JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Comprehensive Approach to Mitigating Network Vulnerabilities: Threats, Risks, and Security Strategies

Sarvesh Thukrul[1], Suyash Patil[2]
Guide:- Asst.prof.Gauri Ansurkar
Keraleeya Samajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra

Network system weaknesses threaten the security of digital infrastructure systems to a dangerous extent. Security professionals must recognize and address all network vulnerabilities since they represent major cybersecurity risks. The research describes Vulnerability Hunter as an innovative automated system which finds and groups network-based vulnerabilities in corporate networks. The combination of machine learning algorithms and deep packet inspection with anomaly detection functions makes Vulnerability Hunter a strong platform for detecting security vulnerabilities effectively. This paper details the development process of Vulnerability Hunter accompanied by its developed methodology and practical framework deployment as well as its effectiveness evaluation within different real-world situations. Keywords: Network vulnerability, Cybersecurity, Anomaly Detection, Machine Learning, Deep Packet Inspection, Vulnerability Detection Framework .

The word "cyber" is used to describe networks with infrastructure information systems , also referred to as "virtual reality". Cyber security protects the security, integrity, and confidentiality of communication, life, integration, tangible or intangible assets, and data in an electronic environment established by institutions, organizations, and individuals in information systems.

Keywords

Cyber security, Network security, security, vulnerabilities, risks, mitigation strategies, Security awareness

1. Introduction

1.1 What is network vulnerability?

User-approved network infrastructure expansion has created enormous opportunities for attackers to threaten systems. The existence of network weaknesses enables intruders to gain unauthorized system access and enables breaches that result in disruption to services along with massive system failures. The security

methods which use firewalls alongside intrusion detection systems (IDS) lack the ability to spot new and complicated network vulnerabilities. The purpose of Vulnerability Hunter is to resolve current gaps by employing modern functionalities of anomaly detection along with deep packet inspection through machine learning for real-time network vulnerability identification.

This research document examines Vulnerability Hunter framework while explaining its framework design together with its components and its proven capability to identify and protect network vulnerabilities for improved system security..

1.2 Various Systems to check for vulnerabilities

In the realm of cybersecurity, vulnerability detection and management are critical. Existing tools for vulnerability detection include:

Intrusion Detection Systems (IDS): These systems identify malicious activities in a network by analyzing network traffic. They are effective but often rely on predefined signatures and rules, which may not detect zero-day vulnerabilities or advanced persistent threats.

Vulnerability Scanners: Tools such as Nessus and OpenVAS scan networks for known vulnerabilities. However, these tools can only identify known weaknesses and are often time-consuming and prone to false positives.

Anomaly Detection Systems: Some modern tools focus on recognizing network traffic patterns that deviate from the norm. While promising, anomaly detection is often challenged by high rates of false positives and may struggle with complex network environments.

The novelty of Vulnerability Hunter lies in its integration of anomaly detection, deep packet inspection, and machine learning, offering a more adaptive and robust solution compared to traditional approaches".

2. Common vulnerability

2.1 Weak Authentication and Credential Exploitation

Poor password policies and weak authentication mechanisms allow attackers to gain unauthorized access through brute-force attacks, credential stuffing, and phishing.

2.2 Misconfigured Network Devices

Improper configurations in routers, firewalls, and servers can expose networks to security risks. Examples include open ports, default credentials, and poorly set access controls.

2.3 Unpatched Software and Firmware

Outdated operating systems, network devices, and applications contain known vulnerabilities that attackers can exploit. Organizations failing to apply security patches leave their systems exposed.

2.4 Insecure Communication Channels

Unencrypted data transmission via insecure protocols (e.g., HTTP, Telnet, and FTP) allows attackers to intercept sensitive information through man-in-the-middle (MITM) attacks.

2.5 Insider Threats

Employees with malicious intent or negligence may expose a network to risks, whether by leaking confidential data or falling victim to social engineering attacks.

3. What are the problems in Network

Security tools exist but organizations lack effective methods to precisely detect and forecast network-based vulnerabilities during active use. Security methods used today commonly respond to existing attack habits while failing to discover emerging threats. Detecting vulnerabilities continues to pose difficulties because of the challenge to achieve optimal threat detection while avoiding either too many false alarms or any critical alerts. An automated system needs development to detect network vulnerabilities because it should integrate modern techniques while maintaining scalability and intelligence.

Recent research has explored the integration of machine learning techniques with deep packet inspection (DPI) to enhance network vulnerability detection and anomaly detection. DPI involves examining the content of data packets transmitted over a network, allowing for detailed traffic analysis and the identification of malicious activities.[1]

A comprehensive survey on machine learning in network anomaly detection highlights the challenges of traditional detection approaches and emphasizes the flexibility of machine learning methods. The survey reviews various implementations of machine learning techniques in both traditional and next-generation networks, underscoring their applicability across diverse network structures. [2]

4. Threats, Vulnerabilities, Exploits, and Attacks

This part of the study extensively discusses widely known cyber threats, security risks, vulnerabilities, and attacks. First, viruses, Trojans, worms, rootkits, and hackers are examined as cyber threats. Then, known threats such as spyware, scareware, joke programs, and ransomware are explained. Next, security vulnerabilities and primarily used vulnerability scanning tools are presented. Finally, the most common types of attacks, from social engineering attacks to applications, cryptography, hijacking, computer networks, phishing, malware, bots, and botnets, as well as password and man-in-the-middle attacks, are discussed in detail. Recommendations, precautions, and awareness for each type of attack are also included.

research on the vulnerability assessment of machine learning-based network anomaly detection systems examines potential weaknesses in these systems. The study assesses how adversaries might exploit machine learning models and discusses strategies to enhance the robustness of these detection systems against such threats.[3]

5. how to mitigate these Vulnerabilities

5.1 Implementing Strong Authentication Mechanisms Enforce complex password policies.
Enable multi-factor authentication (MFA).
Regularly rotate credentials and use password managers.
5.2 Securing Network Configurations Close unnecessary ports and disable default accounts.
Use network segmentation and strict access controls. Regularly audit firewall and router settings.
5.3 Patch Management and Software Updates
Deploy security patches and firmware updates promptly. Automate updates to reduce human oversight.
Conduct vulnerability assessments regularly.
5.4 Encrypting Network Communications Enforce HTTPS, TLS, and VPNs for secure data transmission. Disable outdated protocols such as SSL, Telnet, and FTP. Implement endpoint encryption to protect data at rest and in transit.
5.5 Strengthening Insider Threat Defenses Conduct cybersecurity awareness training for employees. Implement role-based access controls (RBAC).
Monitor privileged user activities. Establishing Robust Network Policies and Monitoring
Define clear security policies and enforce compliance. Utilize intrusion detection and security information and event management (SIEM) systems. Conduct regular network penetration testing and audits.

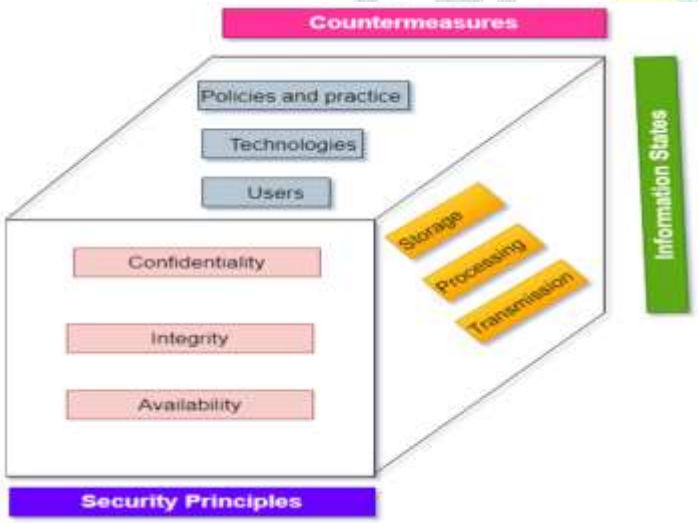


Fig:- Three dimensions of security
The above figure illustrates the three dimensions of cyber security. The first dimension is focused on protecting information from attackers, also known as the "principle of information security." This principle includes the concepts of confidentiality, integrity, and availability (CIA)[4]

Methodology

This research paper combines qualitative and quantitative analysis both to learn if peoples are aware of Deepfake Technology, From Positive Applications to Malicious Exploits. We can analyse and draw a conclusion from people's responses on a public survey.

Public Survey

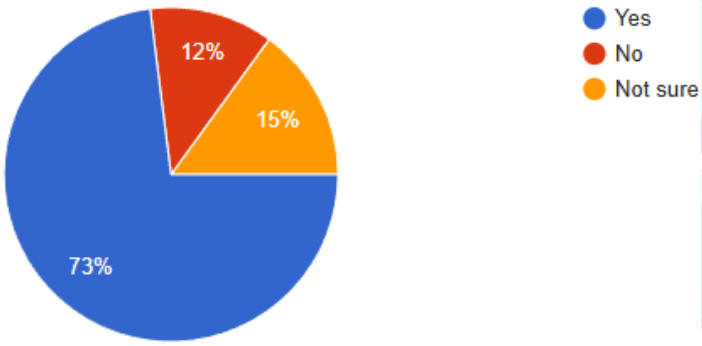
The survey is used to gather the data. Boththe outcome and the process by which it wasarrived at will be examined. In this instance, 100 people were asked their opinions about their awareness Deepfake Technology, and its Positive Applications also Malicious Exploits Conducting a survey isessential to obtaining reliable data that can be analyzed and used to determine the survey's outcome.

Questionnaire

1. Have you heard of the term "network vulnerability"?
2. Do you know that hackers can exploit network vulnerabilities to steal personal data?
3. Do you use antivirus software or any security applications on your devices?
4. Have you ever experienced a security issue such as hacking, phishing, or identity theft till now
5. Do you use strong passwords (a mix of letters, numbers, and symbols) for your important accounts ?
6. How often do you update your passwords?
7. Are you aware that public Wi-Fi can be unsafe and may expose your data to hackers?
8. Have you ever received suspicious emails or messages asking for personal information (phishing attempts)?

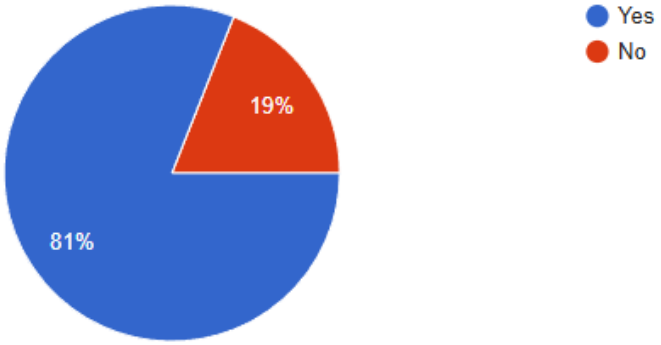
Results

1. Have you heard of the term "network vulnerability"?



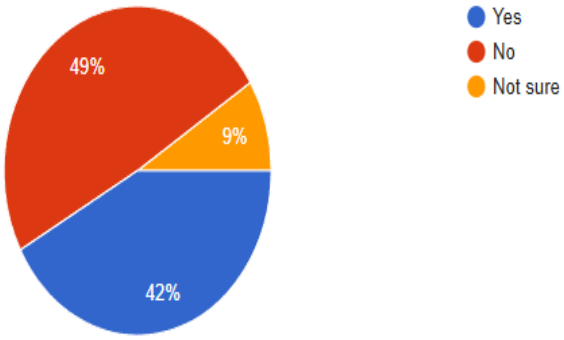
When people were asked how familiar they were with concept "network vulnerability" 73% said they were familiar with the term network vulnerability, 12% said no they were not familiar with the term network vulnerability and 15% said they are not sure.

2. Do you know that hackers can exploit network vulnerabilities to steal personal data?



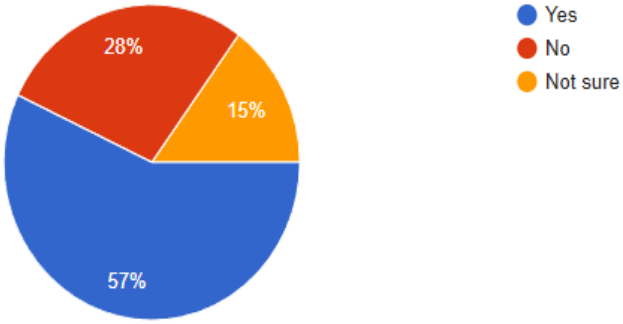
When people were asked if they know that hackers can exploit network vulnerabilities to steal personal data 81% answered with yes they were aware of it and 19% said no they were not aware of it.

3. Do you use antivirus software or any security applications on your devices?



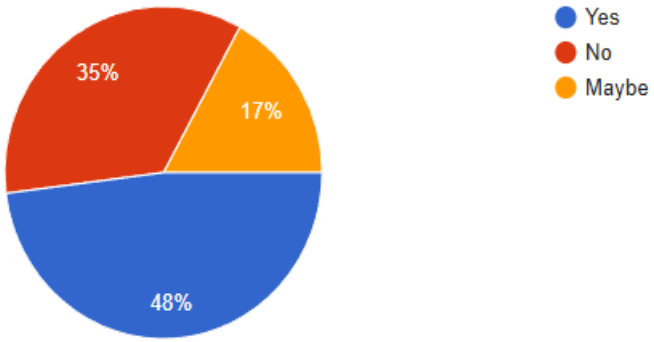
When people were asked about any antivirus software they use any antivirus software or security application 49% said no they don't use any software, 42% said yes they use security application and 9%
Said not sure.

4. Have you ever experienced a security issue such as hacking, phishing, or identity theft till now ?



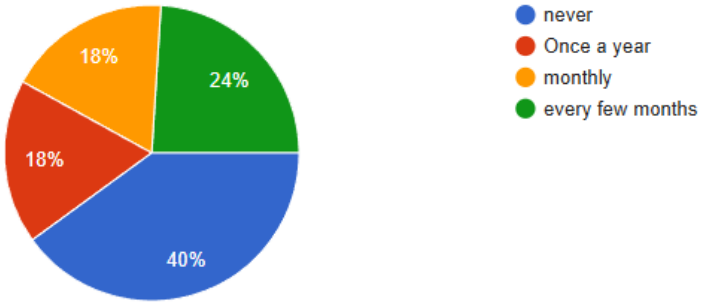
When people were asked about ever experienced a security issue such as hacking, phishing, or identity theft till now 57% people said yes they have experienced such issues, 28% said no they haven't had any such issues, 15% said not sure about such issues.

5. Do you use strong passwords (a mix of letters, numbers, and symbols) for your important accounts ?



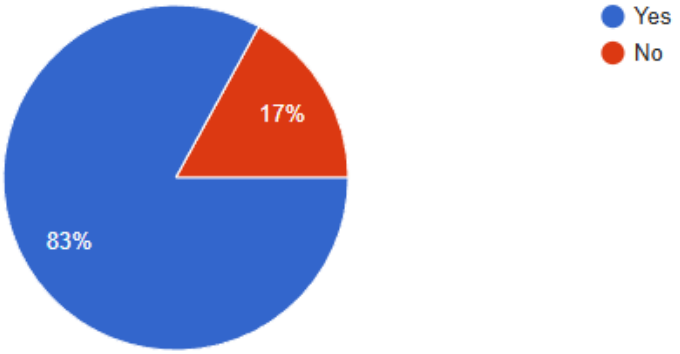
When people were asked about use strong passwords
48% people said yes they use strong passwords, 35% people said no they don't use complex passwords, 17% people weren't aware if their password is strong or not.

6. How often do you update your passwords?



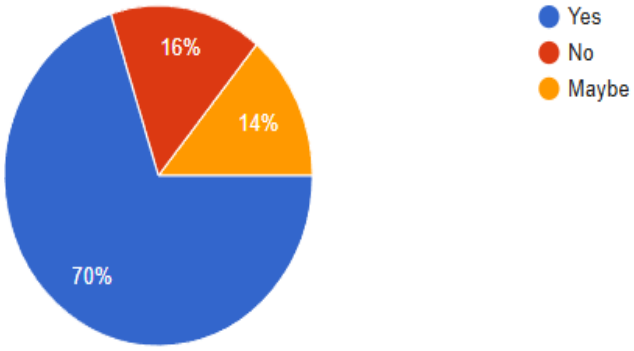
When people were asked about how often they update their passwords on online accounts 40% people said they never update their password, 18% people said they update their password once a year, 18% people said they update their password monthly and 24% people said they update their password every few months.

7. Are you aware that public Wi-Fi can be unsafe and may expose your data to hackers?



When people were asked about if they were aware of that the public wifi can be unsafe and can leak the data to hackers 83% of the people said yes they were aware of the fact while 17% people said no they were not aware of the fact that public wifi can be dangerous.

8. Have you ever received suspicious emails or messages asking for personal information (phishing attempts)?



When people were asked about receiving suspicious emails or messages asking their personal information for some activities that seems legitimate 70% people said yes they received such emails or messages while 16% people said no they didn't receive such emails or messages and rest of the 14% people said Maybe they got such emails or messages but they were not so sure about it.

Hypothesis testing

Hypothesis testing is a sort of statistical reasoning that includes analyzing data from a sample to derive inferences about a population parameter or probability distribution. First, a hypothesis is created regarding the parameter or distribution. This is known as the null hypothesis, abbreviated as H0. After that, an alternative hypothesis (denoted Ha) is defined, which is the polar opposite of the null hypothesis. Using sample data, the hypothesistesting technique determines whether or not H0 may be rejected. The statistical conclusion is that the alternative hypothesis Ha is true if H0 is rejected. For this paper, Null hypothesis

(H0): Peoples are concerned about effects of 5G network radiation. Alternative hypothesis (Ha): Peoples are not concerned about effects of 5G network radiation.

TEST (STATISTICS) There are many tests available to determine if the null hypothesis is to be rejected or not. Some are: 1. Chi-squared test 2. T-student test (T-test) 3. Fisher's Z test. For this paper, we will be using Chi-Squared Test Pearson's chi-square test is a statistical test for categorical data. It is used to determine whether your data are significantly different from what you expected. Level of significance - (Also known as alpha or α). A significance level of 0.05, for example, means there's a 5% probability of discovering a difference when there isn't one. Lower significance levels indicate that more evidence is required to reject the null hypothesis. Level of confidence The confidence level indicates the probability that the location of a statistical parameter (such as the arithmetic mean) measured in a sample survey is also true for the entire population.

Sr.no	Name	Grade
1	Anish	Concerned
2	Mayank	Not Concerned
3	Surya	Concerned
4	Rohit	Concerned
5	Vinish	Not Concerned
6	Dinesh	Concerned
7	Apurva	Concerned
8	Vedang	Not Concerned
9	Prachi	Concerned
10	Riya	Concerned
11	Ganesh	Concerned
12	Manasi	Not Concerned
13	Suyash	Concerned
14	Chetan	Concerned
15	Vighnesh	Concerned
16	Janhavi	Concerned
17	Nishant	Concerned
18	Kshipra	Concerned
19	Ruchika	Not Concerned
20	Mugdha	Concerned

	Concerned	Not Concerned	Total
Male	8.00	3.00	11
Female	7.00	2.00	9
Total	15.00	5.00	20
Ei	8.25	6.75	15

Level of significance = 0.09 i.e., confidence =96%

The chance of accepting the null hypothesis in achi- squared test depends on the chosen significance level and whether the calculated Chi-value is more than or equal to that significance level. Then we can reject the alternative hypothesis and conclude that
5G network radiation have bad impact onenvironment

Step 1: Determine what the null andalternative hypothesis are-

Null hypothesis (H0): The Vulnerability detection system present today does not significantly improve the detection and mitigation of network vulnerabilities compared to traditional security methods.
(Ha): The Vulnerability detection system significantly improves the detection and mitigation of network vulnerabilities compared to traditional security methods.

Step 2: Find the test statistic - Calculating Eivalue-

To Calculating Ei= Row total*Column
Total/Grand Total 9*15/20=6.75, 9*5/20=2.25
11*15/20=8.25, 11*5/20=2.25

Step 3- Calculating Σ(Oi-Ei2)/Ei-

$\Sigma (7-6.75)^2/6.75= 0.009259$

$\Sigma (2-2.25)^2/2.25= 0.027778$

$\Sigma (8-8.25)^2/8.25= 0.007576$

$\Sigma (3-2.75)^2/2.25= 0.027778$

Step 4-To Calculate Chi Squared value

The formula Is =CHIINV (0.06,2)
Where 0.05 is the level of significance and 2 isthe degree of freedom (3-1) *(2-1) =2 CHIINV(0.06,2) = 0.968112086

Since this Chi Squared-value is greater than our chosen alpha level of 0.05, we can accept the nullhypothesis. Thus, we have sufficient evidence to say that The Vulnerability detection system present today does not significantly improve the detection and mitigation of network vulnerabilities compared to traditional security methods.

Findings

Majority of the audience surveyed has felt network vulnerabilities in their day to day lives.

Audience was concerned with their safety when using internet also they were concerned about their data being stolen.

Conclusion

In conclusion Audience was concerned about their privacy and data being stolen and misused. To stop these attempts majority o the audience was using some Anti virus software or vulnerability detector software in their day to day lives.

Reference

1. https://www.researchgate.net/publication/384542254_Deep_Packet_Inspection_Model_Based_on_Support_Vector_Machine_for_Anomaly_Detection_in_Local_Area_Networks

2. https://ieeexplore.ieee.org/document/9610045

3. https://ieeexplore.ieee.org/document/9258068

4. https://www.mdpi.com/2188484