iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.52554

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Identification of Network Vulnerabilities through IISRA Framework

Keerti Dixit[1], Dr. Umesh Kumar Singh[2], Dr. Bhupendra Kumar Pandya[3]
Institute of Computer Science, Vikram University, Ujjain

Abstract: ***As the globe transitions to complicated networks and as we move towards digitization, its worth is rising daily. Working in an organization across a network and the internet creates vulnerabilities. As is well known, data is a crucial component of every organization and must be safeguarded from threats. The attackers' job is to try and take advantage of the networks by using these weaknesses. When organizations use the Internet, intranets, and related technologies more frequently, system security becomes one of the key considerations. Network security protects computer systems from unauthorized threats and breaches, which lowers the likelihood that confidential information may be stolen. The organization will feel more secure if these vulnerabilities are closed up in the systems and network well in advance of an attack. The availability of numerous technologies for network vulnerability assessment enables organizations to thwart potential attacks. In this research paper, we have developed an Integrated Information Security Risk Assessment (IISRA) Framework for identification of Network Vulnerabilities. We have implemented this IISRA Framework on real computing environment of an organization.***
Keywords: Network Vulnerabilities, Risk, Threat, Impact.

I. INTRODUCTION

The internet is the method that people use the most frequently in the twenty-first century to collect information and data. The main purpose of the internet is to convey information from one node to another through a network. The development of computer networks, mobile devices, and other technologies has significantly increased internet usage. For efficient data distribution, the Internet is a global network of millions of uniquely interconnected computers, networks, and related devices. These data, which were moved from one machine to another, contain extremely sensitive information that must be safeguarded. Cybercriminals are attracted to the internet because of this sudden rise in usage and the significant volume of important data being transferred from one computer to another [1]. [2].

When an unauthorized person, programme, or illegal infiltration enters a computer or network with the intention of doing harm or interfering with the usual course of business, the integrity and security of the computer system are put at risk. ICT (information and communication technology) has significantly improved governance effectiveness and ease for people. The trend of cyberattacks has moved from small-scale intrusion attempts and financial breaches to highly organized state-sponsored operations due to the growing reliance on ICT and sophistication of attack tactics [3].

These cyberattacks prompted the development of cyber security and its defenses against damaging cyberattacks [4]. The human factor is one of the main causes of the success of many cyberattacks since the untrained computer user is the weakest link that social engineering by cybercriminals targets.

To reduce the likelihood that computer hackers and attackers would take advantage of human weaknesses, formal cyber security awareness is necessary [5, 6].

Cybersecurity is a collection of security methods that can be used to safeguard user assets and the internet from intrusion and attack. From this vantage point, it is obvious that cybercriminals have a strong propensity to attack any database that includes important data that could expose that specific database. Additionally, all fields and areas of human endeavor are now the targets of cyberattackers who want to invade their privacy, break into their systems, gather crucial data, and make it accessible to the general public [7-9]. Fighting these cyber security threats and keeping up with their increasing speed is becoming more and more difficult [10-15].

II. IISRA FRAMEWORK FOR NETWORK VULNERABILITIES IDENTIFICATION

We have developed an Integrated Information Security Risk Assessment (IISRA) Framework for identification of Network vulnerabilities. IISRA Framework helps in identifying and assessing potential security vulnerabilities of network.

©IJRASET: All Rights are Reserved



Fig 1: IISRA Framework for Network Vulnerability Identification

The process of IISRA network vulnerability identification involves the following steps:

1) *Preparation:* Before starting the identification, it is important to prepare the network and the vulnerability scanning tool. This may involve installing and configuring the vulnerability scanning tool, determining the scope of the scan (e.g., which systems and devices will be included), and ensuring that the necessary permissions and access controls are in place.
2) *Scan Configuration:* This involves setting up the vulnerability scanning tool and configuring it to scan the desired network assets. The scan configuration may include specifying the IP address range to be scanned, the types of vulnerabilities to be searched for, and the level of detail to be included in the scan results.
3) *Scan Initiation:* This involves starting the vulnerability scan, which typically involves sending packets to the target systems and analyzing the responses to identify potential vulnerabilities
4) *Scan Progress Monitoring:* This involves monitoring the progress of the scan to ensure that it is running as expected and to identify any issues that may impact the accuracy of the scan results.
5) *Scan Results Analysis:* This involves reviewing the results of the vulnerability scan to identify the potential security risks to the network. The results are typically displayed in a report that includes information about each identified vulnerability, including its severity, the potential impact of exploitation, and recommended remediation steps.
6) *False Positive Verification:* This involves verifying that the vulnerabilities identified by the scan are actual security weaknesses and not false positives, which are inaccuracies in the scan results that do not represent actual vulnerabilities.
7) *Risk Prioritization:* This involves prioritizing the vulnerabilities based on their potential impact and likelihood of exploitation, and determining the appropriate response for each vulnerability, such as patching, mitigating, or accepting the risk.
8) *Remediation:* This involves implementing the recommended remediation steps for each vulnerability, such as applying patches, modifying access controls, or deploying security controls to mitigate the risk.

It is important to perform regular vulnerability scans to ensure that the network remains secure and to identify new vulnerabilities as they emerge. The results of the vulnerability scan should be combined with the results of other assessment methods, such as manual review and penetration testing, to provide a complete view of the network's security posture.

III. RESULTS AND REMEDIATION PLAN

We have implemented IISRA Framework in the real scenario of an organization to assess the Network vulnerabilities of that organization. We have identified total 94 assets in the organization [ ].

Table 1: Assets of the Organization

Network Device	Server	Workstation	WIFI controller
2	8	83	1

Below table illustrates distribution of observations of Network vulnerabilities identification based on the risk categorization i.e., Critical, High, Medium, and Low.

1) Network Devices

Table 2: Risk Assessment result of Network Devices

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	0	2	5	1	8

2) Servers

Table 3: Risk Assessment result of Servers

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	4	2	7	1	14

3) Workstations

Table 4: Risk Assessment result of Workstations

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	3	4	9	2	18

4) WIFI Controller

Table 5: Risk Assessment result of WIFI Controller

Domain	Critical	High	Medium	Low	Total
Vulnerability Assessment	1	1	4	2	8

Table 6: Network Device Risk Assessment and Mitigation Plan through IISRA Framework

Vulnerabilities	Impact	Risk	Observations	Recommendations
SSL Certificate Signed Using Weak Hashing Algorithm	This can be used by an attacker to create a new certificate with the identical digital signature, giving them the ability to pretend to be the affected Service.	High	It has been observed that SSL certificate is signed using SHA-1With RSA Encryption.	It is recommended to sign SSL certificate using strong encryption algorithm such as SHA-512.
Unencrypted Telnet Server	This enables a remote man-in-the-middle attacker to eavesdrop in on a Telnet session to intercept traffic between a client and server and intercept credentials or other sensitive information.	High	It has been observed that remote host is using unencrypted telnet services. Since telnet is being used inside the secured network hence it has least impact.	It is recommended to disable the Telnet service and use SSH instead.

Internet Key Exchange (IKE) Aggressive Mode with Pre- Shared Key	Aggressive Mode with Pre-Shared Key (PSK) authentication appears to be supported by the remote Internet Key Exchange (IKE) version 1 service. A VPN gateway's PSK could be captured and cracked using such a configuration, giving an attacker unauthorized access to private networks.	Medium	It has been Observed that remote host supports aggressive mode with pre-shared key (PSK).	It is recommended to disable Aggressive Mode if supported. Do not use Pre- Shared key for authentication if it's possible. If using Pre-Shared key cannot be avoided, use very strong keys. If possible, do not allow VPN connections from any IP addresses.
TLS Version 1.1 Protocol Deprecated	TLS 1.1 does not permit the usage of ciphers that support encryption prior to MAC computation or authorized encryption modes like GCM. Hence, a man-in-the-middle attack on the remote host is possible.	Medium	It has been observed that Remote host supports TLS version 1.1.	It is recommended to enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
SSL Certificate Cannot Be Trusted	Any interruption in the chain makes it more difficult for users to confirm the authenticity and identity of the web server if the remote host is a public host in production. This might make man-in-the-middle attacks against the remote host simpler to execute.	Medium	It has been observed that remote host is using untrusted SSL certificate.	It is recommended to purchase or generate a proper SSL certificate for this service.
JQuery 1.2 < 3.5.0 Multiple XSS	Cross-site scripting attacks can be carried out in a variety of ways by an attacker.	Medium	It has been observed that remote host is running on outdated jQuery version.	It is recommended to upgrade to jQuery version 3.5.0 or later.
IP Forwarding Enabled	An attacker can use this to evade some firewalls, routers, and NAC filtering by routing packets through the host.	Medium	It has been observed that IP forwarding is enabled on remote hosts.	It is recommended to disable the IP Forwarding.
SSH Weak Key Exchange Algorithms Enabled	Attackers can quickly take advantage of a remote SSH server that is set up to support weak key exchange algorithms.	Low	It has been observed that remote host allow weak key exchange algorithms. The following are weak key exchange algorithms that are enabled: diffie-hellman- group-exchange- sha1 diffie-hellman- group1-sha1	It is recommended to disable the weak key exchange algorithms.

Table 7: Server Risk Assessment and Mitigation Plan through IISRA Framework

Vulnerabilities	Impact	Risk	Observations	Recommendations
Apache 2.4.x< 2.4.53 Multiple Vulnerabilities	The remote host's installation of Apache HTTP Daemon is version 2.4.46, which has a number of vulnerabilities. A carefully constructed request body could result in a read to a random region of memory, which might result in a process crash. When problems are discovered, it neglects to terminate the inbound connection, discarding the request body and leaving the server vulnerable to HTTP Request Smuggling Acknowledgements	Critical	It has been observed that the remote host is using older Apache version	It is recommended to upgrade the Apache version to 2.4.53 or above.
Microsoft SQL Server Unsupported Version Detection	The remote Windows host's Microsoft SQL Server is no longer maintained and is likely to have security vulnerabilities that an attacker could exploit.	Critical	It has been Observed that Microsoft SQL Server on the remote host is no longer supported.	It is recommended to upgrade to Microsoft SQL Server 2019 (15.x).
SSL Version 2 and 3 Protocol Detection	Man-in-the-middle attacks or the decryption of client-to-affected service communications are also options for an attacker.	Critical	It has been observed that devices are using SSL version 2.0 and 3.0.	It is recommended to disable SSL 2.0 and 3.0. Use TLS 1.2 with higher cipher suites listed below.
Unsupported Web Server Detection	Absence of support suggests that the vendor won't provide any new security updates for the product. Thus, it can have security vulnerabilities.	Critical	It has been observed that remote web server is obsolete /unsupported.	It is recommended to upgrade to a supported version if possible or switch to another server.
SSL Certificate Signed Using Weak Hashing Algorithm	This can be used by an attacker to create a new certificate with the identical digital signature, giving them the ability to pretend to be the affected Service.	High	It has been observed that SSL certificate is signed using SHA-1 With RSA Encryption.	It is recommended to sign SSL certificate using strong encryption algorithm such as SHA-512.
SSL Medium Strength Cipher Suites Supported (SWEET32)	The attacker would find it much simpler to get around medium strength encryption if they were on the same physical network as the remote host, which supports the use of SSL ciphers that provide it.	High	It has been observed that SSL is using medium strength encryption such as DES-CBC3-SHA which can be easily compromised if the attacker is on the same physical network.	It is recommended to reconfigure the affected application if possible to avoid use of medium strength ciphers.

HTTP TRACE /TRACK Methods Allowed	With an XmlHttpRequest, the attacker is reading cookies using the TRACE/TRACK method of cross-site scripting. Modern browsers are unable to accomplish this, hence the vulnerability can only be used to target users of outdated and unpatched browsers.	Medium	It is observed the vulnerability can only be used when targeting users with unpatched and old browsers.	It is recommended to disable these HTTP methods.
SMB Signing not enabled	This can be used by a remote, unauthenticated attacker to launch man-in-the-middle attacks against the SMB server.	Medium	It has been observed that remote host is not signing SMB Server.	It is recommended to enable signing is on the remote SMB server. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'.
SSL Certificate Cannot Be Trusted	Any interruption in the chain makes it more difficult for users to confirm the authenticity and identity of the web server if the remote host is a public host in production. This might make man-in-the-middle attacks against the remote host simpler to execute.	Medium	It has been observed that remote host is using untrusted SSL certificate.	It is recommended to purchase or generate a proper SSL certificate for this service.
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	An attacker may be able to deduce the plaintext if the plaintext is repeatedly encrypted (for example, in HTTP cookies) and the attacker can access a large number of ciphertexts (tens of millions).	Medium	It has been observed that remote host is using weak cipher suite such as RC4-MD5-128bit and RC4-SHA1-128bit.	It is recommended to reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE)	A man-in-the-middle (MitM) information disclosure technique called POODLE can be used by an attacker. If a MitM attacker is successful in getting a target application to repeatedly send the same data over freshly formed SSL 3.0 connections, they may be able to decrypt a particular byte of a cypher text in as few as 256 attempts.	Medium	It has been observed that the remote host is vulnerable to padding oracle attack.	It is recommended to disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Terminal Services Doesn't Use Network Level Authentication (NLA) Only	In order to achieve robust server authentication through TLS/SSL or Kerberos protocols, NLA uses the Credential Security Support Provider (CredSSP) protocol. This protocol helps prevent man-in-the-middle attacks, but if it is not configured correctly, an attacker may use it to their advantage.	Medium	It has been observed that services don't use only for Network Level Authentication (NLA).	It is recommended to enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
TLS Version 1.1 Protocol Deprecated	TLS 1.1 does not permit the usage of cyphers that support encryption prior to MAC computation or authorised encryption modes like GCM. Hence, a man-in-the-middle attack on the remote host is possible.	Medium	It has been Observed that Remote host supports TLS version 1.1.	It is recommended to enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	A brute force attack can readily be used to break an encryption with a key size less than 2048 bits.	Low	It has been observed that 2048-bit RSA key provides 112-bit of security.	It is recommended to replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Table 8: Workstation Risk Assessment and Mitigation Plan through IISRA Framework

Vulnerabilities	Impact	Risk	Observations	Recommendations
Apache 2.4.x< 2.4.53 Multiple Vulnerabilities	The remote host's installation of Apache HTTP Daemon is version 2.4.46, which has a number of vulnerabilities. A carefully constructed request body could result in a read to a random region of memory, which might result in a process crash. When problems are discovered, it neglects to terminate the inbound connection, discarding the request body and leaving the server vulnerable to HTTP Request Smuggling Acknowledgements.	Critical	It has been observed that the remote host is using older Apache version	It is recommended to upgrade the Apache version to 2.4.53 or above.

Microsoft SQL Server Unsupported Version Detection (remote check)	The remote Windows host's Microsoft SQL Server is no longer maintained and is likely to have security vulnerabilities that an attacker could exploit.	Critical	It has been Observed that Microsoft SQL Server on the remote host is no longer supported.	It is recommended to upgrade to Microsoft SQL Server 2019 (15.x).
SSL Version 2 and 3 Protocol Detection	Man-in-the-middle attacks or the decryption of client-to-affected service communications are also options for an attacker.	Critical	It has been observed that devices are using SSL version 2.0 and 3.0.	It is recommended to disable SSL 2.0 and 3.0. Use TLS 1.2 with higher cipher suites.
SSL Medium Strength Cipher Suites Supported (SWEET32)	The attacker would find it much simpler to get around medium strength encryption if they were on the same physical network as the remote host, which supports the use of SSL ciphers that provide it.	High	It has been observed that SSL is using medium strength encryption such as DES-CBC3- SHA which can be easily compromised if the attacker is on the same physical network.	It is recommended to reconfigure the affected application if possible to avoid use of medium strength ciphers.
SNMP Agent Default Community Name (public)	The remote system's configuration could be altered by an attacker. if such alterations are allowed by the default community.	High	It has been observed that Remote host SNMP Agent Using default community name that is “Public”	It is recommended to disable the SNMP service on the remote host if you do not use it. Either filter incoming UDP packets going to this port, or change the default community string.
SSL Certificate Signed Using Weak Hashing Algorithm	This can be used by an attacker to create a new certificate with the identical digital signature, giving them the ability to pretend to be the affected Service.	High	It has been observed that SSL certificate is signed using SHA-1 With RSA Encryption.	It is recommended to sign SSL certificate using strong encryption algorithm such as SHA-512.
Unencrypted Telnet Server	This enables a remote man-in-the-middle attacker to eavesdrop in on a Telnet session to intercept traffic between a client and server and intercept credentials or other sensitive information.	High	It has been Observed that remote host is using unencrypted telnet services. Since telnet is being used inside the secured network hence it has least impact.	It is recommended to disable the Telnet service and use SSH instead.

©IJRASET: All Rights are Reserved

SMB Signing not enabled	This can be used by a remote, unauthenticated attacker to launch man-in-the-middle attacks against the SMB server.	Medium	It has been observed that remote host is not signing SMB Server.	It is recommended to enable signing is on the remote SMB server. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'.
SSL Certificate Cannot Be Trusted	Any interruption in the chain makes it more difficult for users to confirm the authenticity and identity of the web server if the remote host is a public host in production. This might make man-in-the-middle attacks against the remote host simpler to execute.	Medium	It has been observed that remote host is using untrusted SSL certificate.	It is recommended to purchase or generate a proper SSL certificate for this service.
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	An attacker may be able to deduce the plaintext if the plaintext is repeatedly encrypted (for example, in HTTP cookies) and the attacker can access a large number of ciphertexts (tens of millions).	Medium	It has been observed that remote host is using weak cipher suite such as RC4-MD5-128bit and RC4-SHA1-128bit.	It is recommended to reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.
SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE)	A man-in-the-middle (MitM) information disclosure technique called POODLE can be used by an attacker. If a MitM attacker is successful in getting a target application to repeatedly send the same data over freshly formed SSL 3.0 connections, they may be able to decrypt a particular byte of a cypher text in as few as 256 attempts.	Medium	It has been observed that the remote host is vulnerable to padding oracle attack.	It is recommended to disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.
JQuery 1.2 < 3.5.0 Multiple XSS	Cross-site scripting attacks can be carried out in a variety of ways by an attacker.	Medium	It has been observed that remote host is running on outdated jQuery version.	It is recommended to upgrade to jQuery version 3.5.0 or later.

IP Forwarding Enabled	An attacker can use this to evade some firewalls, routers, and NAC filtering by routing packets through the host.	Medium	It has been observed that IP forwarding is enabled on remote hosts.	It is recommended to disable the IP Forwarding.
HTTP TRACE /TRACK Methods Allowed	With an XmlHttpRequest, the attacker is reading cookies using the TRACE/TRACK method of cross-site scripting. Modern browsers are unable to accomplish this, hence the vulnerability can only be used to target users of outdated and unpatched browsers.	Medium	It is observed the vulnerability can only be used when targeting users with unpatched and old browsers.	It is recommended to disable these HTTP methods.
Terminal Services Doesn't Use Network Level Authentication (NLA) Only	In order to achieve robust server authentication through TLS/SSL or Kerberos protocols, NLA uses the Credential Security Support Provider (CredSSP) protocol. This protocol helps prevent man-in-the-middle attacks, but if it is not configured correctly, an attacker may use it to their advantage.	Medium	It has been observed that services don't use only for Network Level Authentication (NLA).	It is recommended to enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
TLS Version 1.1 Protocol Deprecated	TLS 1.1 does not permit the usage of cyphers that support encryption prior to MAC computation or authorised encryption modes like GCM. Hence, a man-in-the-middle attack on the remote host is possible.	Medium	It has been Observed that Remote host supports TLS version 1.1.	It is recommended to enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
SSH Weak Key Exchange Algorithms Enabled	Attackers can quickly take advantage of a remote SSH server that is set up to support weak key exchange algorithms.	Low	It has been observed that Remote host allow weak key exchange algorithms. The following are weak key exchange algorithms that are enabled: diffie-hellman- group-exchange-sha1	It is recommended to disable the weak key exchange algorithms.

			diffie-hellman-group1-sha1	
SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	A brute force attack can readily be used to break an encryption with a key size less than 2048 bits.	Low	It has been observed that 2048-bit RSA key provides 112-bit of security.	It is recommended to replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Table 9: WIFI Controller Risk Assessment and Mitigation Plan through IISRA Framework

Vulnerabilities	Impact	Risk	Observations	Recommendations
SSL Version 2 and 3 Protocol Detection	Man-in-the-middle attacks or the decryption of client-to-affected service communications are also options for an attacker.	Critical	It has been observed that devices are using SSL version 2.0 and 3.0.	It is recommended to disable SSL 2.0 and 3.0. Use TLS 1.2 with higher cipher suites.
SSL Medium Strength Cipher Suites Supported (SWEET32)	The attacker would find it much simpler to get around medium strength encryption if they were on the same physical network as the remote host, which supports the use of SSL ciphers that provide it.	High	It has been observed that SSL is using medium strength encryption such as DES-CBC3- SHA which can be easily compromised if the attacker is on the same physical network.	It is recommended to reconfigure the affected application if possible to avoid use of medium strength ciphers.
TLS Version 1.1 Protocol Deprecated	TLS 1.1 does not permit the usage of cyphers that support encryption prior to MAC computation or authorised encryption modes like GCM. Hence, a man-in-the-middle attack on the remote host is possible.	Medium	It has been Observed that Remote host supports TLS version 1.1.	It is recommended to enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.
SSL RC4 Cipher Suites Supported (Bar Mitzvah)	An attacker may be able to deduce the plaintext if the plaintext is repeatedly encrypted (for example, in HTTP cookies) and the attacker can access a large number of ciphertexts (tens of millions).	Medium	It has been observed that remote host is using weak cipher suite such as RC4-MD5-128bit and RC4-SHA1-128bit.	It is recommended to reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

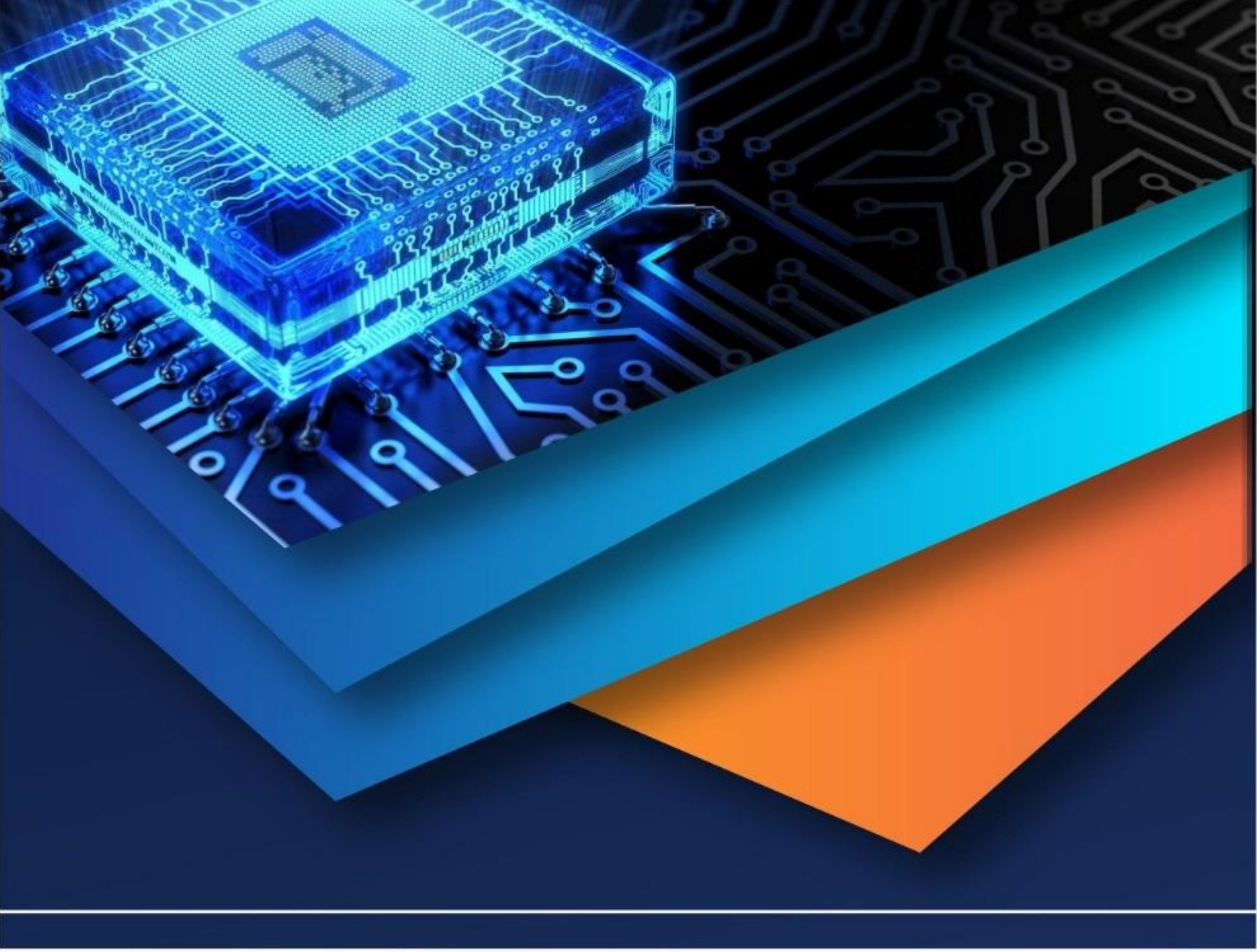
SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE)	A man-in-the-middle (MitM) information disclosure technique called POODLE can be used by an attacker. If a MitM attacker is successful in getting a target application to repeatedly send the same data over freshly formed SSL 3.0 connections, they may be able to decrypt a particular byte of a cypher text in as few as 256 attempts.	Medium	It has been observed that the remote host is vulnerable to padding oracle attack.	It is recommended to disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.
SSL Certificate Cannot Be Trusted	Any interruption in the chain makes it more difficult for users to confirm the authenticity and identity of the web server if the remote host is a public host in production. This might make man-in-the-middle attacks against the remote host simpler to execute.	Medium	It has been observed that remote host is using untrusted SSL certificate.	It is recommended to purchase or generate a proper SSL certificate for this service.
SSH Server CBC Mode Ciphers Enabled	Cipher Block Chaining (CBC) encryption is supported by the SSH server's configuration. An attacker might then be able to extract the plaintext from the ciphertext.	Low	It has been observed that remote host is using CBC Mode Cipher. The following Cipher Block Chaining (CBC) algorithms are supported: 3des-cbc aes128-cbc aes256-cbc	It is recommended to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.
SSH Weak Key Exchange Algorithms Enabled	Attackers can quickly take advantage of a remote SSH server that is set up to support weak key exchange algorithms.	Low	It has been observed that Remote host allow weak key exchange algorithms. The following are weak key exchange algorithms that are enabled: diffie-hellman- group-exchange-sha1 diffie-hellman-group1-sha1	It is recommended to disable the weak key exchange algorithms.

IV. CONCLUSION

In this Research paper, we have developed an Integrated Information Security Risk Assessment (IISRA) Framework for network vulnerabilities identification. We have assessed network vulnerabilities of an organization through IISRA framework. For the network vulnerability assessment, we have categorized assets in four categories: Network devices, servers, workstations and WIFI controller. We have observed that these devices are vulnerable to various network related security issues as on date tasted. We found that these devices has eight critical, nine high, twenty five medium and six low network risk vulnerability.

REFERENCES

[1] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," IEEE Access, vol. 8, pp. 222310– 222354, 2020, doi: 10.1109/ACCESS.2020.3041951.
[2] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber security in New Space: Analysis of threats, key enabling technologies and challenges," Int J Inf Secur, vol. 20, no. 3, pp. 287–311, Jun. 2021, doi: 10.1007/s10207- 020-00503-w.
[3] N. Shafqat and A. Masood, "Comparative Analysis of Various National Cyber Security Strategies," 2016. [Online]. Available: https://sites.google.com/site/ijcsis /
[4] M. Z. Gunduz and R. Das, "Cybersecurity on smart grid: Threats and potential solutions," Computer Networks, vol. 169, Mar. 2020, doi: 10.1016/j.comnet.2019.107094.
[5] M. D. Richardson, P. A. Lemoine, W. E. Stephens, and R. E. Waller, "Educational Planning," 2020.
[6] D. Craigen, N. Diakun-Thibault, and R. Purse, "Technology Innovation Management Review Defining Cybersecurity," 2014. [Online]. Available: www.timreview.ca.
[7] D. Ghelani, Diptiben Ghelani., "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review," American Journal of Science, Engineering and Technology, vol. 3, no. 6, pp. 12–19, 2022, doi: 10.22541/au.166385207.73483369 /v1.
[8] D. Schatz, R. Bashroush, and J. Wall, "Towards a More Representative Definition of Cyber Security," The Journal of Digital Forensics, Security and Law, 2017, doi: 10.15394/jdfsl.2017.1476.
[9] S. P.S, N. S, and S. M, "Overview of Cyber Security," IJARCCE, vol. 7, no. 11, pp. 125–128, Nov. 2018, doi: 10.17148/ijarcce.2018.71127.
[10] Keerti Dixit, "Information Security Risk Assessment in Higher Educational Institutions-Issues and Challenges" presented in 36th M.P. Young Scientist Congress, March 23 - 26, 2021
[11] K. Dixit, U. K. Singh, B. K. Pandya, "Comparative Framework for Information Security Risk Assessment Model", ICCIDS-2022 International Conference on Computational and Intelligent Data Science(Elsevier) 21 May 2022.
[12] K. Dixit, U. K. Singh, B. K. Pandya, "Threat and Asset Identification through IISRA Framework", International Journal of Creative Research Thought (IJCRT), Vol. 11, Issue 4, Apr. 2023.
[13] K. Dixit, U. K. Singh, B. K. Pandya, "Identification of Web Vulnerabilities through IISRA Framework", International Journal of Novel Research and Development (IJNRD), Vol. 8, Issue 5, May 2023.
[14] K. Dixit, U. K. Singh, B. K. Pandya, "Comparative study of Information Security Risk Assessment Model", International Journal of Computer Application (IJCA), Vol. 185, No. 7, May 2023.
[15] K. Dixit, U. K. Singh, B. K. Pandya, "An Integrated Information Security Risk Assessment (IISRA) Approach" presented in 2nd International Conference on Data Science and Artificial Intelligence ICDSAI 2023, California State University USA and Lendi Institute of Engineering and Technology, Apr. 24-25, 2023.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)