International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

Backdoor Implementation in Android using Open Source Tools

Rajasekhar Reddy. R, P.S.G.Aruna Sri, Ram Sai. P, Jedediah.B, Anusha. M

Abstract - In this paper, we are showing the usage of hacking into android framework with the help of an open source tool. Turn around TCP opens an indirect access on the target system and which is remotely operated by the attacker without the target's information. However the connection must be initiated by the victim. The Metasploit tool is an open source tool. It help about the susceptibilities and helps in performing penetration testing. Metasploit framework consists of an exploits database, payloads, and vulnerabilities. By this attack, the assaulter creates a payload, and that payload is transferred into the victim system. When the payload is initiated, the attacker gets access to the victim's system, files, images, contacts, messages etc.

Keywords—Metasploit framework; Firewall; Remote Backdoor; Reverse TCP;

I. INTRODUCTION

The world we are living in is gradually becoming dependent on networks. Therefore, cyber-attacks are becoming more and more dangerous. Cyber-attacks can vary from loss of personal information to disclosure of national secrets to other countries. These attacks can be done by simply by clicking a button. Any one with enough knowledge and required tools can do hacking. The knowledge required for performing many attacks can be obtained just by searching online. 3 major types of cyber-attacks are: Malware attacks, MITM attacks and Dos attacks.

In this paper ,The attack performed is creating a backdoor to the target's machine. In this category ,so many types of real time attacks are there. CCleaner is the recent one. CCleaner is one of the software held by Avast Company which is intended to remove waste files and cache. The attackers changed the source code of the tool and built a backdoor to the tool.

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
Rajasekhar Reddy. R*, Student, Department of Electronics & Computer Engineering ,Konreu Lakshmaiah Education Foundation, Vaddeswaram ,AP, India. Email: rajasekhar12033@gmail.com
P.S.G.Aruna Sri, Associate Professor, Department of Electronics & Computer Engineering ,Konreu Lakshmaiah Education Foundation, Vaddeswaram ,AP, India.. Email: pabbisettiarunasri@gmail.com
Ram Sai.P, Student, Department of Electronics & Computer Engineering ,Konreu Lakshmaiah Education Foundation, Vaddeswaram ,AP, India. Email: ramsai.pala236@gmail.com
Jedediah.B, Student, Department of Electronics & Computer Engineering ,Konreu Lakshmaiah Education Foundation, Vaddeswaram ,AP, India. Email: jedediahboggarappu@gmail.com
Anusha.M. Associate Professor, Department of Computer Science Engineering ,Konreu Lakshmaiah Education Foundation, Vaddeswaram ,AP, India Email: anushaaa9@gmail.com

This altered application again downloads a malware in to the target's system from attacker's server [2].

Backdoor attacks don't seem to be always dangerous. As an example, accessing the info is very important because it might facilitate in gathering information regarding a target. So, backdoor attacks also play a important role in modern world .

The firewall technology can be assessed into 3 types. Packet filtering firewall is first one that is present at the network and transport layers. The subsequent one is a alternative server-based firewall, whether a packet should be sent or discarded will be decided by this firewall. The third one is a mixed firewall which contains many firewalls [2]. Machine learning techniques are used in the latest firewalls for identifying the threats based on logs of previous firewalls. These firewall logs store tons of information on these threats like, time of the attack done, that helps find and analyzing the new reasonably cyberattacks [3].

II. RELATED WORK

The most powerful virus, Stuxnet had a significant impact on the planet. It affected the Asian country nuclear facilities. Stuxnet worm is made with the help of Metasploit Framework. It consists a user and kernel level Rootkit which helps it to get the root access along with hiding its existence [4].

[5] describes the importance of the Metasploit framework tool in penetration testing precise the phases concerned in hacking a specific system and varied tools existing to realize them. Implementation of this attack can be done by this Metasploit tool.

The analysis conducted within the paper [6], reveals the tactic of hacking the commercial management systems (ICS) using Metasploit tool. They used attacker's system for performing attack and retrieving data from the victim and victim's system to perform the attack on. This revisions shows the danger and damage which can be caused if Metasploit is used for illicit intentions.

Bootable pendrive:

The quickest methodology, for running Kali Linux is to run it "live" from an external USB drive. This methodology has many advantages:

• It's non-destructive — it causes no problems for booting up
• It's moveable — we'll be able to carry around Kali Linux where ever you go and can run it in on any offered system
• It's readjust able — we can readjust the kali linux as per our needs
• It's probably persistent — with additional effort, we can create persistence for our Kali Linux to save data

Persistence:

While running bootable kali linux it is important to have persistence to save collected data, test results, configurations in the os. While booting live kali linux we have choice to select persistence or not. The persistent data is kept in the allocated partition, which can even be encrypted. To setup persistence some additional work needs to be done.

This guide assumes that you just have already created a Kali UNIX "Live" USB drive as delineate within the section on it subject. For the needs of this text, we'll assume you're functioning on a Linux-based system.

III. METASPLOIT FRAMEWORK

It's a penetration testing tool that helps the user to test, and implement the exploit codes. It consists a default set of tools that can be used for testing vulnerabilities, scanning networks, performing attacks. It was used for developing many powerful and dangerous malwares in history. It's a tool that can be used for penetration testing. The Metasploit framework consists of various modules.

1) Exploit:

It is a code that helps a hacker to get access into the target system, by exploiting a vulnerability. Associate exploit is working to hold the payload and transfer it into the victim's system.

2) Payload:

It is the malware that is implemented on the victim's system after the exploit is executed. In this Reverse Shell and bind shell are the two types of payloads presented .

3) Database:

Metasploit framework contains the various information on exploits. "start PostgreSQL" is the command that is required for database. Core components of Metasploit are:

1) Libraries: There are many libraries present in Metasploit. These are used for managing and working of Metasploit. Interfaces, plugins, modules are some types of libraries.

2) Rex: It is the basic part of Metasploit. It is used for performing many basic operations in Metasploit which contains wrapper socket system, exploit utility categories, protocol shoppers, categories, protocol shoppers, and servers, and additionally a work system.

3) Core: Plugins, sessions that are used by the attacker for attacking the target are provided by this core.

4) Base: The utility classes that are required by the core library to work properly are present in base library.

5) Interfaces: There are only some interfaces in Metasploit that allows user to access. Essential Component of Metasploit Framework is Datastore. It proposes some interfaces for settings and exploits. It includes a list of named values that allows configuration of parts.

IV. METHOLODOGY

1) Select the module: Before continuing we should determine what kind of module is required for the target. The best method to choose the module is to choose from the list of present modules. To do so, we need to execute "show all" command which shows all the exploits, payloads, modules.

A) Exploit Modules: It is used for exploiting a vulnerability. Exploit module uses the vulnerability for installing a backdoor in the target system for the attacker. Code injection, buffer overflow are some types of exploit modules.

B) Auxiliary modules: They are not used for installing any backdoor. They are used for vulnerability scanning, network scanning etc.

C) Post-Exploitation modules: These are used after installing backdoor to collect data from the target system like get SMS, dump contacts.

2) Configure the Module: According to our application the values of RHOST, RPORT, LHOST, LPORT, TIMEOUT, WORKSPACE, and GWHOST should be configured.

3) Options Setting: The attacker have to set the options for LHOST, RHOST, LPORT etc. If the module is changed these options will be lost.

4) Select a target: The target needs to be selected carefully because the target should be scanned for vulnerabilities and the module should be selected according to the vulnerability.

5) Select a payload: The payload should be selected based on the module, target system, vulnerability. The payload can be selected from the list of available payloads.

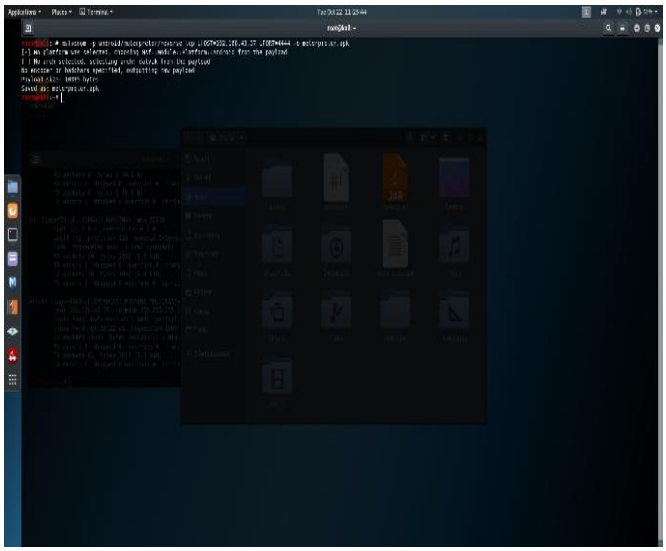
6) Module Run: The module is ready to be executed after configuring the module and selecting the payload .

7) Exploit the infected device: once the pay load is running within the host's device. we tend to begin our attack and access the information transfer that is sensitive to the user involved.

V. RESULT ANALYSIS:

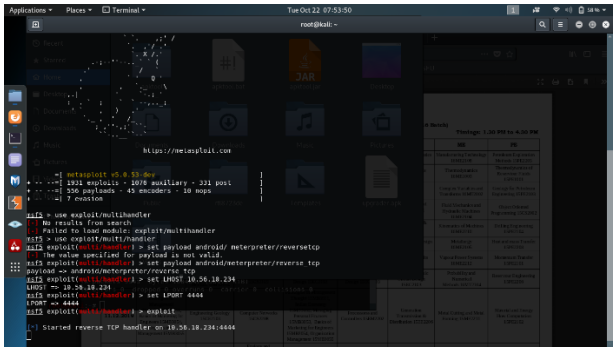
Payload creation:

Here, we created payload using msfvenom command.

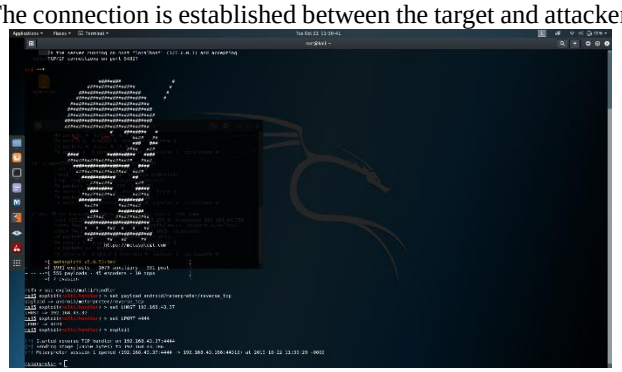


Creating listener:

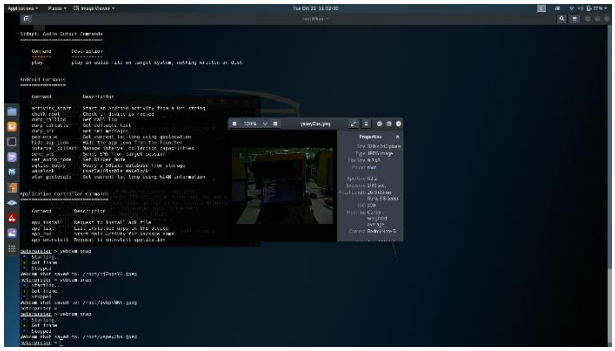
We created listener to receive connection from the target system.



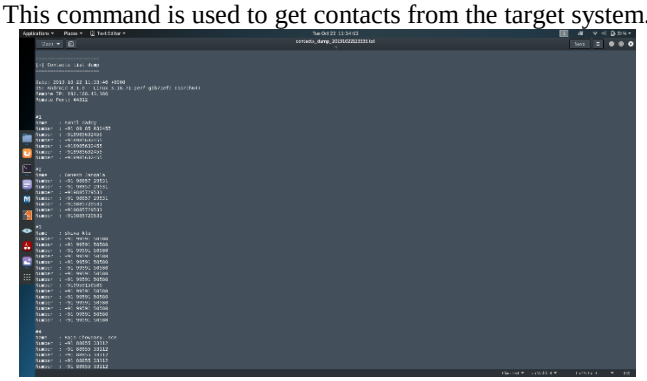
Payload connected:
The connection is established between the target and attacker.



Webcam snap:
This command is used to take a snap taken from the target system's camera.



Dump contacts:
This command is used to get contacts from the target system.



VI. CONCLUSION:

- Now a days, the victims to those sorts of attacks are those who don't seem to be cautious concerning their security, not alert to cyber-attacks, shares their personal info with none considerations, provides system access for an application to system although it is unnecessary etc. The preventive steps are terribly easy like scrutiny the items like mails, application permissions, sharing the private info, inspection the legitimacy of the web site.
- Metasploit framework is an open source tool. Therefore, it is useful to organizations that need to style Associate in Nursing exploit to check their tool for vulnerabilities. Overall, such Associate in Nursing implementation may well be simply unified into a introductory cybersecurity course for increased student education.

REFERENCES

1. T. Fox-Brewster, "Hackers Hid Backdoor In CCleaner Security App With 2 Billion Downloads -- 2.3 Million Infected," Forbes, 18 September 2017. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2017/09/18/ccleanercybersecurity-app-infected-with-backdoor/#72697057316a. [Accessed 14 February 2018].
2. X. Yue, et.al, "The Research of Firewall Technology in Computer Security," pp. 1-4, 2009.
3. R. Winding, et.al, "System Anomaly Detection: Mining Firewall Logs," pp. 1-5, 2006.
4. R. Masood et.al, "SWAM: Stuxnet Worm Analysis in Metasploit," IEEE, 2011.
5. F. Holik, J. Horalek, O. Marik, S. Neradova and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," IEEE, 2014.
6. N. Wallace and T. Atkison, "Observing Industrial Control System Attacks Launched Via Metasploit Framework," ACMSE, 2013.
7. Swain G. "Adaptive pixel value differencing steganography using both vertical and horizontal edges" Multimedia Tools and Applications,2016.
8. Kumar J.D., Srikanth V., Tejeswini L." Email phishing attack mitigation using server side email addon" Indian Journal of Science and Technology,2016
9. Jaya Rohit K., Siva Rama Krishna M., Geetha Krishna C.H., Aruna Sri P.S.G. "Securing message at end-to-end mobile communication using cryptography algorithm" Indian Journal of Science and Technology,2016.
10. MAH Mohammad Arshad "Automatic Vulnerability Attack Detection And Prevention System For Web Security" International Journal of Pure and Applied Mathematics,2018