ISSN:0971-1260
Vol-22-Issue-10-November-2019

An Overview of Network Attack Tools

[1] Rutuja Vilas Kotkar, [2] Tanpure Renuka Subhash, 3 Snehsudha Popatrao Dhage

[1] PIRENS Institute of Computer Technology Loni (bk), Ahmednagar, India

rutuja.kotkar@gmail.com

[2] PIRENS Institute of Computer Technology, Loni (bk), Ahmednagar, India

renukatanpure24@gmail.com

[3] Loknete Ramdas Patil Dhumal Arts science and commerce college, Rahuri, Ahmednagar, India

snehsudhadhage@gmail.com

Abstract

The Internet has become an integral part of each and everyone's life. As the use of the internet is increasing, on the other hand, threats of network attacks are also increasing. Users are expecting the robust security of their credentials on the internet. It is necessary to prevent the network from the attacks and the attackers. Many network security tools are available in the public domain. This paper provides information about the network attack tools available in the public domain, that are used for monitoring the network traffic and for cracking the password of the wireless network.

I. Introduction

In our daily routine, the Internet has become a fundamental need. The use of mobile phones is increasing, and due to the internet at an affordable rate, its use is also increased. Many people are connected to the web. It happens that every time we need our mobile phone at our workplace to accomplish some task. So the use of a mobile phone is a must nowadays. The Wi-Fi hotspots can quickly found at maximum places. Many people use remote at their home network to interface with the devices that are available at their homes like AC, fridge, lights, etc. All the users can see the local Wi-Fi networks in the framework, and they wanted to use it. Many networks are protected by the secret key.

It is essential for the user to keep in mind the security key or to remember the security key. In case if the user's network is down, then it will search for the Local Network if the user needs the internet on an urgent basis. At this time, many users and for the Wi-Fi security and try to get unauthorized access to the remote network. This type of unauthorized access is also known as an atom regardless of the intention.

Same as an individual, there are many people like to scan other's computer or the network for a particular intention or without any intention. Many organizations wanted to know what is is happening in the network that is which company is doing what type of business on the network. Show the organizations are also monitoring The Other organization's network for the business purpose.

ISSN:0971-1260
Vol-22-Issue-10-November-2019

few people you can crack the password of others network for hotspot connection or just for fun. Business Rivals monitor network is the business purpose. many people crack the password or monitor the network to harm someone.

Wireless hacking has become very common. The norms for the wireless network are based on IEEE 802.11. There should be at least one access point to the network for the traffic between the nodes. Wireless LAN has two types of vulnerabilities that are weak encryption and deprived setup. Wi-Fi LAN uses two security conventions WEP and WPA.

Apart from the traditional attacks nowadays, attackers are using the tools to attack the network. Many times the attacker tries to crack the password and get unauthorized access.

II. Network Attack Tools

1. WireShark

The attacker uses the Wireshark tool to analyze network protocols. It allows the attacker to check activities on the network. The attacker captures the packet check the data at the micro-level. Wireshark tool runs on Linux, Windows, Solaris, and FreeBSD operating systems. the attacker must have proper knowledge of network protocol for analyzing the information obtained from the network. If the attacker does not have proper knowledge of network protocol, then he may not find this tool easy [1].

Wireshark network analyzer tools are the standard tool. Currently, there are many downloads occurring in each month. Many IT organizations are using the Wireshark tool for the security of the network, troubleshooting, and optimization of the network [2]. Figure 1 shows the WireShark Interface.

2. Air jack

Airjack is used by the attackers for injecting the packet. It is also called a packet injection tool.This tool is an 802.11 device. The Prism network card is used with Airjack.Different names incorporate monkey-jack, WLAN-jack, kracker-jack, and essid-jack.

This device initially utilized as an advanced tool for remote applications. The drivers used for catching, infusing, and getting the packets as they are transmitted. The attacks like Man-in-the-Middle attack and DOS attacks are performed using this tool. Its capacities incorporate having the option to infuse information parcels into a system to wreak devastation on the associations between the wireless node and their present access point. When the attack is performed, the first thing done is to terminate everyone from the access point as soon as possible and then keep all the users logged off till the time user wishes.

Without the Layer-1, outline level validation on all 802.11a/b/networks, a Computer running Air jack would inactively accept the identity of an access point and afterward once within the channel of correspondence among hub and Access Point, and Air jack would start sending

ISSN:0971-1260
Vol-22-Issue-10-November-2019

separate or deauthenticate outlines consecutively at a soaring rate. The clients' systems organize cards to translate this as their Acess Point , and they fall their association [3].

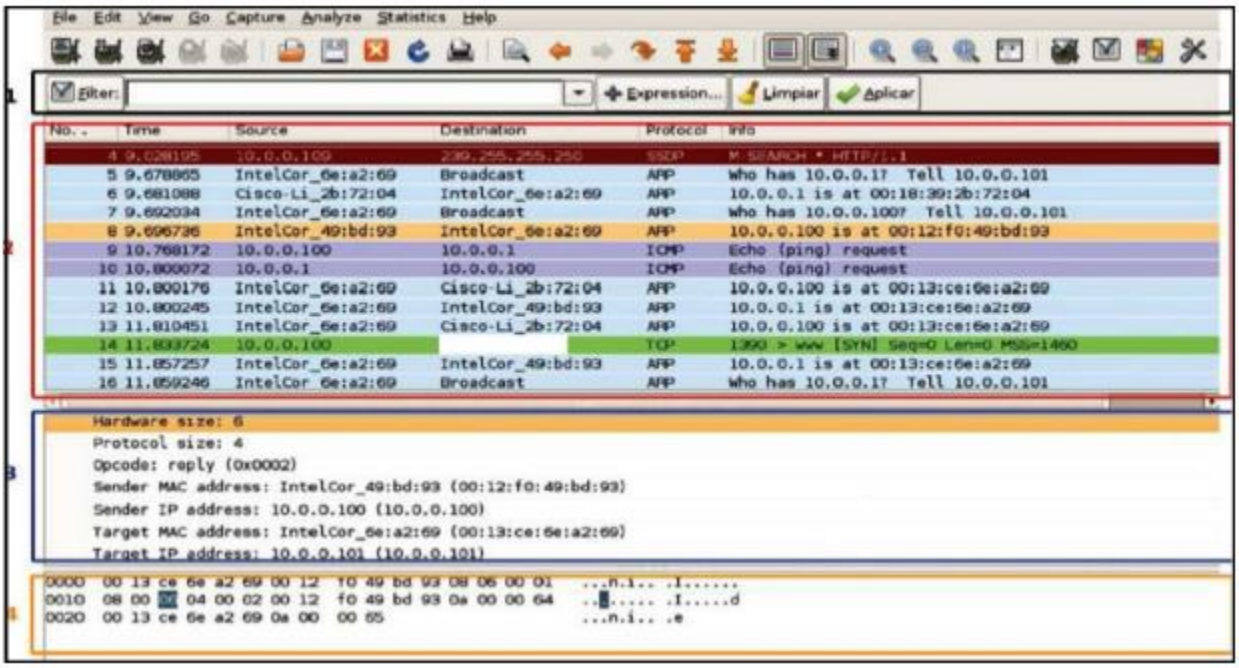

Fig 1: Example of WireShark Interface [2]

3. CoWPAtty

CoWPAtty is an automated tool, and the attackers use this tool to perform the dictionary attack for WPA-PSK. On Linux OS, this tool runs, so it has the command-line interface. It runs on a word-list consisting of the password to use in the attack. CoWPAtty is easy to use, but it is slow. It is slow because the hash uses SHA1 with a kernel of SSID. Similar passwords are having dissimilar SSIM. Using a table of rainbow alongside every access point will not always work. A password dictionary is used by the CowPAtty tool for generating the hack for every word enclosed in the dictionary by using the SSID. In the new version, the pre-computed hash is used to get better the speed. The precomputed file consists of a 172000 dictionary file for about 1000 most current SSID [4].

4. WepAttack

WepAttack tool is used by the attacker to attack the WLAN. Wepattack is an open-source Linux tool. This tool is used to crack 802.11 WEP keys. WepAttack is based on an active dictionary attack. This tool tests millions of words to discover the right key. One packet is enough to start this attack [5] [6].

5. OmniPeek

ISSN:0971-1260
Vol-22-Issue-10-November-2019

The attacker uses the OmniPeek tool for packet sniffing and analyzing the network. It is used for capturing and analyzing the wireless traffic. This tool runs on only Windows operating systems. The user should know protocols to understand things properly. There are many network interface cards available in the market, and the OmniPeek tool works with all. Omni Peek supports the plug-in. this tool is used for network troubleshooting [7].

It helps desk staff can do the following remote assistance using OmniPeek tool:

- Determine the root cause of problems quickly
- Decrease mean-time-to-resolution (MTTR)
- Eradicate the need to send staff out to the customer site to reproduce problems

6. CommView

Attackers use the CommView tool for Wi-Fi to monitor and analyze packet. CommView is designed for LAN administrators, network programmers, and security experts. It virtually gives the full representation of the traffic flowing throughout a PC or LAN part. Its GUI is easy to understand. On 802.11 a/b/g/n/ac networks, this tool works finely. CommonView captures each packet and displays useful information as a list. The data such as network connections, access points, signal strength, stations, and protocol distribution is acquired from this tool. User-defined WEP or WPA keys are used to decrypt the captured packets. Wi-Fi administrator and security professionals use this tool. If an individual wants to monitor his/her home Wi-Fi traffic, they can also use it. The attackers can also use this tool to monitor home traffic. Programmers who work on software for wireless networks also use this tool. Figure 2 shows detailed information about your computer's network connections [8] [9].

7. Aircrack

Aircrack is the tool used by the attacker. It is prevalent and used for cracking the passwords of wireless networks. This tool is used for 802.11a/b/g WEP and WPA cracking. The feature of the Aircrack tool is that it uses the best algorithms for recovering the password of the wireless. For this, it captures the packets. When enough packets get collected, it tries to recover the password. Standard FMS attack with some optimizations is used to make the attack faster.

Aircracking is an entire suite of tools to evaluate Wi-Fi network security.

Its focus on diverse areas of Wi-Fi security:

- Monitoring: the third party tool is used for Packet capture and export of data to text files for further processing.
- Attacking: it performs deauthentication, Replay attacks, fake access points, and others through packet injection
- Testing: Checks the Wi-Fi cards and capabilities of the driver.
- Cracking: It cracks the WEP and WPA PSK.

Attackers learn this tool from the tutorial provided by the company. The attackers learn how to install the tool and crack wireless passwords. This tool comes as Linux distribution, Live CD, and VMware image options. Aircrack supports maximum wireless adapters and is almost certain

ISSN:0971-1260
Vol-22-Issue-10-November-2019

to work. The attacker who is using this tool on the Linux operating system should have in-depth knowledge of Linux. If the attacker is not at ease with Linux, then it is difficult to use this tool [10].

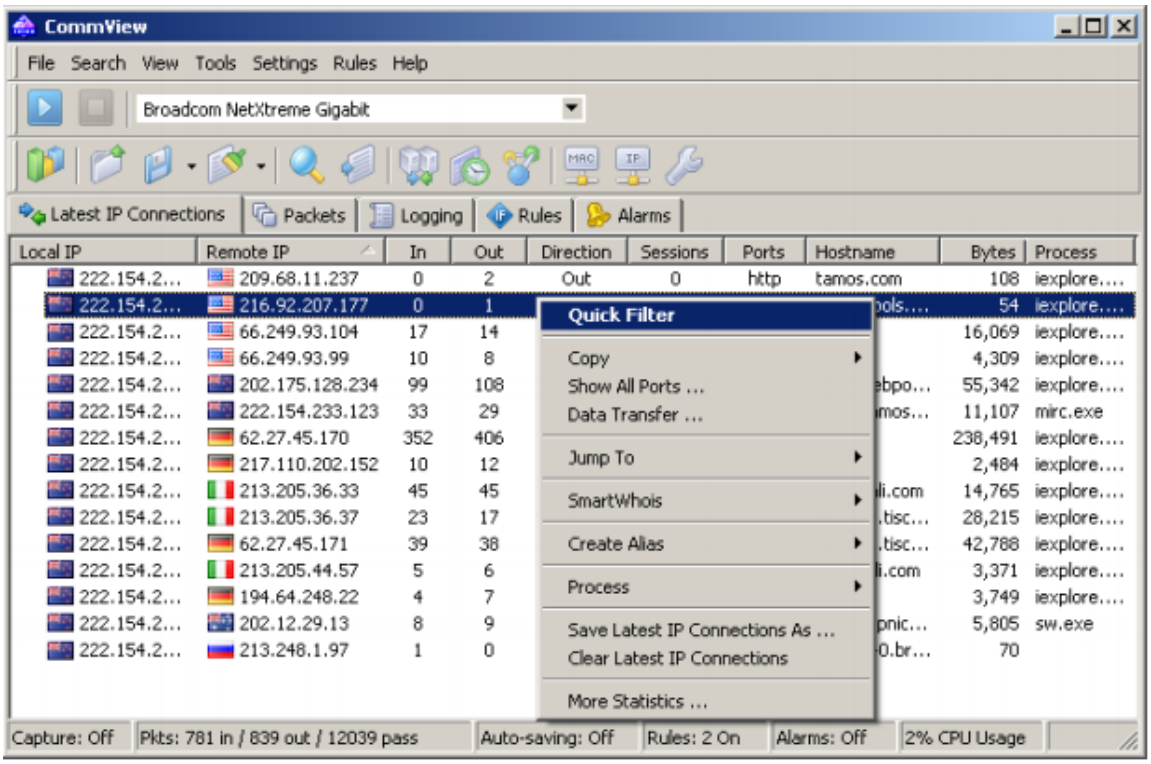

Fig 2: Common view interface with the network connections [8]

8. CloudCracker

Cloud cracker is an online WPA/WPA 2 and a Hash cracker tool. Attackers use this tool for password cracking of the WPA protected Wi-Fi networks. This tool also cracks the different password hashes. To use the tool user has to upload the handshake file, then type the name of the network and initiate the tool. The tool has a dictionary of 300 million words to carry out attacks. This tool is easy to use, and it saves time and money. It supports WPA/WPA2, SHA-512, NTLM, MD5, MS-CHAPv2, and secures the transmission. It is a fast password cracking service [11].

9. AirSnort

AirSnort used for decrypting WEP encryption on a Wi-Fi 802.11b network. This is a popular tool and free, which runs on Windows and LINUX platforms. This tool is not in use in much, but it is available for download. this tool is for wireless LAN for cracking encryption keys on 802. 11b WEP networks. This tool monitor traffic passively and calculates the encryption key when it will get enough the packets. This tool is straightforward to use, so, the attacker used this tool to crack the WEP password[12]

ISSN:0971-1260
Vol-22-Issue-10-November-2019

10. Cain & Able

Attackers used Cain & Able tool for password cracking. This tool intercepts network traffic, and after that, it finds out passwords by a brute-force attack and cryptanalysis attack methods. Attackers analyze the wireless network and recover the keys. If the attacker is trying to learn wireless security and password cracking, he should once try this tool [13].

Table 1: Network Attack Tools

Name of the tool	**Tool Description**
Airjack	Used for Packet Injection
CoWPAtty	Dictionary attack tool
OmniPeek	Network monitoring tool
CommonView	Monitoring and analyzing the packets
Cloud Cracker	Password and hash cracker tool
WepAttack	cracks 802.11 WEP keys
WireShark	Network protocol analyzer
Cain & Able	Password cracking tool

Conclusion

Wireless hacking tools are discussed in the paper. There are a few tools that are used to crack the password and gain unauthorized access. Some tolls are used for monitoring and troubleshooting the network. Many people are interested in cracking the wireless hotspot to get free internet access. Some tools discussed in the paper also try the dictionary attack for cracking the Wi-Fi password. It is a crime to hack the network and get unauthorized access. It is advisable not to use the tools for illegal access. WEP encryption key has to be used by the user for a wireless network, but it is also possible to crack the WEP keys. Wireless monitoring and troubleshooting tools are beneficial to the network administrator to solve the problem of connecting to the network.

References

[1] S. Pavithirakini, D.D.M.M. Bandara, C.N.Gunawardhana, K.K.S. Perera, B.G.M.M. Abeyrathne, Dhishan Dhammearatchi, “Improve the Capabilities of Wireshark as a tool for Intrusion Detection in DOS Attacks,” International Journal of Scientific and Research Publications, Volume 6, Issue 4, April 2016 378, ISSN, 2250-3153

ISSN:0971-1260
Vol-22-Issue-10-November-2019

[2] Jhilam Biswas, Ashutosh, "An Insight into Network Traffic Analysis using Packet Sniffer," International Journal of Computer Applications (0975 – 8887) Volume 94 – No 11, May 2014.

[3] http://www.hackingtools.in/free-download-air-jack/

[4] https://hackaday.com/tag/cowpatty/

[5] https://noise.getoto.net/2018/11/23/wepattack-wlan-802-11-wep-key-hacking-tool/

[6] http://anonhacktivism.blogspot.com/2013/10/wepattack-wlan-dictionary-attacker.html

[7] https://www.monitortools.com/software/product/omnipeek/

[8] https://www.tamos.com/docs/cv65.pdf
[9] https://www.tamos.com/docs/cv_datasheet.pdf
[10] https://www.aircrack-ng.org/
[11]Posted by Kapil Soni, http://www.toolwar.com/2014/03/cloud-cracker-online-wpawpa2-and-hash.html

[12]https://airsnort.apps112.com/
[13]https://cain_abel.en.downloadastro.com

Authors Profile

Rutuja Vilas Kotkar has done Masters in Computer Application. Currently, she is working as a lecturer PIRENS Institute of Computer Technology. She has the six-year experience, and her area of interest is Management Information System, Discrete mathematics, Information security and Audit, computer organization.

Tanpure Renuka Subhash has done Masters in Computer Application. Currently, she is working as a lecturer PIRENS Institute of Computer Technology. She has5 year experience, and her area of interest is Operating System, programming in Java, PHP, DBMS

Snehsudha Popatrao Dhage has done Bachelorette in Computer Science and MBA in Information Technology. Currently, she is working as a lecturer at Loknete Ramdas Patil Dhumal Arts science and commerce college. She has the eight-year of experience, and her area of interest is DBMS, RDBMS, Recent Trends in IT, Visual Basic, VB.Net, O.S.