International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

HACKING ON NETWORK SECURITY

A1: KAVYA R

M.C.A.STUDENT, DAYANANDA SAGAR COLLEGE OF ENGINEERING

A2: Dr VIBHA M B

ASST.PROF, DEPT OF MCA, DAYANANDA SAGAR COLLEGE OF ENGINEERING

***Abstract*— Network security is one of the most important issues to consider and one of the most invested factors in an organization [1]. With the advancement of technology in society, the need for wireless and wired networks has become essential. Its advantages and disadvantages after security. Wireless networks take into the range, mobility, and various types of hardware components required to build a wireless network. Wired networks have different hardware requirements and are different in scope and benefits. This article covers different types of articles, network configurations, and security and attack prevention measures that must be taken to keep your network safe.**

***Keywords*— Network Domain, Wireless Network, WEP, WPA, Wired network**

I. INTRODUCTION

Networks, specially the Internet, have already turn out to be a platform that helps no longer best high-pace information message, however additionally effective allotted computing for lots of private and enterprise approaches on a day by day foundation in supplying connection and message capabilities till a number of "protection disasters" passed off at the Internet. If security is not regarded as an integral some of the network and development process, old networks are very risk to network attacks due to various security vulnerabilities. When used by hackers, it can be used as an incentive to develop various hacking. Directly against cyber attacks, and these attacks are becoming a growing threat to our society.

II. WHAT IS HACKING?

When the word hacking is mentioned, what type of pictures come to mind? Do you think it is illegal activity? Do you think that encrypted programs are sent to people in order to gain unauthorized access to their computers remotely?

Majority of humans assume that hacking is an unlawful activity. While it's miles fact that criminals are nonetheless exist however they're in small minority. Hacking is truly locating an opportunity or accidental use of hardware or software, so that you could beautify their packages or clear up problems. Hacking is basically a principle where a person or individual or group of a person try to break a computer system with some security flows.

III. NETWORK DOMAIN

The network domain is much more difficult as it is more related to servers or the application side. Network hacking commonly manner accumulating statistics approximately the area the use of equipment like Telnet, Ns Look Up, Ping, Tracert, Netstat , etc. Networking is very important in the field of hacking as most of the devices are connected to the network.

1) Attacks on network and Prevention techniques:

Man-in-the-middle attack: It is a software attack where attacker come between sender and receiver, where sender sends some information to the receiver but attacker comes in between sender and receiver and act as a sender and send bogus information to the receiver and receiver thinks that sender has send this information.

Computer virus: It is a software that can spread through the computer to computer or it can spread through network to network, this virus will spread without user's knowledge and destroy system and it can also corrupt or damage information.

Malware: Malware is a malicious software program or a code where this attack goes into computer without user's permission.

Trojan horse: Trojan is an attack where it's copies the information as a same and steal the information from other computer.

Logic bombs: Logic Bomb is basically enter into the system through links or it may be by opening emails, then attacker will set timings so that logic bomb explode the system automatically.

Rootkit: Rootkit is fixed in an operating system and it can also modify or even the structure of the system.

Denial-of-service: In this DOS attack there are mainly two major things will happen either flooding or crash the system. DOS attacks also cost the organization to solve the problem.

2) Preventions for network attack

Delete unwanted E-mails and avoid downloading or opening unwanted links: deleting unwanted emails regularly helps user to get rid of spam emails, avoid opening links from other websites, some links are programed for hacking personal information about the user

Strong password and change regularly: Strong password makes hackers to difficult to open websites and changing regularly is the best practice to get avoid from the hackers.

Use anti-virus software program: Before software starts its better to use anti-virus software into your computer so that it can avoid getting attacked by malicious virus.

Firewall on Network: Setting Firewall on to your network is the most effective way to avoid unwanted network issues from the hackers. Firewall makes network safe from the other dangerous network.

Use data encryption: Using Data encryption can avoid by misleading conversation between sender and receiver. Data encryption helps to keep safe information between end users.

Security policy and deployment: By setting privacy policy help user to be safe from giving unwanted permissions for hackers.

Train your employee: Before getting hacked by hackers its better to train or educate employees to be alter.

IV. Wireless Network attacks

1) Types of attacks on wireless networks and how they can be prevented from security

Packet detection: Packet detection is a collection of information for future access. It can be network login traffic over a wired or wireless network. Exchange of information between sender and recipient. The hackers will use this attack for unencrypted data.

Driving War - While driving, the attacker drives in a automobile with a in particular configured laptop on which software program software collectively with Net Stumbler or Kismet is set up that identifies the network characteristics. A GPS are uniquely select out the area of a wireless network. The hackers detects the wireless LANs. This attack offers the starting point for further attacks.

SQL and Code Injection Attack: It is an attack to express the uses dishonest, SQL code to exploit back-end databases to access information that was not right for display. Company data, user lists or private client details.

De-authentication Attack: When sender sends request to AP then AP send back respond for sender. Sender while sending group of messages to AP then hacker come in between and send unwanted data to AP, AP thinks that unwanted data is actual data and request

becomes de-authentication, AP send back de-authentication respond.

Proximity Access Point: An unknown hacker will install from some unsecured proxy access such as in airport, office , or outside of a building to stop the traffic from valid wireless clients to whom it appears to be a well founded authenticator. It is not gate way to a trusted network. The hacker make them o trust the well founded customer by changing their Service Set ID so that they can easily target the aimed organization. It is easy to trick unknown users into connecting to the rogue access point.

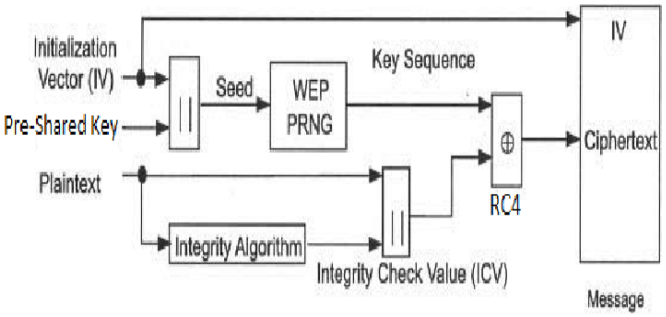
Password theft: User's credentials can easily be stolen. Crimes like identity theft and fraud. once all of your passwords are the same, any hacker can need to make out a password and have access to everything else. Not solely is it necessary to settle on terribly secure and sophisticated paroles that don't have anything to try and do together with your personal life, however it's additionally important to alter your passwords frequently.

Interference: It is also called as jamming. Interference attack is to collect the data from other sources and use that data for illegal purpose. In this attack hackers will steal very sensitive information.

Bluetooth attacks: Blue bugging allows hackers to approach a device and listen to all calls, connect to the internet, text messages (send and receive) and emails, and even make calls (although holder cannot White). It is usually located with older phone models.

1) WEP Attack

Wired Equivalent Privacy, WEP possess for offer stage of safety equal to a stressed out community, even though this purpose turned into now no longer carried out for the essential cryptographic weakness. From the listing of security features summarized in Table 1, WEP offers a confined stage of get right of entry to manage and private the usage of a mystery key, normally a passphrase this is entered on the get right of entry to factor and ought to be regarded to each station trying to connect with the get right of entry to factor. However, you can not really map or decrypt statistics to view community traffic.



Step (1) the ICV is calculated in order that the statistics block is transmitted with inside the body. Step (2) the ICV is delivered to statistics block. Step (3) The starting vector is blended with the name of the game key to generate the important thing of the entire encryption. Step (4) the RC4 set of rules is used to transform the encryption key right into a key circulation. Step (5) an XOR operation is carried out among the important thing circulation and the output of step (2). Step (6) the vector initialization is blended with textual content encryption. [2]

2) WPA Attack

Wi-Fi Protected Access is a protection general for reckon gadgets prepared with Internet connections [9]. WPA turned into evolved from the Wi-Fi Alliance to offer greater advanced statistics encryption and higher consumer authentication than WEP (Wired Equivalent Privacy), the authentic Wi-Fi protection general [2].

WPA 2: WPA2 nonetheless has weaknesses. Above all, those vulnerabilities consist of the capacity for unauthorized get right of entry to the company wi-fi network. This takes place while an assault vector has penetrated positive Wi-Fi networks. Fi Protected Setup (WPS) get right of entry to points. It is usually recommended to disable WPS for every assault vector get right of entry to factor in WPA2 to counter such threats. There also are different vulnerabilities in WPA2, such as: B. Transport Layer Security that chance actors can assault with downgrade attacks.

WPA 3: WPA3 assist isn't routinely introduced to all gadgets. Users who need to apply WPA3-authorised

gadgets inclusive of wi-fi routers have to purchase new routers that assist WPA3 or have the tool improve from the manufacturer.

3) Wireless Security Measure

User permission	Confirm that users trying to access the network are who they say they are
User access control	Allows access to the network only to authenticated users who are authorized to access it.
Data privacy	Ensures that the data transmitted over the network is encrypted to prevent eavesdropping or other unauthorized access.
Key management	Create, protect, and distribute keys that are used to encrypt data and other messages.
Message integrity	Check to see if there is a message that was not modified in transit

Table1: Wireless Security Measure

4) Prevention for Wireless Network

Use WPA2 security: WPA2 is a form of encryption used to guard maximum Wi-Fi networks. A WPA2 community presents specific encryption keys for each wi-fi patron that connects to it. Wi-Fi customers have to replace their enabled Wi-Fi immediately. Devices as quickly as a software program replace is available. As with many lately determined vulnerabilities, it's miles most effective a be counted of time earlier than hackers locate approaches to take benefit of this vulnerability.

Use WAF - A WAF protects your web applications through filtering and monitoring and blocks the transmitted HTTP traffic Malicious / S. to the web application in order to prevent unauthorized data from leaving the application. To this end, a number of guidelines are followed that can be used to determine which traffic is malicious and which traffic is safe. The guidelines can be customized to meet the specific needs of your web application or a range of web applications.

Minimize the range of your network: Set access restrictions for your network.

Use VPN on Open Networks - A VPN lets in a user's gadgets to hook up with a personal community over a public community. VPNs had been created to safely join gadgets inside a company community to personal Internet servers.

Software and firmware: Like any software, firmware can also be improved: bugs can be found and corrected, new functions can be added. Whenever a manufacturer releases new firmware for one of its devices that you own, you can take it and take your firmware with you update to the new version. With cope with filtering you may outline a listing of gadgets and simplest permit those gadgets in your Wi-Fi network.

Enable MAC filtering: enable the MAC filter for secure Wi-Fi network.

Monitor Network Traffic: Monitoring network traffic is beyond belief powerful method to understand problems or issues in your IT environment. Comprehensive Performance Analysis • Monitor, track, and analyze network traffic data simultaneously

V. WIRED NETWORK ATTACKS

1) Types of attacks on the wired network and how to prevent them

Attacks on the private network: In this, the community is especially a LAN inside a agency that connects and helps conversation for all regions of agency such as head office, sales, factory, R&D etc. Foreign trade information is transmitted via a rented phone, post office or fax and entered into the system. This form of community is commonly hacked from within. An legal person or administrator can misconfigure legal software, which ends up in customers connecting their personal computer to their pc and beginning lower back door for the personal LAN over rent smartphone lines.

Web service for Private networks attacks: A website is additional to the private network so that customers

can place orders over the Internet. As long as the web server is providing information, it is susceptible to dos attacks from the Internet. If internet users can invoke it as a buffer overflow error, attackers could take over the web server.

Firewalls and Virtual Private Networks: Firewalls are used to secure inner network. Whatever, this is not absolutely certain. Failure to cautiously configure the firewall can create a fake experience of safety and permit outsiders to hack into inner systems.

1) Prevention for Wired Network

Keep the network up to date.
Physically protect the network.
Take into account the Media access control address filtering.
Gadget Virtual local area Networks to separate traffic.
Secure the entire network

VI. Challenges of network

Data Compression: With data compression, information is encoded with fewer bits than the original. Loss compression reduces bits through doing away with useless or much less vital information. Reducing the scale of a information report is frequently called information compression.
Data aggregation: It's the manner of gathering and aggregating beneficial records. In WSN, records aggregation is an effective manner to keep restrained resources. The important aim of records aggregation algorithms is to accumulate and mixture records in an power green manner to enhance the lifestyles of the network. In a network, latency measures the time it takes a few records to attain its vacation spot over the network. It is commonly measured as the round-trip delay, the time it takes for information to reach its destination and return measured in milliseconds.
Quality of Service: Quality of Service (QoS) is a fixed of technology that perform on a community to make sure its dependency capacity. Run an application with high priority and traffic with limited network capacity.
Production costs: The production costs refer to all costs that a company incurs to manufacture a product or to provide a service. Production fee can encompass loads of prices which includes labour, uncooked materials, consumables for making consumables, and standard overheads.
Scalability: Scalability is an characteristic that describes the cap potential of a process, network, software program or employer to develop and deal with multiplied demand. A system business this is defined as scalable has the benefit of being extra adaptable to converting desires or necessities for clients.
Fault performance: fault management programs routinely send queries to devices and nodes to determine if the hardware is working properly is working. They collect information such as system logs and Simple Network Management Protocol trap data and analyse them for abnormal behaviour or performance.

VII. Literature Survey

- More than two-thirds of cyber protection specialists don't have any self assurance they could be capable of save you a wi-fi attack, the second one instalment of the Wireless Security: 2020 Internet of Evil Things document via way of means of Outpost24 has revealed. The take a look at has highlighted the quantity to which cyber-professionals are involved approximately the extra threats posed to companies via way of means of the developing range of shadow net of things (IoT) and wi-fi gadgets in workplaces [7].
- Recently 10crore Indian's card data selling on Dark Web:
  Independent cyber safety researcher Rajshekhar Rajaharia claimed on Sunday that data of almost 10crore credit score and debit card holders in the country is being bought for an undisclosed quantity at the dark web [8].

VIII. Conclusion

In this article, we will discuss a variety of hacking techniques. From the functions, goals and principles of various hacking, we can sum up that the weak points of network or system always result from two main factors, the technical factor and the human factor. The factor relates to incomplete system and network designs such as unencrypted data, unprotected communications, buffer overflow problems, and software errors.

IX. REFERENCES

[1] Nilesh Pandey, Pandey, J Comput Sci Syst Biol 2018, 11:5 Network Security and Ethical Hacking.
[2] Steve rackley, wireless networking technology, from principle to success implementation, 2007.
[3] Dr. Amer S. Elameer, Hacking Techniques in Wired Networks
[4] https://www.insecure.com
[5] https://cyberthreadported.com
[6] https://www.logsign.com/blog/types-of-wireless-network-attacks/
[7] https://www.infosecurity-magazine.com/news/fears-threats-wireless-devices/
[8] https://economictimes.indiatimes.com/tech/technology/10-crore-indians-card-data-selling-on-dark-web-researcher/articleshow/80093994.cms
[9] https://flipboard.com/article/wi-fi-protected-access-wpa/f-8306bffb1a%2Ftechtarget.com