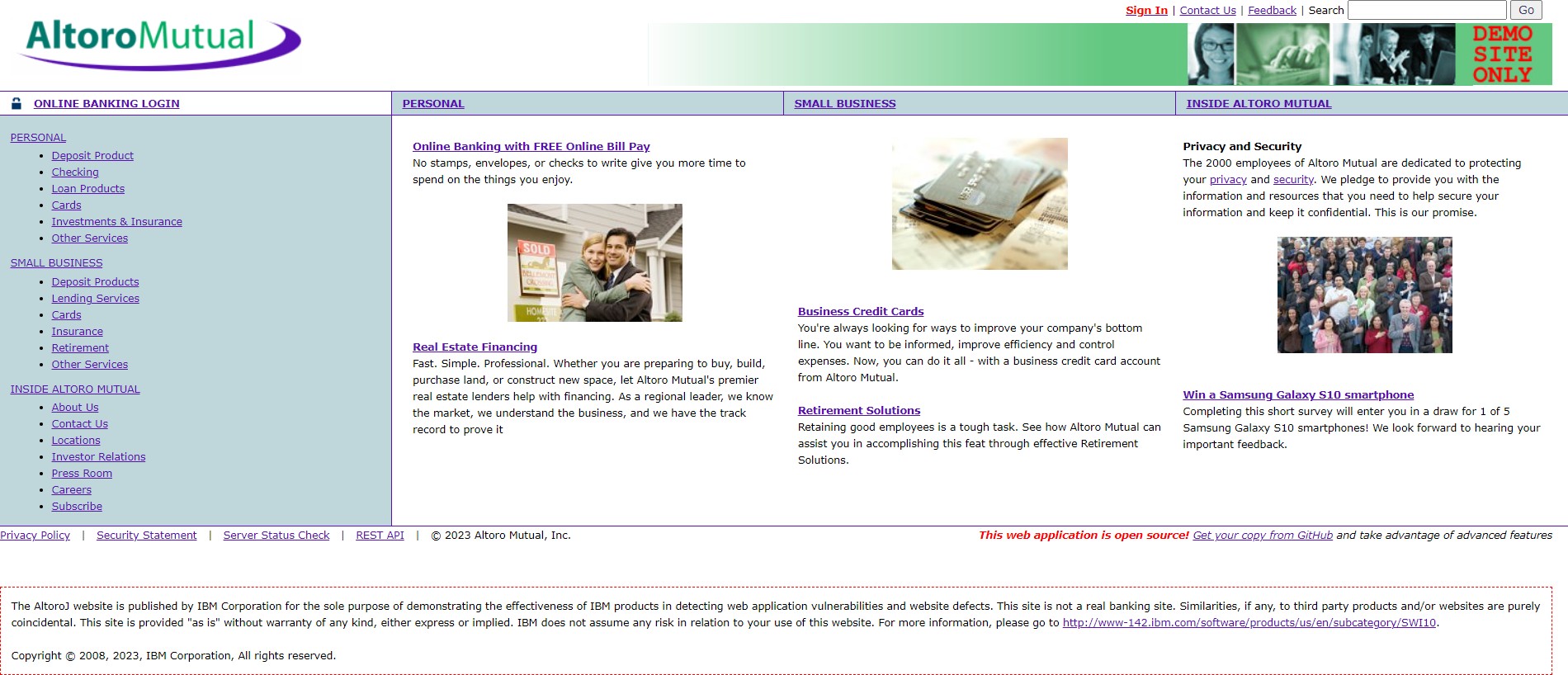


SMARTINTERNZVIRTUALINTERNSHIP

### Vulnerability Exploitation And Patching

AltoroMutual





# Part1:ExecutiveSummary

### Executive Summary: Altoro Mutual Website Vulnerability Exploitation and Patching

**Altoro Mutual is a subsidiary of Altoro, a multi-state holding company located in the heart of Massachusetts. Altoro Mutual has been serving Boston and surrounding communities for nearly 75 years.**

**Altoro Mutual offers a broad range of commercial, private, retail and mortgage banking services to small- and middle-market businesses and individuals**.

Using a combination of manual analysis and automated scanning tools, the assessmentaimed to detect vulnerabilities that could be exploited by malicious actors to gainunauthorized access or compromise the website's sensitive data. Rigorous testing wasperformed, taking into account various attack vectors and techniques commonly used byhackers.

The assessment revealed several ﬁndings regarding the website's network security.Multiple high-severity vulnerabilities were detected, including unpatched software, openports with inadequate security controls, and weaknesses in the password policyimplementation. These critical issues exposed the website to potential cyberattacks, databreaches,andservicedisruptions.

Toaddresstheidentiﬁedvulnerabilities,asetofcomprehensiverecommendationshasbeen provided. Altoro Mutual can signiﬁcantly enhance the security of its website's networkinfrastructure,mitigatepotentialvulnerabilities,andfortifyitsdefenseagainstcyberthreats. Regular follow-up assessments are encouraged to ensure continuous improvementinnetworksecurity.

# Overview

### Overview:Vulnerability Exploitation and Patching

Vulnerability Exploitation and Patching on Altoro Mutual is a comprehensive evaluation ofthe organization's network infrastructure to identify potential security weaknesses andvulnerabilities. Altoro Mutual is a ﬁnancial services company that handles sensitive data,making it imperative to maintain a robust and secure network environment. Thisassessment aims to identify and address security gaps that could expose the company tocyberthreats,databreaches,andﬁnanciallosses.

The primary objectives of the Network Vulnerability Assessment on Altoro Mutual are asfollows:

1. **Identify Vulnerabilities**: The assessment aims to identify potential vulnerabilities in thenetworkinfrastructure,includingunpatchedsoftware,misconﬁgurations,andopenports.
2. **Evaluate Security Controls**: The effectiveness of existing security controls, such asﬁrewalls,intrusiondetectionsystems(IDS),andaccesscontrols,isassessedtodeterminetheirabilitytodetectandpreventattacks.
3. **AssessNetworkArchitecture:**Thenetworkarchitectureisreviewedtoensurepropersegmentation,isolationofcriticalassets,andarobustperimeterdefense.
4. **Password Policy Evaluation**: The assessment examines the strength of passwordpoliciesandtheir adherencetoindustry bestpracticesto preventunauthorizedaccess.
5. **Physical Security Analysis**: Physical security measures in place to protect networkinfrastructureanddatacentersareevaluatedtopreventunauthorizedphysicalaccess.

### Methodology:

Theassessmentfollowsawell-deﬁnedmethodology,includingthefollowingsteps

1. **Reconnaissance**:Passivereconnaissancetechniquesareusedtogatherinformationaboutthenetworkanditsassets.
2. **Vulnerability Scanning**: Automated scanning tools are employed to identify potentialvulnerabilitiesinthenetwork.
3. **Manual Veriﬁcation**: The identiﬁed vulnerabilities are manually veriﬁed to eliminatefalsepositivesandprioritizecriticalissues.
4. **Exploitation (with Authorization)**: Ethical exploitation of vulnerabilities is conducted todeterminetheextentofpotentialdamageifexploitedmaliciously.
5. **AnalysisandReporting**:Theassessmentﬁndingsareanalyzed,andadetailedreportisgenerated,includingalistofvulnerabilities,riskseverity,andactionablerecommendations.

### Deliverables:

Theassessmentwillprovidethefollowingdeliverables:

1. **Network Vulnerability Assessment Report**: A comprehensive report detailing theassessmentmethodology,ﬁndings,riskanalysis,andactionablerecommendations.
2. **ExecutiveSummary:**Aconcisesummaryhighlightingkeyﬁndingsandcriticalvulnerabilitiesforexecutivestakeholders.
3. **Remediation Plan:** A roadmap outlining the prioritized actions required to addressidentiﬁedvulnerabilitiesandimprovenetworksecurity.

# Part2:DetailReport

### InformationGathering:

Informationgatheringisacrucialphaseinthecybersecurityandassessmentprocess.Itinvolves collecting relevant data and intelligence about a target system, network, ororganization to understand its vulnerabilities and potential attack surfaces. Here aredifferentaspectsofinformationgathering:

1. EmailFootprintAnalysis:

Email footprint analysis is a technique used to collect information about an individual or organization by analyzing their email communications. This can include analyzing the email headers, email addresses, and email content to gather information such as the sender IP address, email service providers, and communication patterns. This technique can be useful in threat intelligence, social engineering, and other cyber investigations**.**

1. DNSInformationGathering:

DNS (Domain Name System) information gathering involves gathering information about a target domain DNS records. This can include the domain IP address, mail servers, subdomains, and other related information. This technique can be used to identify vulnerabilities and misconfigurations in a target DNS infrastructure.

1. WHOISInformationGathering:

WHOIS information gathering involves gathering information about the owner of a

domain name, IP address, or autonomous system number (ASN).

This information can include the owner name, contact details, and registration dates.

This technique can be useful in identifying the owners of malicious or suspicious domains..

### Information Gathering For Social Engineering Attacks

Social engineering attacks involve manipulating individuals to divulge sensitive information or

perform certain actions. Information gathering for social engineering attacks involves

researching the target personal and professional information, communication patterns, and

behavior to craft effective social engineering attacks.

### Information Gathering For Physical Security Assessments

Physical security assessments involve identifying vulnerabilities in an organization physical

security measures. Information gathering for physical security assessments involves

researching the organization security measures, physical layout, access control measures,

and employee behavior to identify potential security weaknesses.

1. EmergingTrendsandTechnologiesinInformationGathering:

Information gathering is a constantly evolving field with new trends and technologies emerging all the time. Some emerging trends and technologies in information gathering include the use of machine learning and artificial intelligence to automate data analysis, the increasing use of open-source intelligence (OSINT) tools, and the use of big data analytics to identify patterns and trends..

### Vulnerability Identification

### Identify And Name Each Vulnerability

Understanding and defining vulnerabilities involves identifying potential weaknesses and

flaws in an application design or implementation. This process involves reviewing the

application code and functionality to identify any areas that could potentially be exploited by

an attacker. Once a vulnerability has been identified, it must be defined and classified based

on its severity and potential impact on the application's security.

### Assign A Common Weakness Enumeration (CWE) Code To Each Vulnerability

Identifying and naming vulnerabilities involves the process of discovering and documenting

specific security weaknesses or flaws in an application. This process typically involves using

automated tools or manual testing techniques to identify potential vulnerabilities. Once a

vulnerability has been identified, it must be given a descriptive name that accurately reflects

the nature of the vulnerability.

### Provide Corresponding Open Web Application Security Project (OWASP) Category And Description For Each Vulnerability

Assigning CWE codes to each vulnerability is an essential step in the vulnerability

identification process. A CWE code is a unique identifier assigned to a specific type of

vulnerability, making it easier to identify and categorize similar types of vulnerabilities.

Assigning a CWE code to each vulnerability allows developers and security professionals

to more easily track, analyze and remediatepotential security issues.

### Understanding And Defining Vulnerabilities

Understanding and defining vulnerabilities is a critical first step in identifying and mitigating

potential risks in an application. A vulnerability can be defined as a flaw or weakness in the

system that can be exploited by attackers to compromise the security of the system

Vulnerabilities can exist in different layers of the application, including the network layer,

application layer, and the database layer. By understanding the different types of

vulnerabilities that exist, developers and security professionals can take appropriate measures

to mitigate the risks and prevent attacks.

### Identifying And Naming Vulnerabilities

Identifying and naming vulnerabilities is the next step in the vulnerability assessment process.

This involves conducting a thorough analysis of the application to identify all potential

vulnerabilities that could be exploited by attackers. Once identified, each vulnerability should

be given a clear and concise name that accurately describes the nature of the vulnerability.

### Assigning CWE Codes To Each Vulnerability

Assigning Common Weakness Enumeration (CWE) codes to each vulnerability is an important

step in the vulnerability assessment process. CWE is a community-developed list of common

software and hardware weaknesses, maintained by the MITRE Corporation, which provides a

common language for identifying, understanding, and mitigating software vulnerabilities. By

assigning a CWE code to each vulnerability, security professionals and developers can better

understand the nature of the vulnerability and take appropriate stepto mitigate the risk.

### Providing OWASP Category And Description For Each Vulnerability

Providing OWASP category and description for each vulnerability involves categorizing the

vulnerabilities based on the OWASP Top 10, which is a list of the most common web

application vulnerabilities. This process involves identifying which OWASP category the

vulnerability falls under and providing a detailed description of the vulnerability. This

information is important because it helps developers and security professionals prioritize

which vulnerabilities to address first, based on their potential impact on the application's

security.

**Business Impact Assessment**

### Conduct A Thorough Analysis Of The Potential Business Impact Of Each Vulnerability

Conducting a business impact assessment is an important step in the vulnerability

identification and reporting process. This involves analyzing the potential impact that each

vulnerability could have on the organization&#39;s operations, reputation, and finances. The

assessment should take into account the likelihood of the vulnerability being exploited, the

potential damage that could be caused, and the organization&#39;s ability to respond and

recover from such an incident. By conducting a thorough business impact assessment,

stakeholders can prioritize the vulnerabilities and allocate resources appropriately to

mitigate the risks.

### Understand The Potential Consequences Of Each Vulnerability On The Business:

Understanding the potential consequences of each vulnerability is crucial for effective risk management. This involves identifying and analyzing the potential outcomes of a successful exploit of the vulnerability, such as data loss, system downtime, reputational damage, and financial losses. By understanding the potential consequences, stakeholders can assess the risk associated with each vulnerability and prioritize the mitigation efforts accordingly.

### Conducting A Business Impact Assessment

Conducting a business impact assessment involves evaluating the potential impact of

vulnerabilities on the business. This involves identifying critical business processes and

assessing the impact of the vulnerabilities onthese processes. By conducting a business

impact assessment, organizations can prioritize vulnerabilities based on their potential impact

on the business.

### Understanding Potential Consequences Of Vulnerabilities

Understanding potential consequences of vulnerabilities is crucial in determining the level of

risk posed by each vulnerability. This involves assessing the likelihood of a vulnerability being

exploited, the potential impact of an exploit, and the potential consequences of a successful

attack. By understanding the potential consequences of vulnerabilities, organizations can

develop appropriate mitigation strategies to minimize the risk to the business.

### Assessing The Risk To The Business

Assessing the risk to the business involves evaluating the likelihood of a vulnerability being

exploited and the potential impact it could have on the organization. The risk assessment

should take into account factors such as the threat landscape, the value of the assets at risk,

and the organizations current security posture. By conducting a risk assessment,

stakeholders can identify vulnerabilities that pose the greatest risk to the organization and

prioritize their remediation efforts. It is important to conduct ongoing risk assessments to

ensure that vulnerabilities are identified and addressed in a timely manner.

### Vulnerability Path And Parameter Identification

### Methods For Identifying Vulnerability Paths And Parameters

There are several methods for identifying vulnerability paths and parameters. One method is

to conduct a code review, which involves analyzing the source code of an application to

identify vulnerabilities. Another method is to use automated vulnerability scanners, which can

help identify vulnerabilities and their associated paths and parameters. Additionally,

penetration testing and ethical hacking can be used to identify vulnerabilities by attempting to

exploit them.

### Types Of Vulnerability Paths And Parameters

Vulnerability paths and parameters can vary depending on the type of vulnerability. For

example, a SQL injection vulnerability may have a path that involves submitting malicious

input to a web form, while a cross-site scaripting vulnerability may have a path that involves

injecting malicious code into a web page. Parameters can also vary, depending on the type of

vulnerability and the specific application being tested. Examples of parameters that may be

vulnerable include user input fields, URLs, and cookies.

### Common Tools And Techniques For Identifying Vulnerability Paths And Parameters

There are a variety of tools and techniques that can be used to identify vulnerability paths and

parameters. These include manual code reviews, automated vulnerability scanners, and web

application firewalls. Additionally, network sniffing and packet analysis can be used to identify

vulnerabilities related to network communication.

### Best Practices For Vulnerability Path And Parameter Identification

To ensure that vulnerability paths and parameters are identified accurately and

comprehensively, it is important to use a combination of manual and automated testing

methods. It is also important to test applications in different environments and with different

user roles to identify all possible attack vectors. Finally, thorough documentation and

reporting of identified vulnerabilities and their associated paths and parameters is crucial for

developers to be able to address the vulnerabilities effectively.

### Challenges And Limitations Of Vulnerability Path And Parameter Identification

One of the biggest challenges in identifying vulnerability paths and parameters is the

constantly evolving nature of vulnerabilities and attack methods. Additionally, some

vulnerabilities may be difficult to identify and require specialized knowledge and skills to

detect. Another limitation is the potential for false positives or false negatives in vulnerability

scanning and testing, which can lead to wasted time and resources.

### Detailed Instruction For Vulnerability Reproduction

### Importance Of Providing Detailed Instructions

Providing detailed instructions for reproducing vulnerabilities is crucial for developers to

understand the specific steps required to fix the vulnerability. Without detailed instructions,

developers may have difficulty understanding the nature of the vulnerability and how to fix it.

Detailed instructions also ensure that vulnerabilities are correctly identified and addressed,

reducing the risk of future attacks.

### Components Of A Well-Written Vulnerability Reproduction Instruction

A well-written vulnerability reproduction instruction should include a detailed description of

the vulnerability, steps to reproduce the vulnerability, and expected outcomes. The instruction

should also include information on the platform or application affected, the severity of the

vulnerability, and any potential impact on the business.

### Steps For Reproducing Vulnerabilities

The steps for reproducing vulnerabilities typically involve a series of actions or inputs that

trigger the vulnerability. These steps must be clearly defined and detailed to ensure that

developers can understand and replicate the vulnerability. Additionally, steps for reproducing

vulnerabilities should be consistent across multiple systems or environments to ensure that

the vulnerability can be identified and addressed in a timely manner.

### Best Practices For Writing Effective Vulnerability Reproduction Instructions

Effective vulnerability reproduction instructions should be clear, concise, and easy to

understand. Instructions should be written in plain language and avoid technical jargon.

Screenshots or videos can be used to supplement written instructions and provide visual aids

for developers.

### Tools And Techniques For Verifying Vulnerability Fixes

Tools and techniques for verifying vulnerability fixes may include automated testing tools,manual testing, and code reviews. These methods can be used to ensure that vulnerabilities have been successfully fixed and that no new vulnerabilities have been introduced.

### Challenges And Limitations Of Vulnerability Reproduction Instruction

Challenges and limitations of vulnerability reproduction instruction may include differences in system configurations or environments, difficulty in replicating complex vulnerabilities, and the need for access to source code or proprietary systems. It is important to address these challenges to ensure that vulnerabilities are accurately identified and addressed.

### Comprehensive And Detailed Reporting

### Importance Of Comprehensive And Detailed Reporting

Comprehensive and detailed reporting is crucial for businesses and organizations to make informed decisions. It involves analyzing and presenting data in a clear and concise manner, which helps stakeholders to identify patterns, trends, and potential problems. Comprehensive and detailed reporting provides an accurate picture of an organization's operations, financial performance, and overall health, which can be used to guide strategic planning and resource allocation.

### Key Components Of Comprehensive And Detailed Reporting

Key components of comprehensive and detailed reporting include accurate and relevant data, effective data analysis, clear and concise presentation of findings, and actionable recommendations. The report should be well-organized, easy to understand, and tailored to the audience's needs. It should also provide context for the data presented, such as benchmarking against industry standards or historical data.

### Strategies For Effective Reporting

Strategies for effective reporting include identifying the purpose and scope of the report, understanding the audience's needs, selecting appropriate data sources and analysis techniques, and using clear and concise language to present findings. The report should be well-organized, visually appealing, and use data visualization tools to help the audience better understand the data.

### Challenges In Implementing Comprehensive And Detailed Reporting

Challenges in implementing comprehensive and detailed reporting include data quality issues, data silos, lack of resources, and difficulty in identifying the right metrics to measure. Organizations also face challenges in presenting data in a way that is easily digestible for different stakeholders, such as executives, managers, and frontline employees.

### Impact Of Comprehensive And Detailed Reporting On Decision-Making

Comprehensive and detailed reporting can have a significant impact on decision-making by providing stakeholders with the information they need to make informed decisions. It can help identify areas for improvement, highlight potential risks, and guide resource allocation. By providing a comprehensive view of an organization's operations, financial performance, and overall health, stakeholders can make more informed decisions that align with their strategic goals.

### Best Practices For Creating Comprehensive And Detailed Reports

Best practices for creating comprehensive and detailed reports include defining the purpose and scope of the report, selecting appropriate data sources and analysis techniques, using clear and concise language to present findings, and including actionable recommendations. The report should be well-organized, visually appealing, and tailored to the audience's needs. It should also provide context for the data presented, such as benchmarking against industry standards or historical data.

TheresultoftheinformationgatheringperformedonAltoroMutual(ip:65.61.131.117)domainname:testfire.net

### EmailFootprintAnalysis:

**Toolused:**theHarvester

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,suchassearchengines,publicdatabases,andsocialmediaplatforms,toextractvaluable information about a target organization or individual. The tool primarily focuseson harvesting email addresses, subdomains, hostnames, and other related informationthatcanbeusedforfurtheranalysisorexploitation.

**Commandused:**theHarvester-d testfire.net-b all

### Output:

[\*]IPsfound:3

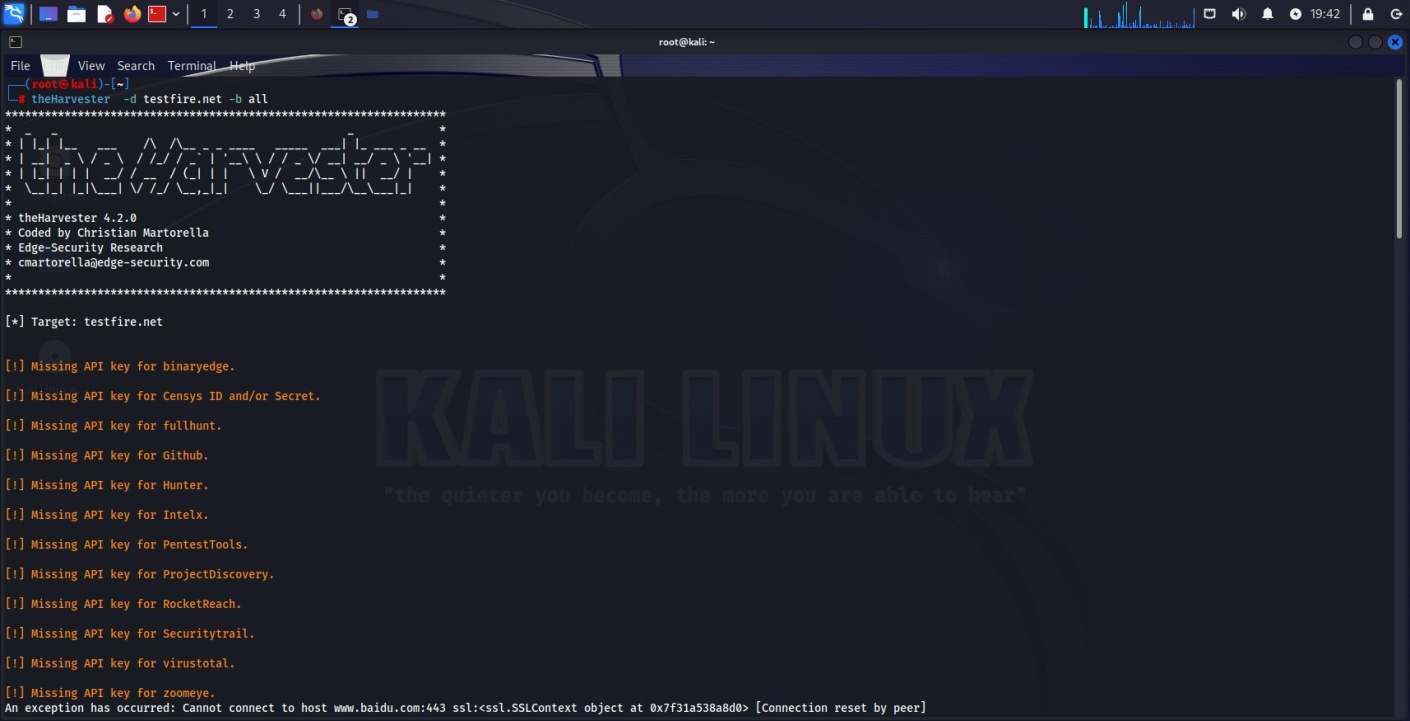
65.61.137.117

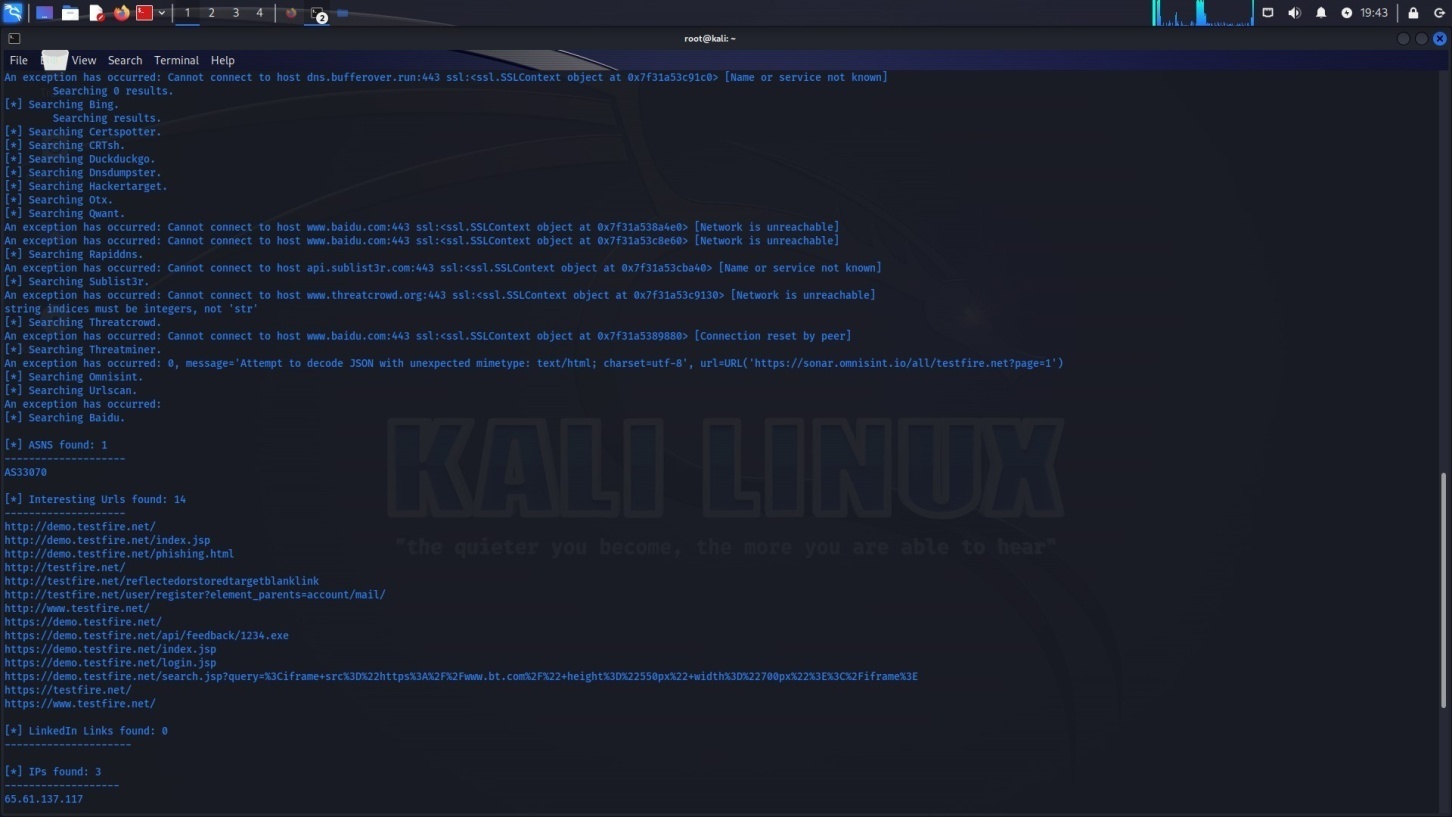
[\*]Noemailsfound.[\*]Hostsfound:41

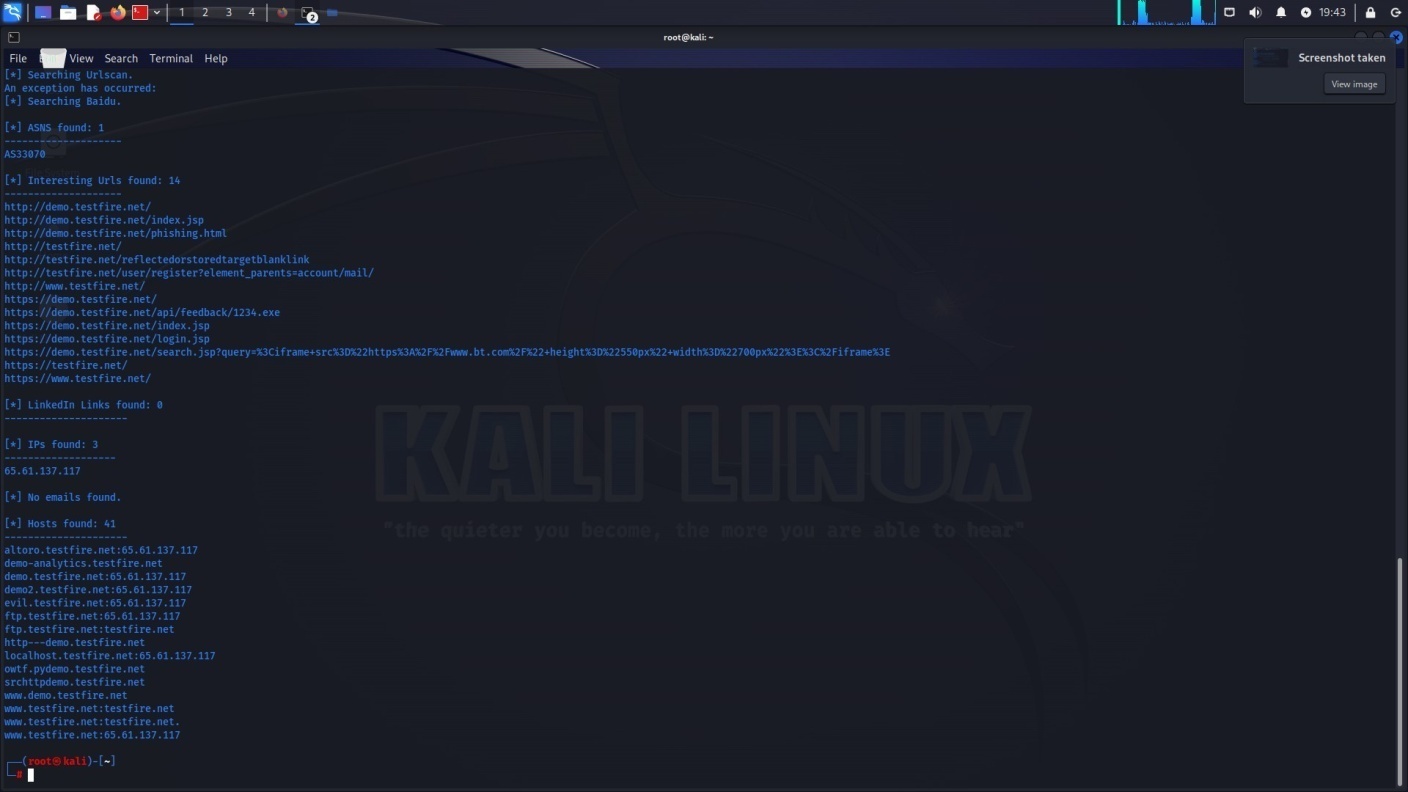
altoro.testfire.net:65.61.137.117demo-analytics.testfire.netdemo.testfire.net:65.61.137.117demo2.testfire.net:65.61.137.117evil.testfire.net:65.61.137.117ftp.testfire.net:65.61.137.117ftp.testfire.net:testfire.net

http---demo.testfire.netlocalhost.testfire.net:65.61.137.117owtf.pydemo.testfire.netsrchttpdemo.testfire.net[www.demo.testfire.net](http://www.demo.testfire.net/)www.testfire.net:testfire.netwww.testfire.net:testfire.net.www.testfire.net:65.61.137.117

**Result:**NoemailfoundinAltoroMutual

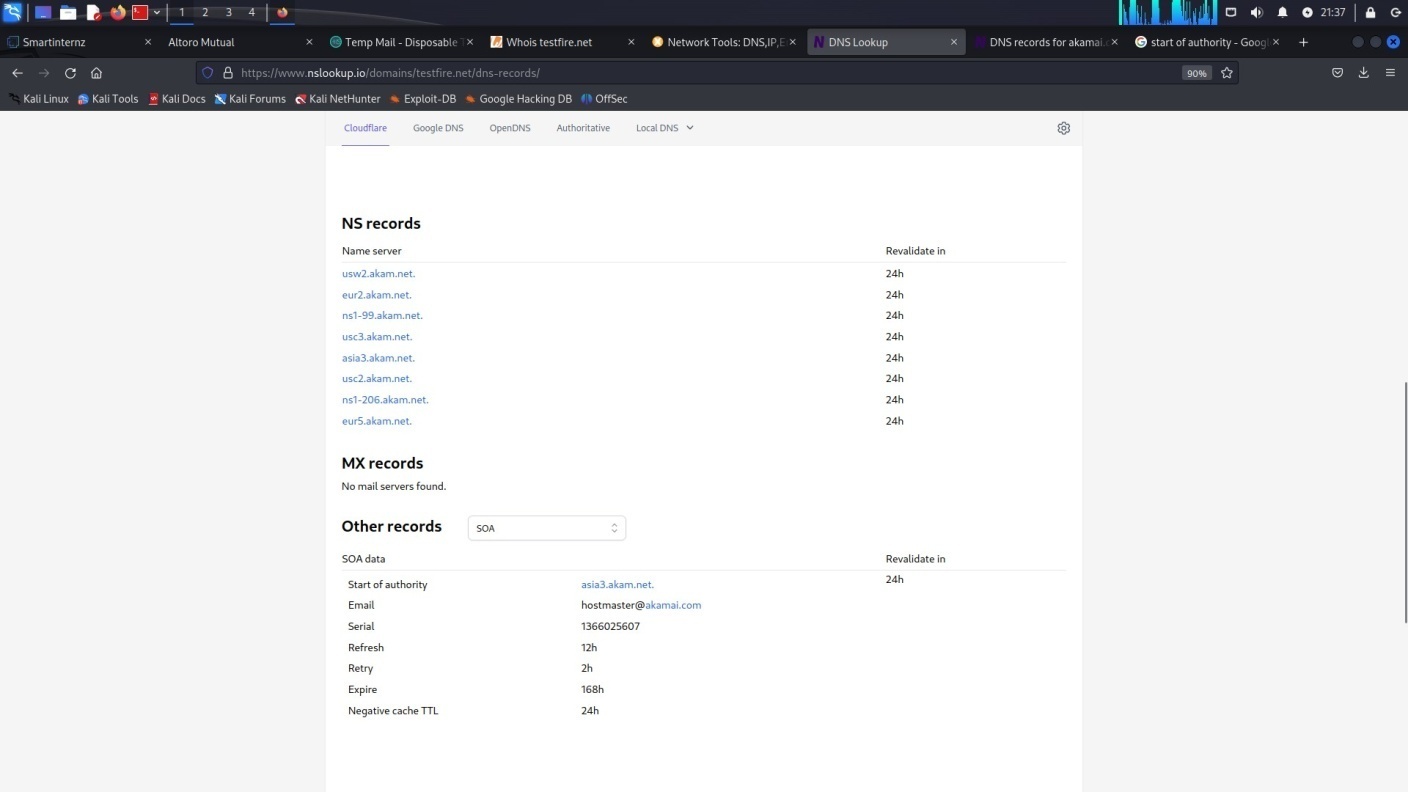
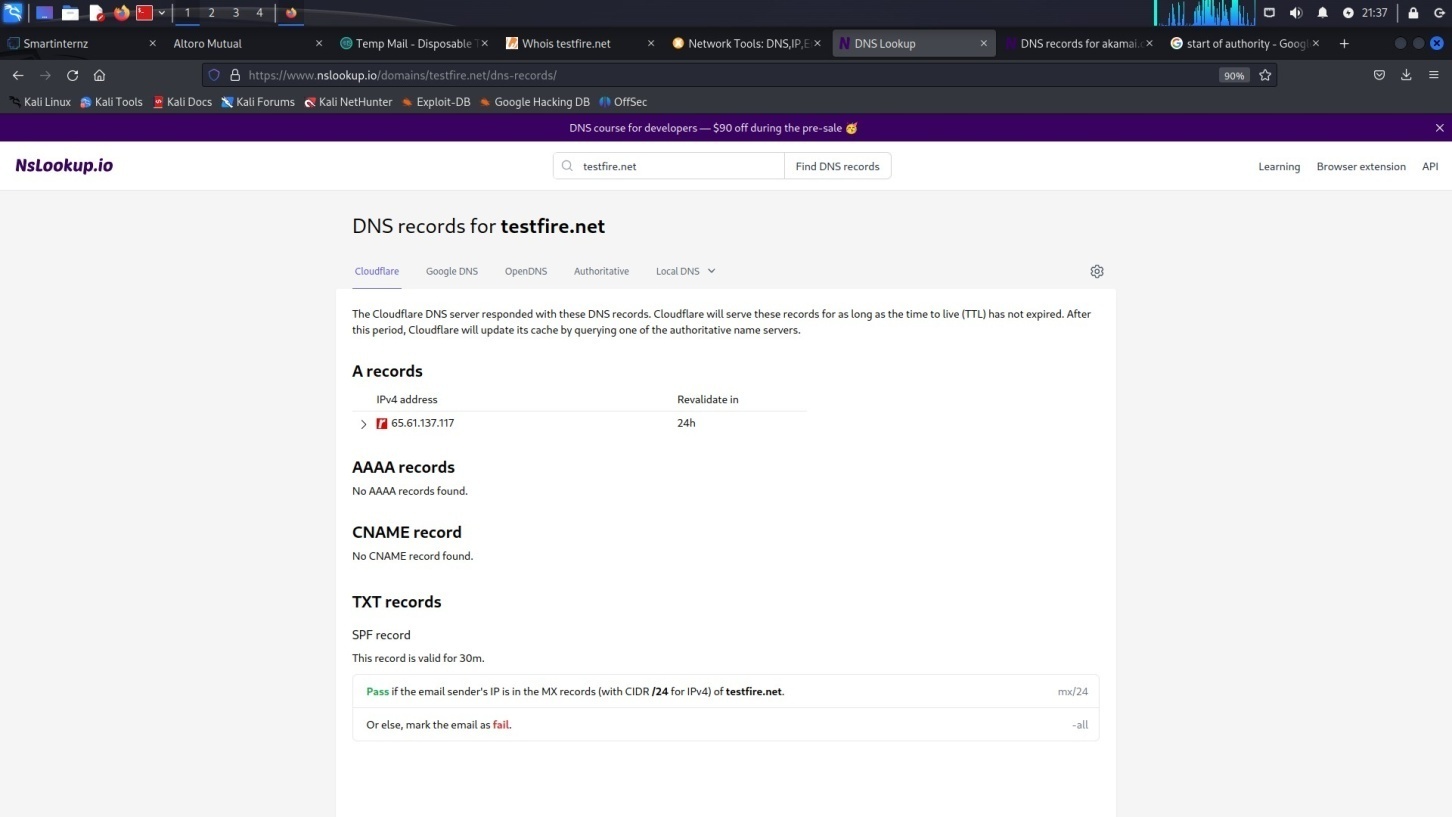






### DNSINFORMATIONGATHERING

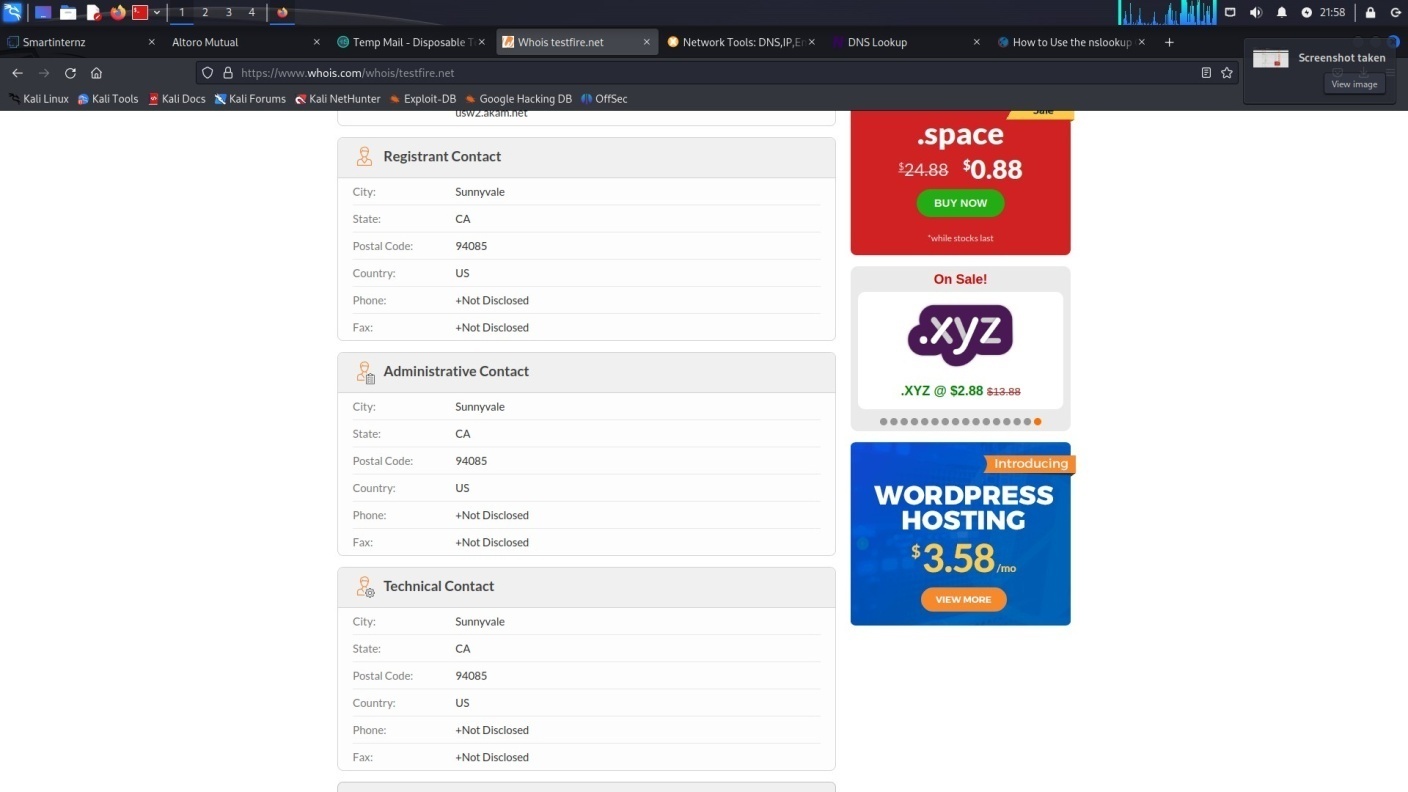
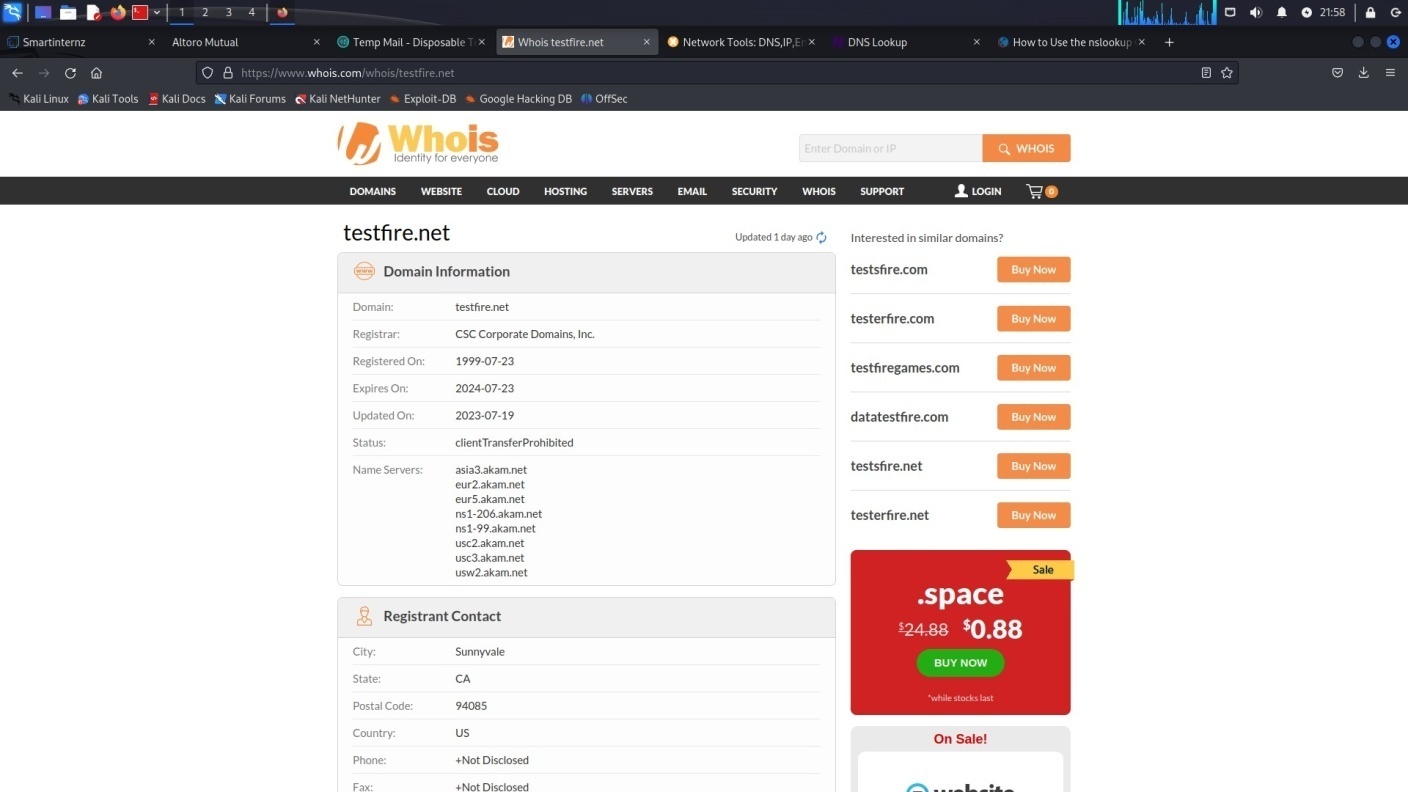
**WebsitelinkofAltoroMutualDnsresult**

[https://www.nslookup.io/domains/testﬁre.net/dns-records/](https://www.nslookup.io/domains/testfire.net/dns-records/)

### WHOISINFORMATIONGATHERING

**WebsiteofwhoisipresultlinkofAltoroMutual**

[https://www.whois.com/whois/testﬁre.net](https://www.whois.com/whois/testfire.net)

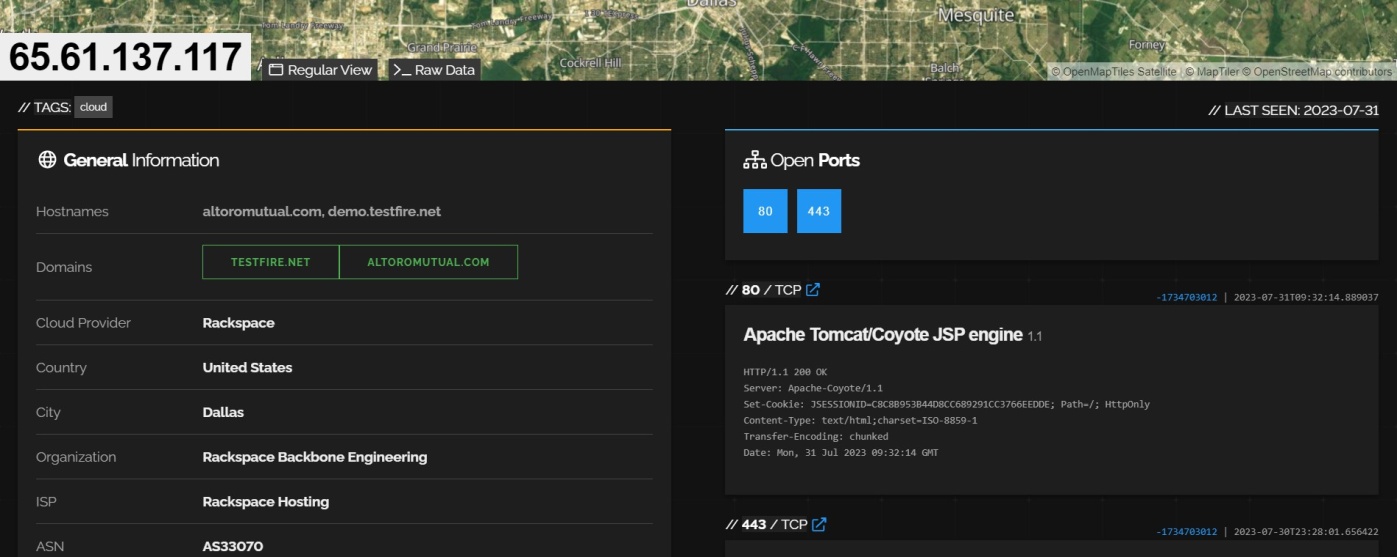


### SHADON

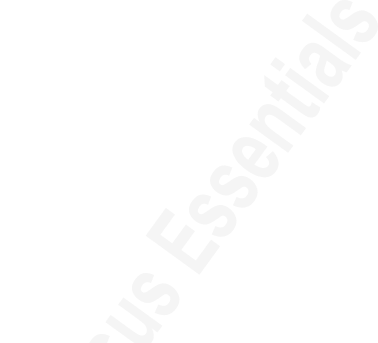
SHODAN: Shodan is a search engine designed to ﬁnd internet-connected devices andsystems. It can provide information about a website's servers, open ports, and otherinternet-facingassets.

**WebsiteofshodanresultofAltoroMutual**

<https://www.shodan.io/host/65.61.137.117>



### VulnerabilityReport





**altoroMutual**

ReportgeneratedbyNessus™ Sun,30Jul202320:46:19IST

**VulnerabilitiesbyHost**

* 65.61.137.117



•

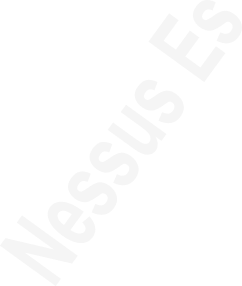
# VulnerabilitiesbyHost

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | **65.61.137.117** |  | |
| 0 | 0 | 1 | 0 | 20 |
| CRITICAL | HIGH | MEDIUM | LOW | INFO |

ScanInformation

Starttime: SunJul3019:36:582023

Endtime: SunJul3020:46:192023



HostInformation

IP: 65.61.137.117

OS: CISCOPIX7.0

Vulnerabilities

Synopsis

TheremoteserviceencryptstrafficusinganolderversionofTLS.

Description

TheremoteserviceacceptsconnectionsencryptedusingTLS1.0.TLS 1.0 has a number ofcryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newerversionsofTLSlike

1.2and1.3aredesignedagainsttheseflawsandshouldbeusedwheneverpossible.

As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer functionproperlywithmajorwebbrowsersandmajorvendors.

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 notbeingsusceptibletoanyknownexploits.

SeeAlso

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

Solution

EnablesupportforTLS1.2and1.3,anddisablesupportforTLS1.0.

RiskFactorMedium

CVSSv3.0BaseScore

6.5(CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

CVSSv2.0BaseScore

* 1. (CVSS2#AV:N/AC:H/Au:N/C:C/I:P/A:N)

References

XREF [CWE:327](http://cwe.mitre.org/data/definitions/327)

PluginInformation

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

PluginOutput



tcp/443/ww



Synopsis

Nessushasdetectedpotentialvirtualhosts.

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 onlythealternatehostnamesforvhostsdiscoveredonawebserver.

Differentwebserversmaybehostedonname-basedvirtualhosts.

See Also<https://en.wikipedia.org/wiki/Virtual_hosting>

Solution

Ifyouwanttotestthem,re-scanusingthespecialvhostsyntax,suchas:[www.example.com](http://www.example.com/)[192.0.32.10]

RiskFactorNone

PluginInformation

Published:2010/04/29,Modified:2022/08/15

PluginOutputtcp/0

Synopsis

ItwaspossibletoenumerateCPEnamesthatmatchedontheremotesystem.

Description

ByusinginformationobtainedfromaNessusscan,thispluginreportsCPE(CommonPlatformEnumeration)matchesforvarioushardwareandsoftwareproductsfoundonahost.

NotethatifanofficialCPEisnotavailablefortheproduct,thisplugincomputesthebestpossibleCPEbasedontheinformationavailablefromthescan.

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

<https://nvd.nist.gov/products/cpe>

Solutionn/aRiskFactorNone

PluginInformation

Published:2010/04/21,Modified:2023/07/27PluginOutputtcp/0





Synopsis

Itispossibletoguesstheremotedevicetype.

Description

Basedontheremoteoperatingsystem,itispossibletodeterminewhattheremotesystemtypeis(eg:aprinter,router,general-purposecomputer,etc).

Solutionn/aRiskFactorNone

PluginInformation

Published:2011/05/23,Modiﬁed:2022/09/09PluginOutputtcp/



Synopsis

ItispossibletodeterminewhichTCPportsareopen.

Description

ThispluginisaSYN'half-open'portscanner.Itshallbereasonablyquickevenagainstafirewalledtarget.

NotethatSYNscansarelessintrusivethanTCP(fullconnect)scansagainstbrokenservices,buttheymight cause problems for less robust firewalls and also leave unclosed connections on the remotetarget,ifthenetworkisloaded.

Solution

ProtectyourtargetwithanIPfilter.RiskFactorNone

PluginInformation

Published:2009/02/04,Modified:2023/06/20Plugin

Output



tcp/80



Synopsis

ItispossibletodeterminewhichTCPportsareopen.

Description

ThispluginisaSYN'half-open'portscanner.Itshallbereasonablyquickevenagainstafirewalledtarget.

NotethatSYNscansarelessintrusivethanTCP(fullconnect)scansagainstbrokenservices,buttheymight cause problems for less robust firewalls and also leave unclosed connections on the remotetarget,ifthenetworkisloaded.

Solution

ProtectyourtargetwithanIPfilter.RiskFactorNone

PluginInformation

Published:2009/02/04,Modified:2023/06/20PluginOutputtcp/443/www





Synopsis

ItispossibletodeterminewhichTCPportsareopen.

Description

ThispluginisaSYN'half-open'portscanner.Itshallbereasonablyquickevenagainstafirewalledtarget.

NotethatSYNscansarelessintrusivethanTCP(fullconnect)scansagainstbrokenservices,buttheymight cause problems for less robust firewalls and also leave unclosed connections on the remotetarget,ifthenetworkisloaded.

Solution

ProtectyourtargetwithanIPfilter.RiskFactorNone

PluginInformation

Published:2009/02/04,Modified:2023/06/20PluginOutputtcp/8080



Synopsis

ThisplugindisplaysinformationabouttheNessusscan.

Description

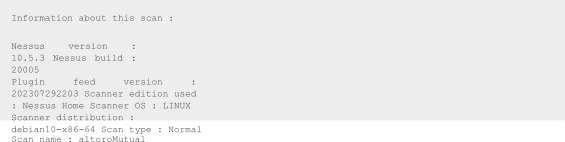
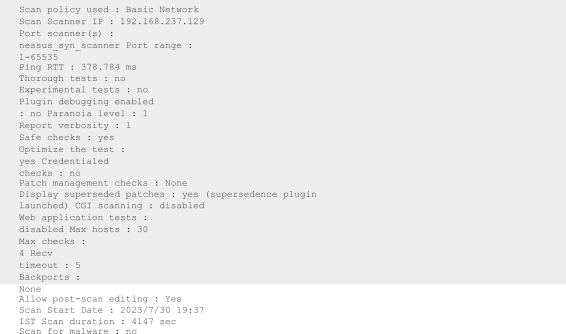
Thisplugindisplays,foreachtestedhost,informationaboutthescanitself:

* Theversionofthepluginset.
* Thetypeofscanner(NessusorNessusHome).
* TheversionoftheNessusEngine.
* Theportscanner(s)used.
* Theportrangescanned.
* Thepingroundtriptime
* Whethercredentialedorthird-partypatchmanagementchecksarepossible.
* Whetherthedisplayofsupersededpatchesisenabled
* Thedateofthescan.
* Thedurationofthescan.
* Thenumberofhostsscannedinparallel.
* Thenumberofchecksdoneinparallel.Solutionn/a

RiskFactorNone

PluginInformation

Published:2005/08/26,Modified:2023/04/27PluginOutputtcp





Synopsis

Itispossibletoguesstheremoteoperatingsystem.

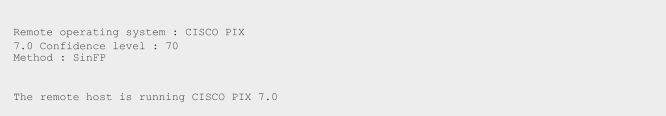
Description

Usingacombinationofremoteprobes(e.g.,TCP/IP,SMB,HTTP,NTP,SNMP,etc.),itispossibletoguessthenameoftheremoteoperatingsysteminuse.Itisalsopossiblesometimestoguesstheversionoftheoperatingsystem.

Solutionn/aRiskFactorNone

PluginInformation

Published:2003/12/09,Modified:2022/03/09





Synopsis

Theremoteserviceencryptscommunications.

Description

ThisplugindetectswhichSSLandTLSversionsaresupportedbytheremoteserviceforencryptingcommunications.

Solutionn/aRiskFactorNone

PluginInformation

Published:2011/12/01,Modified:2023/07/10PluginOutputtcp/443/www





Synopsis

ThisplugindisplaystheSSLcertificate.

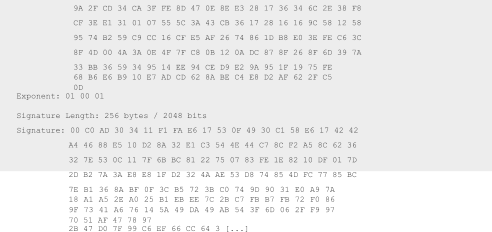
Description

ThispluginconnectstoeverySSL-relatedportandattemptstoextractanddumptheX.509certificate.Solutionn/a

RiskFactorNone

PluginInformation

Published:2008/05/19,Modified:2021/02/03



Synopsis

AknownCASSLcertificateinthecertificatechainhasbeensignedusingaweakhashingalgorithm.

Description

The remote service uses a known CA certificate in the SSL certificate chain that has been signed using acryptographically weak hashing algorithm (e.g., MD2, MD4, MD5, or SHA1). These signature algorithmsare known to be vulnerable to collision attacks (CVE-2004-2761, for example). An attacker can exploitthistogenerateanothercertificatewiththesamedigitalsignature,allowingtheattackertomasqueradeastheaffectedservice.

NotethatthispluginreportsallSSLcertificatechainssignedwithSHA-1thatexpireafterJanuary1,2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1cryptographichashalgorithm.

Note that this plugin will only fire on root certificates that are known certificate authorities aslisted in Tenable Community Knowledge Article 000001752. That is what differentiates thisplugin from plugin 35291, which will fire on any certificate, not just known certificate authorityrootcertificates.

Known certificate authority root certificates are inherently trusted and so any potential issues withthesignature,includingitbeingsignedusingaweakhashingalgorithm,arenotconsideredsecurityissues.

SeeAlso

<http://www.nessus.org/u?ae636e78><https://tools.ietf.org/html/rfc3279><http://www.nessus.org/u?9bb87bf2>

Solution

ContacttheCertificateAuthoritytohavethecertificatereissued.RiskFactorNone

References

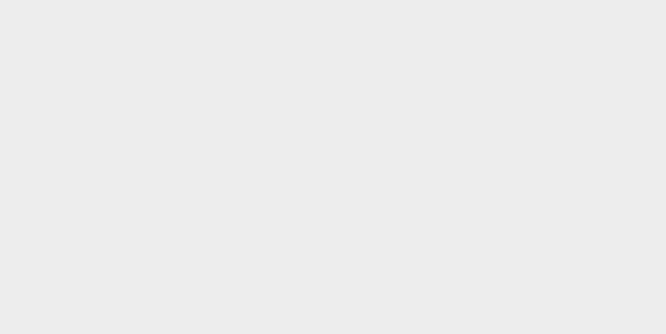
BID [11849](http://www.securityfocus.com/bid/11849)

BID [33065](http://www.securityfocus.com/bid/33065)

XREF [CWE:310](http://cwe.mitre.org/data/definitions/310)

PluginInformation

Published:2016/12/08,Modified:2022/10/12PluginOutputtcp/443/www



ThefollowingknownCAcertificateswerepartofthecertificatechainsentbytheremotehost,butcontainhashesthatareconsideredtobeweak.

SubjectServices

:C=GB/ST=GreaterManchester/L=Salford/O=ComodoCALimited/CN=AAACertificate

SignatureAlgorithm:SHA-1WithRSAEncryptionValidFrom :Jan0100:00:002004GMTValidTo :Dec3123:59:592028GMT

RawPEMcertificate:

-----BEGINCERTIFICATE-----

MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEbMBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDA

+GB+O5AL686tdUIoWMQuaBtDFcCLNSS1UY8y2bmhGC1Pqy0wkwLxyTurxFa70VJoSCsN6sjNg4tqJVfMiWPPe3M/vg4aijJRPn2jymJBGhCfHdr/jzDUsi14HZGWCwEiwqJH5YZ92IFCokcdmtet4YgNW8IoaE+oxox6gmf049vYnMlhvB/VruPsUK6+3qszWY19zjNoFmag4qMsXeDZRrOme9Hg6jc8P2ULimAyrL58OAd7vn5lJ8S3frHRNG5i1R8XlKdH5kBjHYpy

+g8cmez6KJcfA3Z3mNWgQIJ2P2N7Sw4ScDV7oL8kCAwEAAaOBwDCBvTAdBgNVHQ4EFgQUoBEKIz6W8Qfs4q8p74Klf9AwpLQwDgYDVR0PAQH/BAQDAgEGMA8GA1UdEwEB/

wQFMAMBAf8wewYDVR0fBHQwcjA4oDagNIYyaHR0cDovL2NybC5jb21vZG9jYS5jb20vQUFBQ2VydGlmaWNhdGVTZXJ2aWNlcy5jcmwwNqA0oDKGMGh

+k+tZ7xkSAzk/ExfYAWMymtrwUSWgEdujm7l3sAg9g1o1QGE8mTgHj5rCl7r

+8dFRBv/38ErjHT1r0iWAFf2C3BUrz9vHCv8S5dIa2LX1rzNLzRt0vxuBqw8M0Ayx9lt1awg6nCpnBBYurDC/zXDrPbDdVCYfeU0BsWO/8tqtlbgT2G9w84FoVxp7Z8VlIMCFlA2zs6SFz7JsDoeA3raAVGI/6ugLOpyypEBMs1OUIJqsil2D4kF501KKaU73yqWjgo

+ev+to51byrvLjKzg6CYG1a4XXvi3tPxq3smPi9WIsgtRqAEFQ8TmDn5XpNpaYbg==

-----ENDCERTIFICATE-----



Synopsis

TheremoteservicesupportstheuseofSSLCipherBlockChainingciphers,whichcombinepreviousblockswithsubsequentones.

Description

The remote host supports the use of SSL ciphers that operate in Cipher Block Chaining (CBC) mode.These cipher suites offer additional security over Electronic Codebook (ECB) mode, but have thepotentialtoleakinformationifusedimproperly.

SeeAlso

<https://www.openssl.org/docs/manmaster/man1/ciphers.html><http://www.nessus.org/u?cc4a822a><https://www.openssl.org/~bodo/tls-cbc.txt>

Solutionn/aRiskFactorNone

PluginInformation

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| HereisthelistofSSLCBCcipherssupported  :HighStrengthCiphers(>=112-bitkey)  Name Code | | by | theremote  KEX | server  Auth | Encryption | MAC |
| DHE-RSA-AES128-SHA | 0x00,  0x33  0x00,  0x39  0xC0,  0x13  0xC0,  0x14  0x00,  0x67 | DH | | RSA | AES-CBC(128) |  |
| SHA1 |  | |  |  |
| DHE-RSA-AES256-SHA | DH | | RSA | AES-CBC(256) |
| SHA1 |  | |  |  |
| ECDHE-RSA-AES128-SHA | ECDH | | RSA | AES-CBC(128) |
| SHA1 |  | |  |  |
| ECDHE-RSA-AES256-SHA | ECDH | | RSA | AES-CBC(256) |
| SHA1 |  | |  |  |
| DHE-RSA-AES128-SHA256 | DH | | RSA | AES-CBC(128) |
| SHA256 |  | |  |  |

Published:2013/10/22,Modified:2021/02/03PluginOutputtcp/443/www



Synopsis

TheremoteserviceencryptscommunicationsusingSSL.

Description

ThisplugindetectswhichSSLciphersaresupportedbytheremoteserviceforencryptingcommunications.

SeeAlso

<https://www.openssl.org/docs/man1.0.2/man1/ciphers.html><http://www.nessus.org/u?e17ffced>

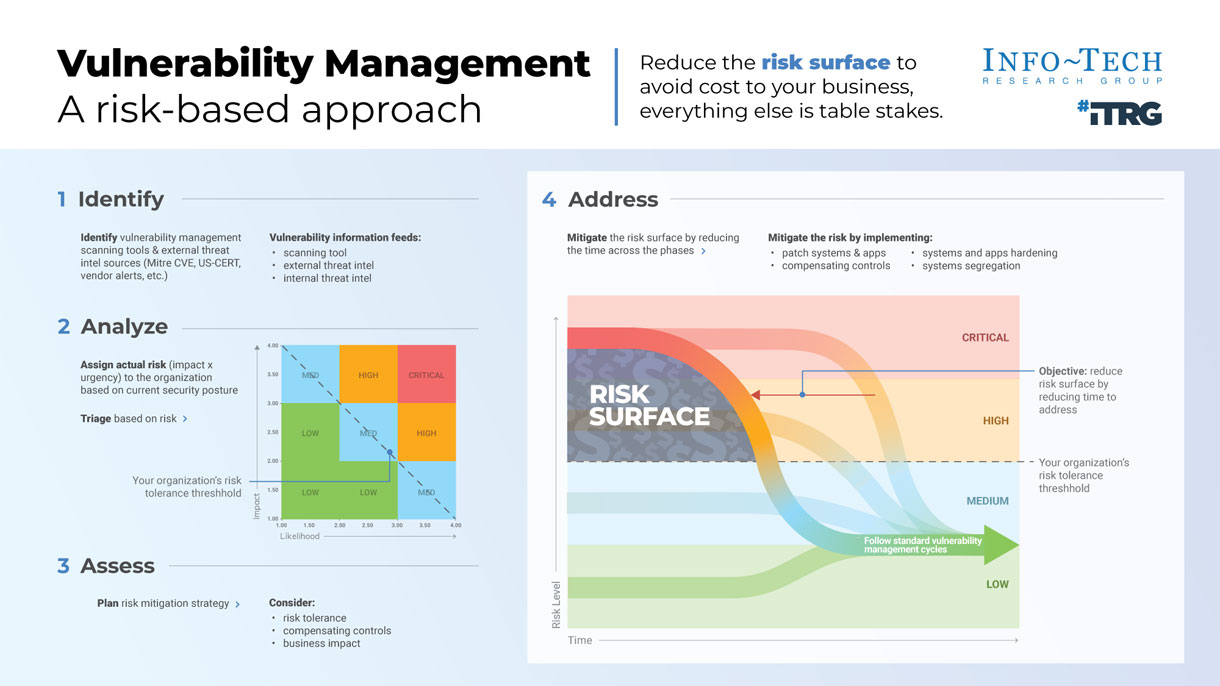
Solutionn/aRiskFactorNone

PluginInformation

Published:2006/06/05,Modified:2023/07/10

PluginOutputtcp/443/www

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| HereisthelistofSSLcipherssupported  :EachgroupisreportedperSSLVersion.  SSLVersion:TLSv12  HighStrengthCiphers(>=112-bitkey)  Name Code | | by | | the | remote  KEX | server | Auth | Encryption | MAC |
| DHE-RSA-AES128-SHA256  SHA256 | 0x00,  0x9E | | DH | | | RSA | | AES-GCM(128) |  |



**Vulnerability Management A risk-based approach**

**1 Identify :**

Identify vulnerability management scanning tools & external threat

intel sources (Mitre CVE, US-CERT, vendor alerts, etc.)

**2 Analyze :**

Assign actual risk (impact x urgency) to the organization based on current security posture

Triage based on risk >

Your organization's risk tolerance threshold

**3 Address**

Mitigate the risk surface by reducing the time across the phases >

INFO-TECH

RESEARCH GROUP



Synopsis

TheremoteservicesupportstheuseofSSLPerfectForwardSecrecyciphers,whichmaintainconfidentialityevenifthekeyisstolen.

Description

The remote host supports the use of SSL ciphers that offer Perfect Forward Secrecy (PFS) encryption.These cipher suites ensure that recorded SSL traffic cannot be broken at a future date if the server'sprivatekeyiscompromised.

SeeAlso

<https://www.openssl.org/docs/manmaster/man1/ciphers.html>

<https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange><https://en.wikipedia.org/wiki/Perfect_forward_secrecy>

Solutionn/aRiskFactorNone

PluginInformation

Published:2011/12/07,Modified:2021/03/09PluginOutputtcp/443/ww

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| HereisthelistofSSLPFScipherssupported  :HighStrengthCiphers(>=112-bitkey)  Name Code | | | by | theremote  KEX | server  Auth | Encryption | MAC |
| DHE-RSA-AES128-SHA256  SHA256  DHE-RSA-AES256-SHA384  SHA384  ECDHE-RSA-AES128-SHA256  SHA256  ECDHE-RSA-AES256-SHA384  SHA384  DHE-RSA-AES128-SHA  SHA1 | 0x00,  0x9E  0x00,  0x9F  0xC0,  0x2F  0xC0,  0x30  0x00,  0x33 | DH | | | RSA | AES-GCM(128) |  |
| DH | | | RSA | AES-GCM(256) |
| ECDH | | | RSA | AES-GCM(128) |
| ECDH | | | RSA | AES-GCM(256) |
| DH | | | RSA | AES-CBC(128) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DHE-RSA-AES256-SHA | 0x00, | 0x39 | DH | RSA | AES-CBC(256) |
| SHA1  ECDHE-RSA-AES128-SHA | 0xC0, | 0x13 | ECDH | RSA | AES-CBC(128) |
| SHA1  ECDHE-RSA-AES256-SHA | 0xC0, | 0x14 | ECDH | RSA | AES-CBC(256) |
| SHA1  DHE-RSA-AES128-SHA256 | 0x00, | 0x67 | DH | RSA | AES-CBC(128) |
| SHA256  DHE-RSA-AES256-SHA256 | 0x00, | 0x6B | DH | RSA | AES-CBC(256) |
| SHA256  ECDHE-RSA-AES128-SHA256 | 0xC0, | 0x27 | ECDH | RSA | AES-CBC(128) |
| SHA256  ECDHE-RSA-AES256-SHA384 | 0xC0, | 0x28 | ECDH | RSA | AES-CBC(256) |
| SHA384 |  |  |  |  |  |
| Thefieldsaboveare:  {Tenableciphername}  {CipherIDcode}Kex={keyexchange}Auth={authentication  }  Encrypt={symmetricencryptionmethod}MAC={messageauthenticationcode}  {exportflag} | | | | | |



Synopsis

ArootCertificationAuthoritycertificatewasfoundatthetopofthecertificatechain.

Description

TheremoteserviceusesanSSLcertificatechainthatcontainsaself-signedrootCertificationAuthoritycertificateatthetopofthechain.

SeeAlso

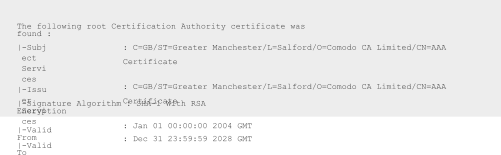
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v%3Dws.10))

Solution

EnsurethatuseofthisrootCertificationAuthoritycertificatecomplieswithyourorganization'sacceptableuseandsecuritypolicies.

Risk Factor NonePluginInformation

Published:2016/11/14,Modified:2018/11/15PluginOutputtcp/443/www



Synopsis

TheremotehostadvertisesdiscouragedSSL/TLSciphers.

Description

TheremotehosthasopenSSL/TLSportswhichadvertisediscouragedciphersuites.Itisrecommendedtoonlyenablesupportforthefollowingciphersuites:

TLSv1.3:

-0x13,0x01TLS13\_AES\_128\_GCM\_SHA256

-0x13,0x02TLS13\_AES\_256\_GCM\_SHA384

-0x13,0x03TLS13\_CHACHA20\_POLY1305\_SHA256

TLSv1.2:

* 0xC0,0x2BECDHE-ECDSA-AES128-GCM-SHA256
* 0xC0,0x2FECDHE-RSA-AES128-GCM-SHA256
* 0xC0,0x2CECDHE-ECDSA-AES256-GCM-SHA384
* 0xC0,0x30ECDHE-RSA-AES256-GCM-SHA384
* 0xCC,0xA9ECDHE-ECDSA-CHACHA20-POLY1305
* 0xCC,0xA8ECDHE-RSA-CHACHA20-POLY1305
* 0x00,0x9EDHE-RSA-AES128-GCM-SHA256
* 0x00,0x9FDHE-RSA-AES256-GCM-SHA384

Thisistherecommendedconfigurationforthevastmajorityofservices,asitishighlysecureandcompatiblewithnearlyeveryclientreleasedinthelastfive(ormore)years.

SeeAlso

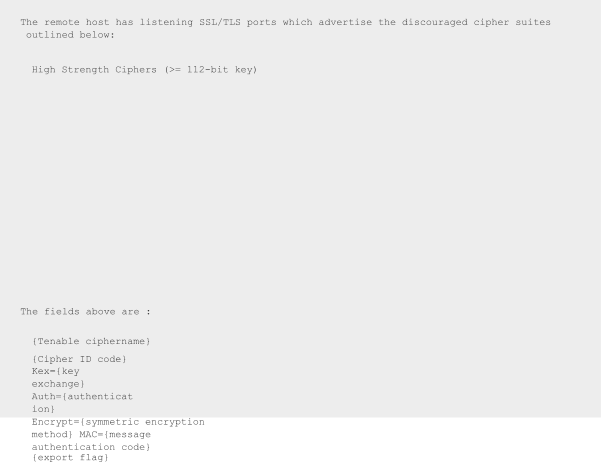
<https://wiki.mozilla.org/Security/Server_Side_TLS><https://ssl-config.mozilla.org/>

Solution

Onlyenablesupportforrecommenedciphersuites.RiskFactorNone

PluginInformation

Published:2022/01/20,Modified:2023/07/1

Plugin Outputtcp/443/www

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Code | KEX | Auth | Encryption | MAC |
| DHE-RSA-AES128-SHA  SHA1  DHE-RSA-AES256-SHA  SHA1  ECDHE-RSA-AES128-SHA  SHA1  ECDHE-RSA-AES256-SHA  SHA1  DHE-RSA-AES128-SHA256  SHA256  DHE-RSA-AES256-SHA256  SHA256  ECDHE-RSA-AES128-SHA256  SHA256  ECDHE-RSA-AES256-SHA384  SHA384 | 0x00,  0x33  0x00,  0x39  0xC0,  0x13  0xC0,  0x14  0x00,  0x67  0x00,  0x6B  0xC0,  0x27  0xC0,  0x28 | DH | RSA | AES-CBC(128) |  |
| DH | RSA | AES-CBC(256) |
| ECDH | RSA | AES-CBC(128) |
| ECDH | RSA | AES-CBC(256) |
| DH | RSA | AES-CBC(128) |
| DH | RSA | AES-CBC(256) |
| ECDH | RSA | AES-CBC(128) |
| ECDH | RSA | AES-CBC(256) |



Synopsis

Theremoteservicecouldbeidentified.

Description

NessuswasabletoidentifytheremoteservicebyitsbannerorbylookingattheerrormessageitsendswhenitreceivesanHTTPrequest.

Solutionn/a

RiskFactorNone

PluginInformation

Published:2007/08/19,Modified:2023/07/10PluginOutputtcp/443/www

tcp/443/www



Synopsis

TheremoteserviceencryptstrafficusingaversionofTLS.

Description

TheremoteserviceacceptsconnectionsencryptedusingTLS1.2.

See Also<https://tools.ietf.org/html/rfc5246>

Solution N/ARiskFactorNone

PluginInformation



Published:2020/05/04,Modified:2020/05/04PluginOutputtcp/443/www

Synopsis

Itwaspossibletoobtaintracerouteinformation.

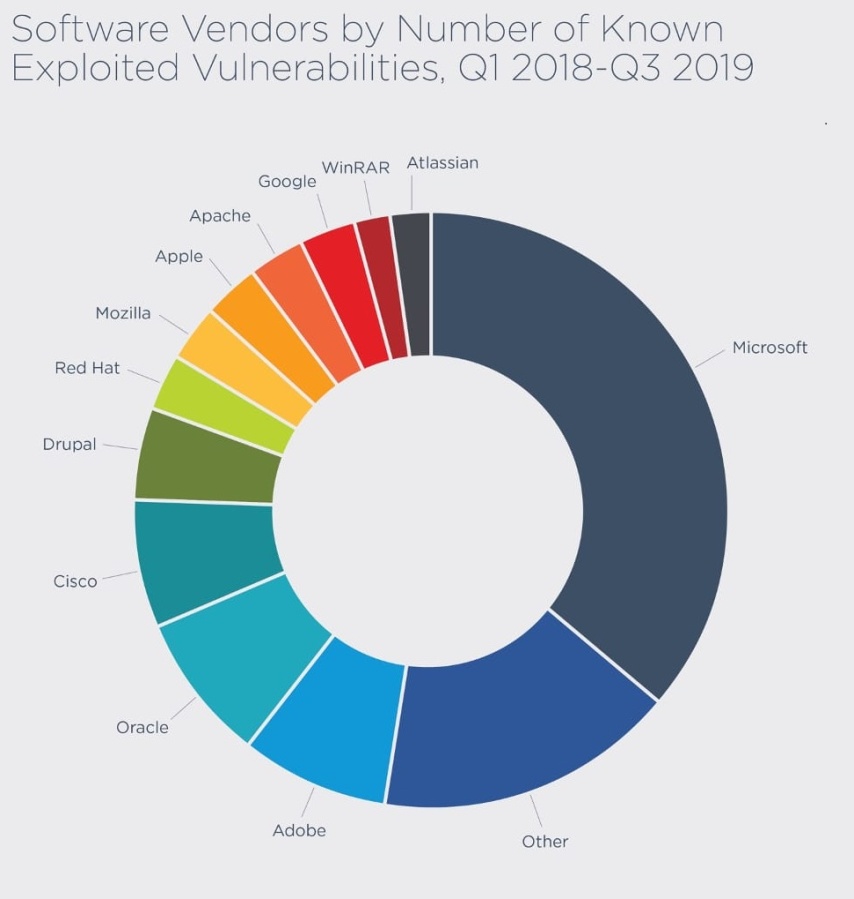
Description

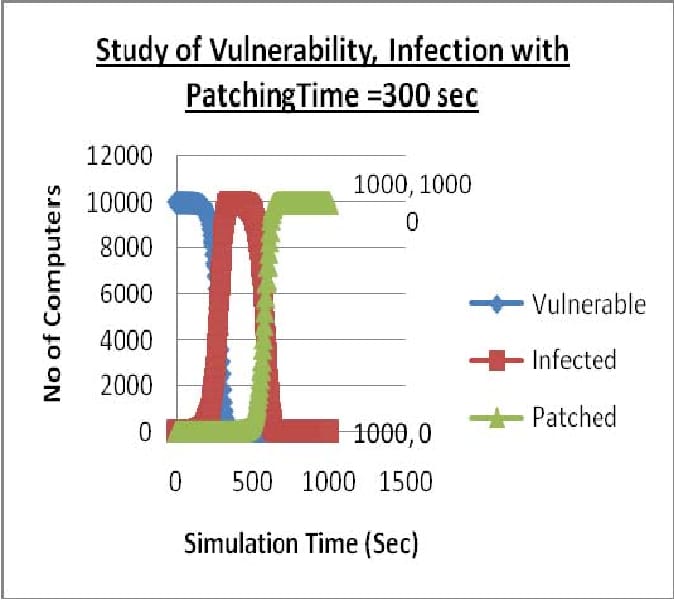
Makesatraceroutetotheremotehost.Solutionn/a

RiskFactorNone

PluginInformation

Published:1999/11/27,Modified:2023/06/26PluginOutputudp/0





### BusinessImpact

**PluginID:46180-AdditionalDNSHostnamesSynopsis:**

The Nessus vulnerability scan has detected potential virtual hosts with diﬀerent hostnames pointing to theremotehost

### Impact:

* + 1. ResourceAllocation
    2. SecurityImplications
    3. WebsiteReputationandTrust
    4. SearchEngineOptimization(SEO)

### RecommendedActions:

1. ReviewVirtualHostConﬁguration
2. MonitorResourceUsage
3. ImplementSecurityMeasures
4. MonitorWebsiteReputation
5. AddressSEOConcerns

### PluginID:45590-CommonPlatformEnumeration(CPE)Synopsis:

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

### Impact:

1. Vulnerability Identiﬁcation and Management
2. AssetInventoryandVisibility
3. RegulatoryCompliance

5.RiskAssessmentandMitigation

### RecommendedActions:

1. RegularScanningandEnumeration
2. PatchManagement
3. VulnerabilityMonitoring
4. AssetInventoryandLifecycleManagement
5. Compliance Reporting

### PluginID:45590-CommonPlatformEnumeration(CPE)Synopsis:

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

### Impact:

1. Vulnerability Identiﬁcation and Management
2. AssetInventoryandVisibility
3. RegulatoryCompliance
4. VendorSupportandUpdates
5. RiskAssessmentandMitigation

### RecommendedActions:

1. RegularScanningandEnumeration
2. PatchManagement
3. VulnerabilityMonitoring
4. AssetInventoryandLifecycleManagement
5. Compliance Reporting

### PluginID:54615-DeviceTypeSynopsis:

TheNessusscanhasidentiﬁedtheremotedevicetypebasedontheremoteoperatingsystem.

### Impact:

1. DeviceProﬁling
2. SecurityPolicyImplementation
3. NetworkVisibility
4. IncidentResponse
5. ChangeManagementandPatching

### RecommendedActions:

1. AccurateDeviceIdentiﬁcation
2. NetworkSegmentation
3. SecurityPolicyTuning
4. IncidentResponsePlanning

### PluginID:11219-NessusSYNscannerSynopsis:

TheNessusSYNscanneriscapableofdeterminingwhichTCPportsareopenonatargetsystem.

### Impact:

1. NetworkVisibility
2. VulnerabilityIdentiﬁcation
3. FirewallResilienceAssessment
4. NetworkLoadandPerformance

### RecommendedActions:

1. ResponsibleScanning
2. FirewallHardening
3. VulnerabilityRemediation
4. MonitoringandIncidentResponse

### PluginID:19506-NessusScanInformationSynopsis:

The plugin provides information about the Nessus scan, including details about the version ofthe plugin set, the type of scanner used the version of the Nessus Engine, the port scanner(s)employed,theportrangescanned,pingroundtriptime,patchmanagementchecks,displayofsuperseded patches, date of the scan, scan duration, number of hosts scanned in parallel, andnumberofchecksperformedinparallel.

### Impact:

1. ScanEﬀectiveness
2. NetworkResourceUtilization
3. PatchManagementandVulnerabilityAssessment
4. SecurityPostureEvaluation

### RecommendedActions:

1. ReviewScanConﬁguration
2. PatchManagement Improvement
3. RegularScanningandUpdates
4. NetworkMonitoring

### PluginID:11936-OSIdentiﬁcationSynopsis:

ThepluginperformsOSidentiﬁcationusingvariousremoteprobes,suchasTCP/IP,SMB,HTTP,NTP,SNMP,etc.

### Impact:

1. SystemProﬁling
2. Vulnerability Assessment
3. SecurityPostureEvaluation
4. NetworkHardening
5. ComplianceandRegulatoryRequirements:

### RecommendedActions:

1. AssetInventoryandDocumentation
2. PatchManagement
3. SecurityControlCustomization
4. NetworkSegmentation

### PluginID:56984-SSL/TLSVersionsSupportedSynopsis:

ThepluginisusedtodetectwhichSSLandTLSversionsaresupportedbytheremoteserviceforencryptingcommunications.

### Impact:

1. DataSecurity
2. ComplianceandIndustryStandards
3. Vulnerability Assessment
4. PublicTrustandReputation

### RecommendedActions:

1. TLSConﬁgurationReview
2. PatchandUpdateSSL/TLSLibraries
3. RegularSecurityAssessments
4. ComplianceAlignment

### PluginID:10863-SSLCertiﬁcateInformationSynopsis:

ThepluginconnectstoeverySSL-relatedportandattemptstoextractanddumptheX.509certiﬁcate.

### Impact:

1. CertiﬁcateValidityandTrustworthiness
2. MitigatingCertiﬁcate-RelatedRisks
3. TrustandUserConﬁdence
4. Vulnerability Assessment

### RecommendedActions:

1. CertiﬁcateMonitoring and Renewal
2. SSLConﬁgurationReview
3. CertiﬁcateTransparency
4. PublicKeyInfrastructure(PKI)Management

### PluginID:95631-SSLCertiﬁcateSignedUsingWeakHashingAlgorithm(KnownCA)Synopsis:

The plugin identiﬁes that the remote service uses a known Certiﬁcate Authority (CA) SSLcertiﬁcateinthecertiﬁcatechainthathasbeensignedusingacryptographicallyweakhashingalgorithm(e.g.,MD2,MD4,MD5,orSHA1).

### Impact:

1. TrustworthinessandIntegrity
2. DataPrivacyandConﬁdentiality
3. ComplianceandRegulatoryConcerns
4. BusinessReputation

### RecommendedActions:

1. CertiﬁcateReplacement
2. SSL/TLSConﬁgurationReview
3. CertiﬁcateLifecycleManagement
4. ComplianceAlignment

### PluginID:70544-SSLCipherBlockChainingCipherSuitesSupportedSynopsis:

ThepluginidentiﬁesthattheremoteservicesupportstheuseofSSLCipherBlockChaining(CBC)ciphers.CBCmodeisacryptographictechnique.

### Impact:

1. DataConﬁdentiality
2. VulnerabilitytoPaddingOracleAttacks
3. ComplianceandSecurityStandards
4. MitigationStrategies

### RecommendedActions:

1. SSL/TLSConﬁgurationReview
2. RegularSoftwareUpdates
3. Vulnerability Assessments
4. MonitoringandLogging

### PluginID:21643-SSLCipherSuitesSupportedSynopsis:

ThepluginidentiﬁesthattheremoteserviceencryptscommunicationsusingSSL.

### Impact:

1. DataConﬁdentiality
2. SecureCommunicationChannel
3. CompliancewithSecurityStandards

### RecommendedActions:

1. SSL/TLSConﬁgurationReview
2. RegularSoftwareUpdates
3. VulnerabilityAssessments
4. ComplianceValidation

### PluginID:57041-SSLPerfectForwardSecrecyCipherSuitesSupportedSynopsis:

ThepluginidentiﬁesthattheremoteservicesupportstheuseofSSLPerfectForwardSecrecy(PFS)ciphersuites.

### Impact:

1. DataConﬁdentiality
2. MitigationofFutureThreats
3. Complianceand Regulatory Requirements
4. ProtectionagainstForwardSecrecyAttacks

### RecommendedActions:

1. SSL/TLSConﬁgurationReview
2. RegularSoftwareUpdates
3. KeyManagementPractices
4. SecurityMonitoringandIncidentResponse

### PluginID:94761-SSLRootCertiﬁcationAuthorityCertiﬁcateInformationSynopsis:

ThepluginidentiﬁesthattheremoteserviceusesanSSLcertiﬁcatechaincontainingaself-signedrootCertiﬁcationAuthority(CA)certiﬁcateatthetopofthechain.

### Impact:

1. CertiﬁcateTrustandSecurity
2. LackofThird-partyValidation
3. ComplianceandRegulatoryConcerns
4. CertiﬁcateChainValidation

### RecommendedActions:

1. ObtainaTrustedRootCACertiﬁcate
2. CertiﬁcateLifecycleManagement
3. CertiﬁcateChainValidation
4. ComplianceandSecurityPolicyReview

### PluginID:156899-SSL/TLSRecommendedCipherSuitesSynopsis:

ThepluginidentiﬁesthattheremotehostadvertisesdiscouragedSSL/TLSciphersuites.

### Impact:

1. DataSecurity
2. Compatibility and Interoperability
3. TrustandReputation
4. CompliancewithSecurityStandards

### RecommendedActions:

1. SSL/TLSConﬁgurationReview
2. RegularSoftwareUpdates
3. VulnerabilityAssessments
4. TestingandMonitoring

### Plugin ID:22964 -Service DetectionSynopsis:

The plugin identiﬁes that the remote service could be identiﬁed based on its banner or the errormessageitsendswhenitreceivesanHTTPrequest.

### Impact:

1. SystemIdentiﬁcation
2. Vulnerability Assessment
3. AttackSurfaceEvaluation
4. SecurityConﬁgurationReview

### RecommendedActions:

1. ServiceHardening
2. PatchManagement
3. SecurityMonitoring
4. AccessControl

### PluginID:136318-TLSVersion1.2ProtocolDetectionSynopsis:

ThepluginidentiﬁesthattheremoteserviceencryptstraﬃcusingTLS1.2.

### Impact:

1. DataSecurity
2. CompliancewithSecurityStandards
3. TrustandReputation
4. Compatibility and Interoperability

### RecommendedActions:

1. TLSConﬁgurationReview
2. RegularSoftwareUpdates
3. VulnerabilityAssessments
4. SecurityAwarenessTraining

### PluginID:10287-TracerouteInformationSynopsis:

Thepluginindicatesthatitwaspossibletoobtaintracerouteinformationfromtheremotehost.

### Impact:

1. NetworkTopologyUnderstanding
2. NetworkPerformanceAssessment
3. SecurityImplications
4. PotentialMisconﬁgurationDetection

### RecommendedActions:

1. RegularNetworkMonitoring
2. AccessControl
3. NetworkSegmentation

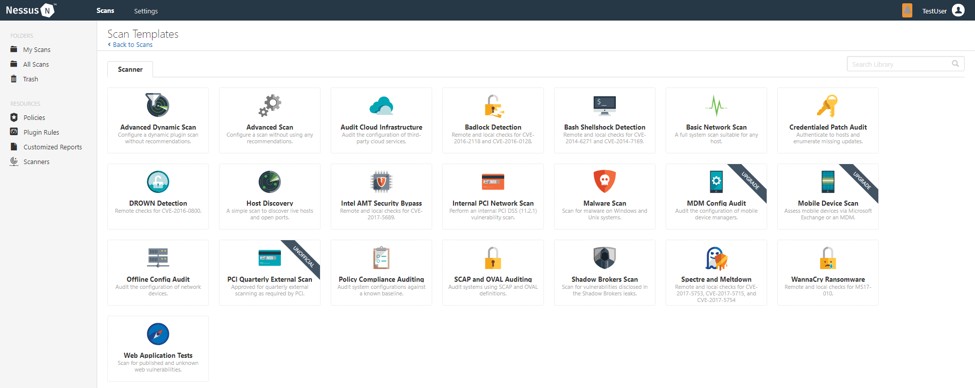
### Stepstoreproducethevulnerabilities

**Step 1: Creating a Scan**

OnceyouhaveinstalledandlaunchedNessus,you’rereadytostartscanning.First,youhavetocreateascan.Tocreateyourscan:

* Inthetopnavigationbar,clickScans.
* Intheupper-rightcorneroftheMyScanspage,clicktheNewScanbutton.

### Step2:ChooseaScanTemplate



Next,clickthescantemplateyouwanttouse.Scantemplatessimplifytheprocessbydeterminingwhich settings are conﬁgurable and how they can be set. For a detailed explanation of all theoptionsavailable,referto[ScanandPolicySettings](https://docs.tenable.com/nessus/8_2/Content/TemplateSettings.htm)intheNessusUserGuide.

A scan policy is a set of predeﬁned conﬁguration options related to performing a scan. After youcreateapolicy,youcanselectitasatemplateintheUserDeﬁnedtabwhenyoucreateascan.Formoreinformation,see[CreateaPolicy](https://docs.tenable.com/nessus/Content/CreateAPolicy.htm)intheNessusUserGuide.

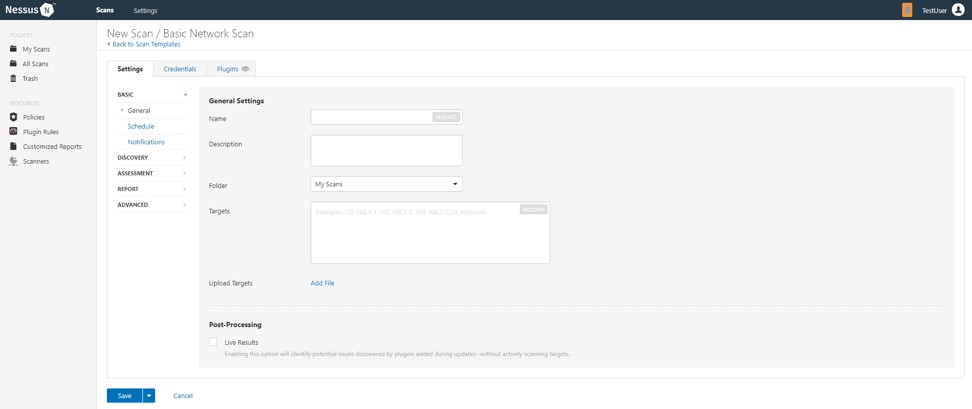
The Nessus interface provides brief explanations of each template in the product. Some templatesareonlyavailablewhenyoupurchaseafullylicensedcopyofNessusProfessional.

ToseeafulllistofthetypesoftemplatesavailableinNessus,see[ScanandPolicyTemplates](https://docs.tenable.com/nessus/Content/ScanAndPolicyTemplates.htm).ToquicklygetstartedwithNessus,usetheBasicNetworkScantemplate.

### Step3:ConﬁgureScanSettings

Prepare your scan by conﬁguring the [settings](https://docs.tenable.com/nessus/Content/ScanAndPolicyTemplates.htm) available for your chosen template. The BasicNetwork Scan template has several default settings preconﬁgured, which allows you to quicklyperformyourﬁrstscanandviewresultswithoutalotofeﬀort.

### Followthesestepstorunabasicscan:

1. **ConﬁgurethesettingsintheBasicSettingssection.**

### ThefollowingareBasicsettings:

|  |  |
| --- | --- |
| **Setting** | **Description** |
| **Name** | **Speciﬁesthenameofthescanorpolicy.ThisvalueisdisplayedontheNessusinterface.** |
| **Description** | **(Optional)Speciﬁesadescriptionofthescanorpolicy.** |
| **Folder** | **efolderwherethescanappearsafterbeingsaved.** |
| **Targets** | **Speciﬁesoneormoretargetstobescanned.Ifyouselecta target group or upload a targets ﬁle, you are notrequiredtospecifyadditionaltargets.** |

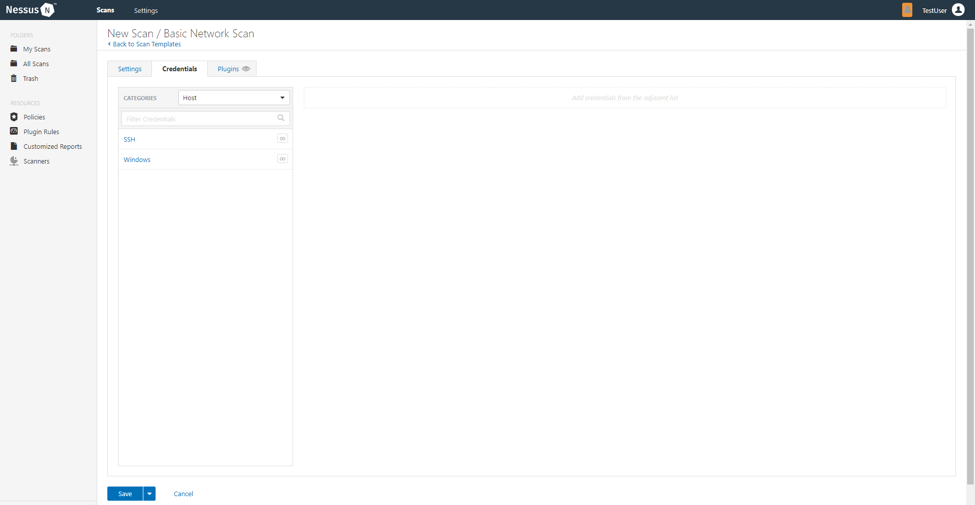
1. **Conﬁgureremainingsettings**

Although you can leave the remaining settings at their pre-conﬁgured default, Tenablerecommends reviewing the Discovery, Assessment, Report and Advanced settings to ensure theyareappropriateforyourenvironment**.**

### Formoreinformation,seethe[ScanSettings](https://docs.tenable.com/nessus/Content/TemplateSettings.htm)documentationintheNessusUserGuide.

1. **ConﬁgureCredentials**

Optionally, you can conﬁgure Credentials for a scan. This allows credentialed scans to run, whichcan provide much more complete results and a more thorough evaluation of the vulnerabilities inyourenvironment.



### LaunchScan

Afteryouhaveconﬁguredallyoursettings,youcaneitherclicktheSavebuttontolaunchthescanlater,orlaunchthescanimmediately.

Ifyouwanttolaunchthescanimmediately,clickthebutton,andthenclickLaunch.Launchingthescanwillalsosaveit.

Thetimeittakestocompleteascaninvolvesmanyfactors,suchasnetworkspeedandcongestion,sothescanmaytakesometimetorun.

### Step4:ViewingYourResults

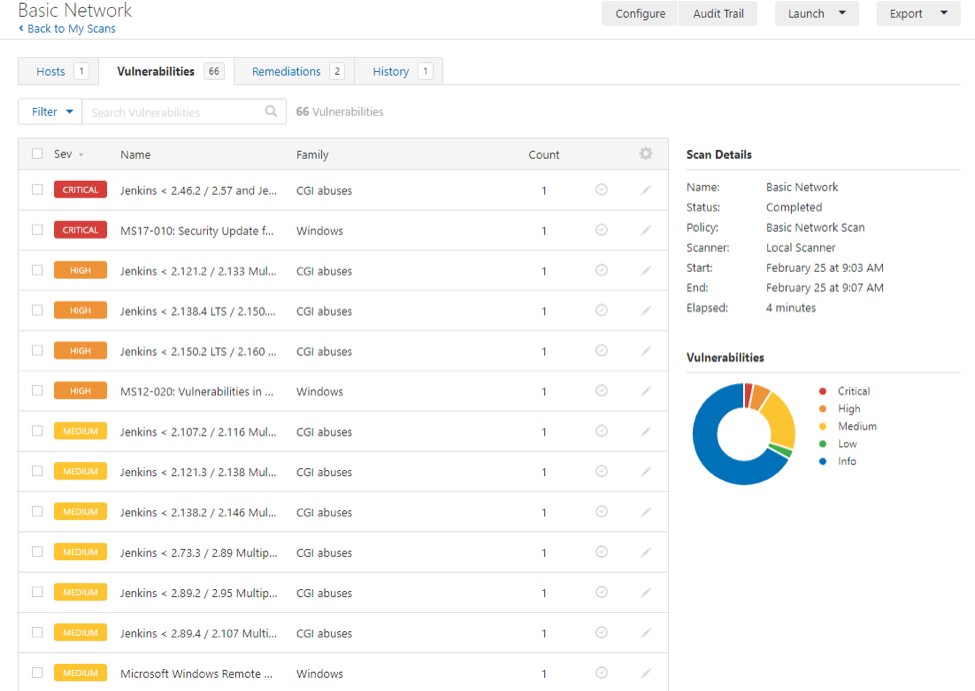
Viewing scan results can help you understand your organization’s security posture andvulnerabilities. Color-coded indicators and customizable viewing options allow you to tailor how youviewyourscan’sdata**.**

### Youcanviewscanresultsinoneofseveralviews:

|  |  |
| --- | --- |
| **Page** | **Description** |
| **Hosts** | **Displaysallscannedtargets.** |

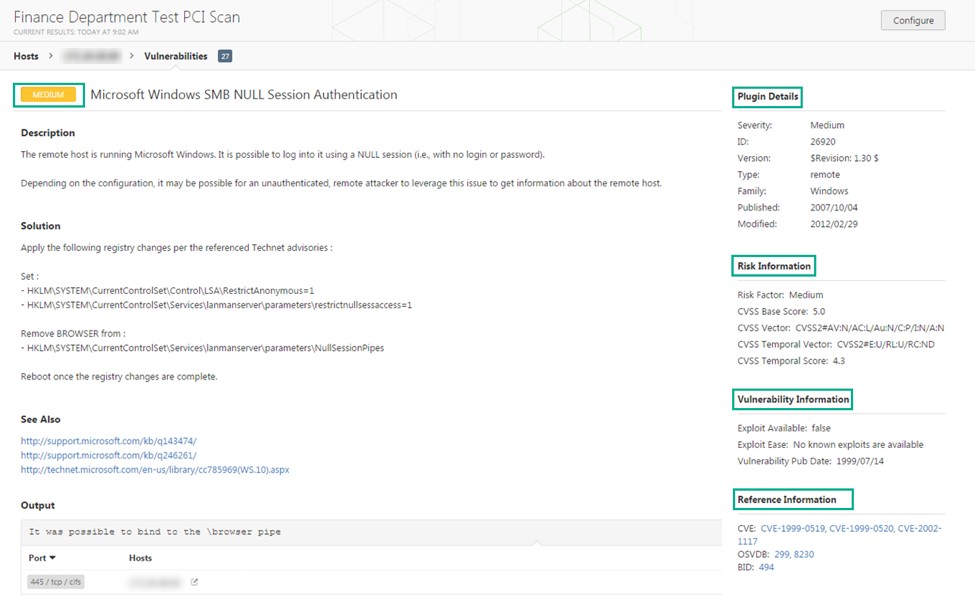
|  |  |
| --- | --- |
| **Vulnerabilities** | **Listofidentiﬁedvulnerabilities,sortedbyseverity.** |
| **Remediations** | **If the scan's results include remediationinformation, this list displays all remediationdetails, sorted bythe numberof vulnerabilities.** |
| **Notes** | **Displays additional information about the scan andthescan’sresults.** |
| **History** | **Displaysalistofscans:StartTime,EndTime,andtheScanStatuses.** |

**Viewingscanresultsbyvulnerabilitiesgivesyouaviewintopotentialrisksonyourassets.**



### Toviewvulnerabilities:

* 1. Inthetopnavigationbar,clickScans.
  2. Clickthescanforwhichyouwanttoviewresults.
  3. Dooneofthefollowing:
     + Clickaspeciﬁchosttoviewvulnerabilitiesfoundonthathost.
     + ClicktheVulnerabilitiestabtoviewallvulnerabilities.
  4. (Optional)Tosortthevulnerabilities,clickanattributeinthetableheaderrowtosortbythatattribute.
  5. Clickingonthevulnerabilityrowwillopenthevulnerabilitydetailspage,displayingplugininformationandoutputforeachinstanceonahost.



### Step5:ReportingYourResults

Chancesareyourjobisn’tdoneyet.Youneedtoreportyourﬁndingstoyourteam.

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 purposeofeach,seethe[NessusUserGuide](https://docs.tenable.com/nessus/8_2/Content/ScanReportFormats.htm).

ToExportaScanReport:

1. Startfromascan'sresultspage
2. Intheupper-rightcorner,clickExport.
3. Fromthedrop-downbox,selecttheformatinwhichyouwanttoexportthescanresults.
4. ClickExporttodownloadthereport.

### Conclusion

The network vulnerability assessment on the "altoroMutual" system conducted using NessusEssentials reveals several vulnerabilities that need attention. Here is a summary of the keyﬁndings:

### TLSVersion1.0ProtocolDetection(VulnerabilityID:104743):

The remote service supports TLS version 1.0, which is considered outdated and has knowncryptographic design ﬂaws. Modern implementations of TLS 1.2 and 1.3 are recommended tomitigatethesevulnerabilities.TLS1.0shouldbedisabledtoenhancesecurityandcomplywithindustrystandards.

### AdditionalDNSHostnames(VulnerabilityID:46180):

The Nessus scan detected additional DNS hostnames pointing to the remote host. It is importanttoverifythesehostnamestoensuretheyarelegitimateanddonotposesecurityrisks.

### CommonPlatformEnumeration(CPE)(VulnerabilityID:45590):

The Nessus scan enumerated CPE names that match the remote system. Understanding the CPEinformation can help in identifying potential vulnerabilities associated with hardware andsoftwareproductsonthehost.

### DeviceType(VulnerabilityID:54615):

TheNessusscaninferredtheremotedevicetypeasa"ﬁrewall"basedontheremoteoperatingsystem information. This helps to identify the nature of the system but does not indicate avulnerability.

### NessusSYNScanner(VulnerabilityID:11219):

TheNessusscandetectedopenTCPportsontheremotehostusingSYNscanning.Whilethisinformation can be useful for legitimate purposes, it should be monitored to prevent anypotentialmisuse.

### NessusScanInformation(VulnerabilityID:19506):

Details about the Nessus scan, including the version of the plugin set, the scanner edition, andthe scan duration, were provided. This information helps in understanding the scan results anditsconﬁguration.

### OSIdentiﬁcation(VulnerabilityID:11936):

TheNessusscanidentiﬁedtheremoteoperatingsystemas"CISCOPIX7.0"usingremoteprobes.Whilethisinformationishelpfulforsystemadministrators,itdoesnotindicateanysecurityrisks.

### 8.SSL/TLSVulnerabilities(VulnerabilityIDs:56984,95631,70544,10863,21643,94761,

**156899):**

VariousSSL/TLS-relatedvulnerabilitiesweredetected,includingweakhashingalgorithmusage,known CA SSL certiﬁcate usage, support for SSL Cipher Block Chaining, and support fordiscouraged SSL/TLS cipher suites. These vulnerabilities can potentially compromise theconﬁdentialityandintegrityofencryptedcommunications.

### Recommendations:

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

1. DisableTLSversion1.0andenablesupportforTLS1.2and1.3toenhanceencryptionsecurityandcomplywithindustrystandards.
2. InvestigateandverifytheadditionalDNShostnamestoensurethattheyarelegitimateanddonotposesecurityrisks.
3. Monitor the open TCP ports identiﬁed by the Nessus SYN scanner to prevent any potentialsecurityissuesorunauthorizedaccess.
4. Review and understand the CPE information to identify any potential vulnerabilities associatedwithhardwareandsoftwareproductsonthehost.
5. AddressSSL/TLS-relatedvulnerabilities,suchasreplacingcertiﬁcatessignedwithweakhashing algorithms, verifying root Certiﬁcation Authority certiﬁcates, and enablingrecommendedciphersuites.
6. Regularly update and patch the system to address any known vulnerabilities and improveoverallsecurity.
7. Implement propernetworksecuritycontrols,includingﬁrewallsandintrusiondetection/preventionsystems,toprotectagainstpotentialthreats.

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 protectionagainstpotentialthreats.