Penetration Testing on Android and Windows

Shailesh D. Kamble
Department of Computer Technology
Yeshwantrao Chavhan College of Engineering
Nagpur, India
shailesh_2kin@rediffmail.com

Aditya Dhande
Department of Computer Technology
Yeshwantrao Chavhan College of Engineering
Nagpur, India
adityadhande083@gmail.com

Omkar Deshpande
Department of Computer Technology
Yeshwantrao Chavhan College of Engineering
Nagpur, India
16111997od@gmail.com

Tazsvi Jamwal
Department of Computer Technology
Yeshwantrao Chavhan College of Engineering
Nagpur, India
tazsvijamwal@gmail.com

Nandini Bharadwaj
Department of Computer Technology
Yeshwantrao Chavhan College of Engineering
Nagpur, India
Nandinibharadwaj14@gmail.com

Parag Dhawan
Computer Science and Engineering
Visvesvaraya National Institute of Technology,
Nagpur, India
dhawanppd@gmail.com

***Abstract* — Maintaining Security/privacy is one of difficult tasks in today's era. As everyone has digital devices (phones, laptops) people are more vulnerable to security attacks and can easily get targeted for any means. Because of this pandemic, use of digital devices and services is rapidly increasing than previous years which makes easy for hackers to attack individual and compromise their privacy. Security attacks on mobiles phone are most consistent attacks than desktop attacks. Security attacks on mobile phone generally focused on mobile application to infect them with malicious files and getting access of victim's device. Once hacker has the access of victim's device they transfer the sensitive and private data with the help of applications backdoor to the backup server or to the hacker's device. In this paper we have analyzed some application working on android as well as windows. We are also manually scripting malware. The goal is not to cause any damage to victims/organizations infrastructure but to prevent being attack by unauthorized user. We have designed threat model to detect various threats which helps to identify attack surface, vulnerabilities and loop holes in the system. In this project we have suggested to perform risk assessments to identify new changes which may or may not be harmful for system and these assessments should only be carried out by penetration tester or a professional.**

Keywords— Pentest, security, vulnerability, android, windows, malware Introduction

I. INTRODUCTION

Penetration testing is a method of identifying security weakness, vulnerabilities, and loopholes of the system/network with legal permission of infrastructures to prevent any further damage to the organization[1]. Vulnerability assessment is a term to run system tests with various aspects and concerns of security architecture of organization. It runs manual as well as automated tests with expert analysis this tests can be run on internet too. After running vulnerability assessment we get results to get it more accurate there is a term named penetration barrier which identify access paths missed by vulnerability assessment by running deep analysis. After getting all the possible attack paths, vulnerabilities and loopholes [2]. we need to find out the way to protect with respect to security architecture without creating any extra threat possibilities. To avoid such on time errors we can setup virtual environment with same network and security architecture and perform prevention changes accordingly without compromising current security.

The major Security concerns were raised and penetration testing came into picture[3]. Several features and functions of devices may increase usage of data and convenient services but simultaneously increases the risk for new vulnerabilities[4]. In operating system, there are stack of different layers and each layer have several program components. The layers that are mainly into consideration for testing are: Kernel layer, which interacts with hardware components and have all the required hardware drivers. Libraries, that enables the devices to deal with variety of data provided [5]. Run time, provides memory management, security and threading support and isolation. Application framework, deals directly with applications. Application layer, this study is regarding the device security concerned with TCP/IP network security. Certifications in Penetration Testing related Work [6], Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH) Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), Certified Penetration Testing Professional (CPENT), and Advanced Penetration Tester (GXPN), CREST Penetration Testing Certifications Communication Electronic Security Group (CESG) IT Health Check Service (CHECK) Certification.

II. PROBLEM DEFINITION

Purpose of this pen testing project is to find out the vulnerabilities which will provide the unauthorized access to the attacker and to eliminate the unauthorized access of the user. Vulnerability assessment is one of the way to find out the loopholes and back doors present in the current system by finding this loopholes and back doors it benefits both business and its operation[7]. Penetration testing helps to find out time risk which will be cost due to network architecture weakness. If there is a loophole in network attacker can easily compromise the system which can affect as well as important documents of the organization. Pen testing not only help the organization to find out how the attacker breach the system But also provides the way to prevent future attacks of similar kind .

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Copyright © Authors

Loop hole in network attacker can easily compromise the system which can affect as well as important documents of the organization. Pen testing not only help the organization to find out how the attacker breach the system But also provides the way to prevent future attacks of similar kind .

As a security aspect penetration testing helps to save the data and to set up an efficient security architecture to identify vulnerabilities in the system. Elimination of vulnerabilities is totally dependent on what type of security measures are present in the system. If proper pen testing measures are present in the system. It will helps to identify actual exploitable security threats by applying countermeasures we can prevent Data loss and damage[2][5]. Every organization have security audits which will helps to identify risk before security breaches and helps to prevent financial losses. Skipping security audits main leads to major damages and financial loss. Penetration testing creates awareness of security and importance at all level of organization Which Helps to avoid security incidents. Figure 1 shows the work procedure of pen testing.

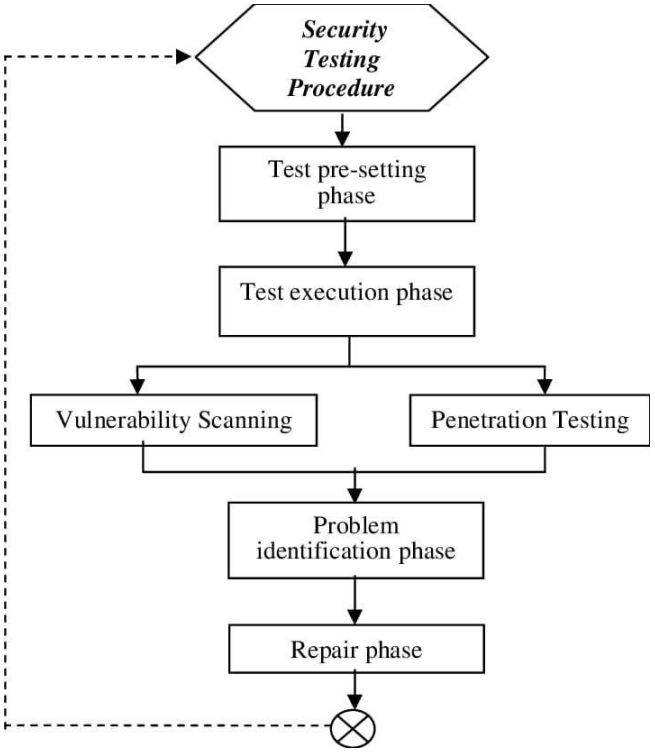

Figure 1 - Work Flow of Penetration Testing.

III. EXPERIMENTAL RESULTS

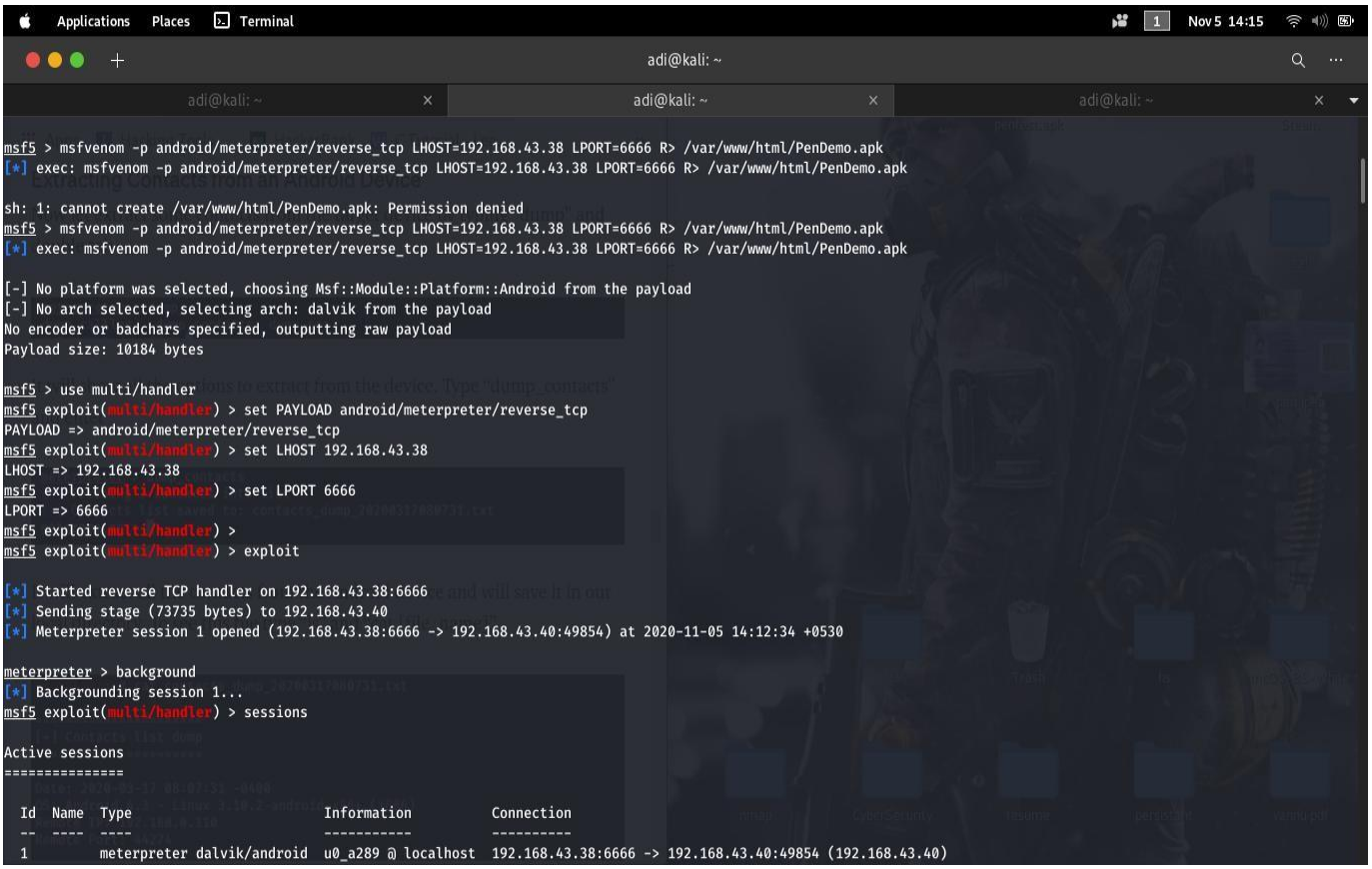

Figure 2 - Creating Payload with Msfvenom

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

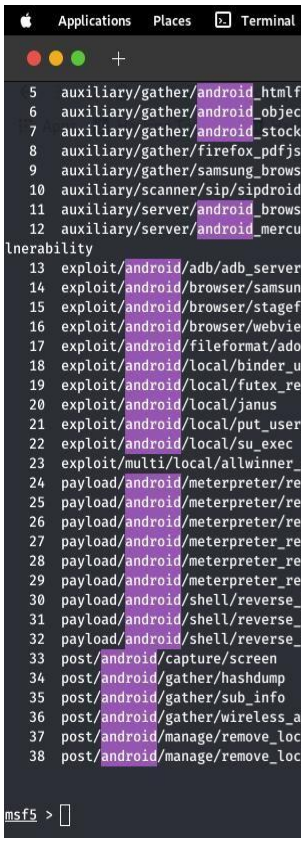

Figure 3 - Vulnerabilities in Android

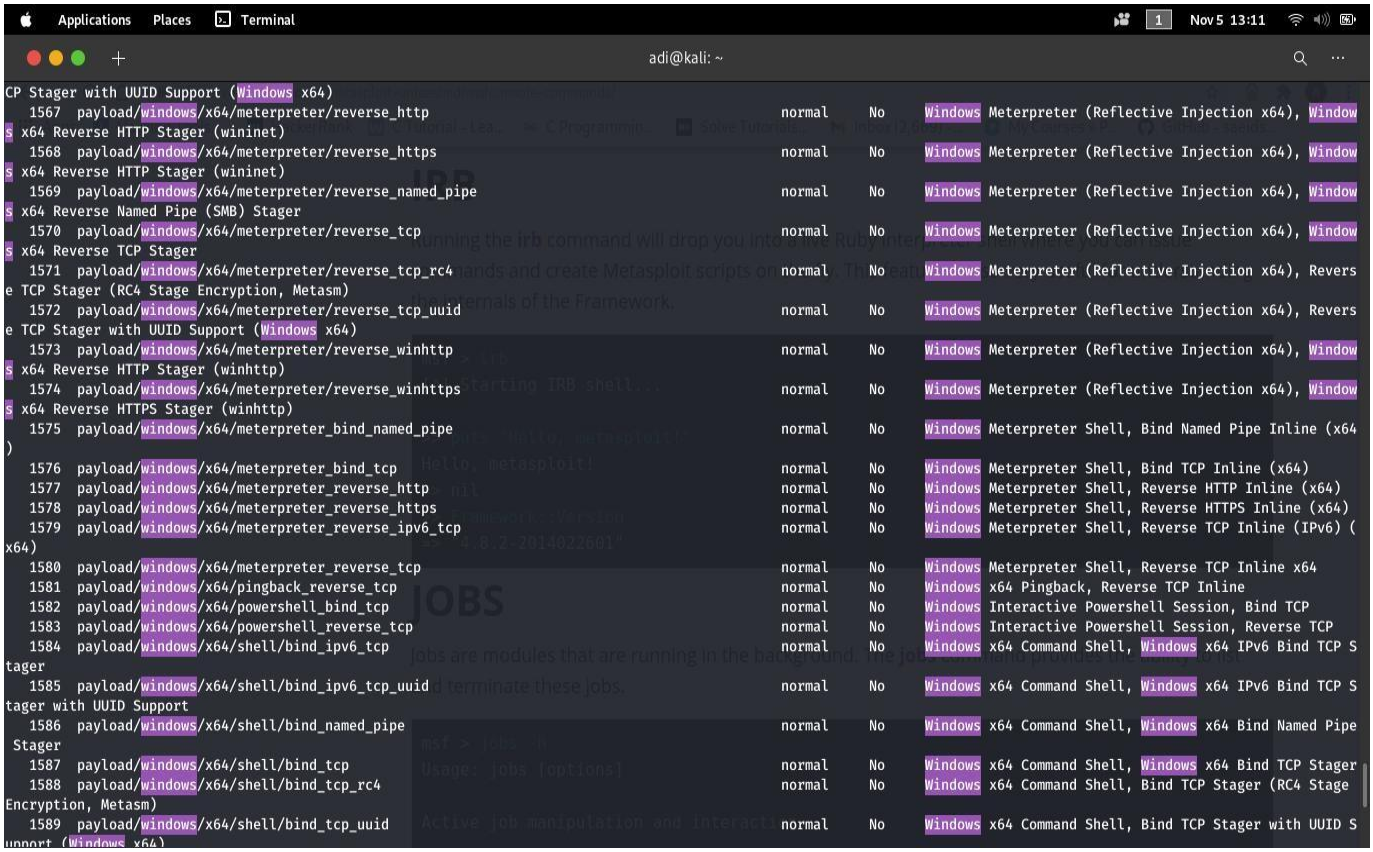

Figure 4 - Vulnerabilities in Windows

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

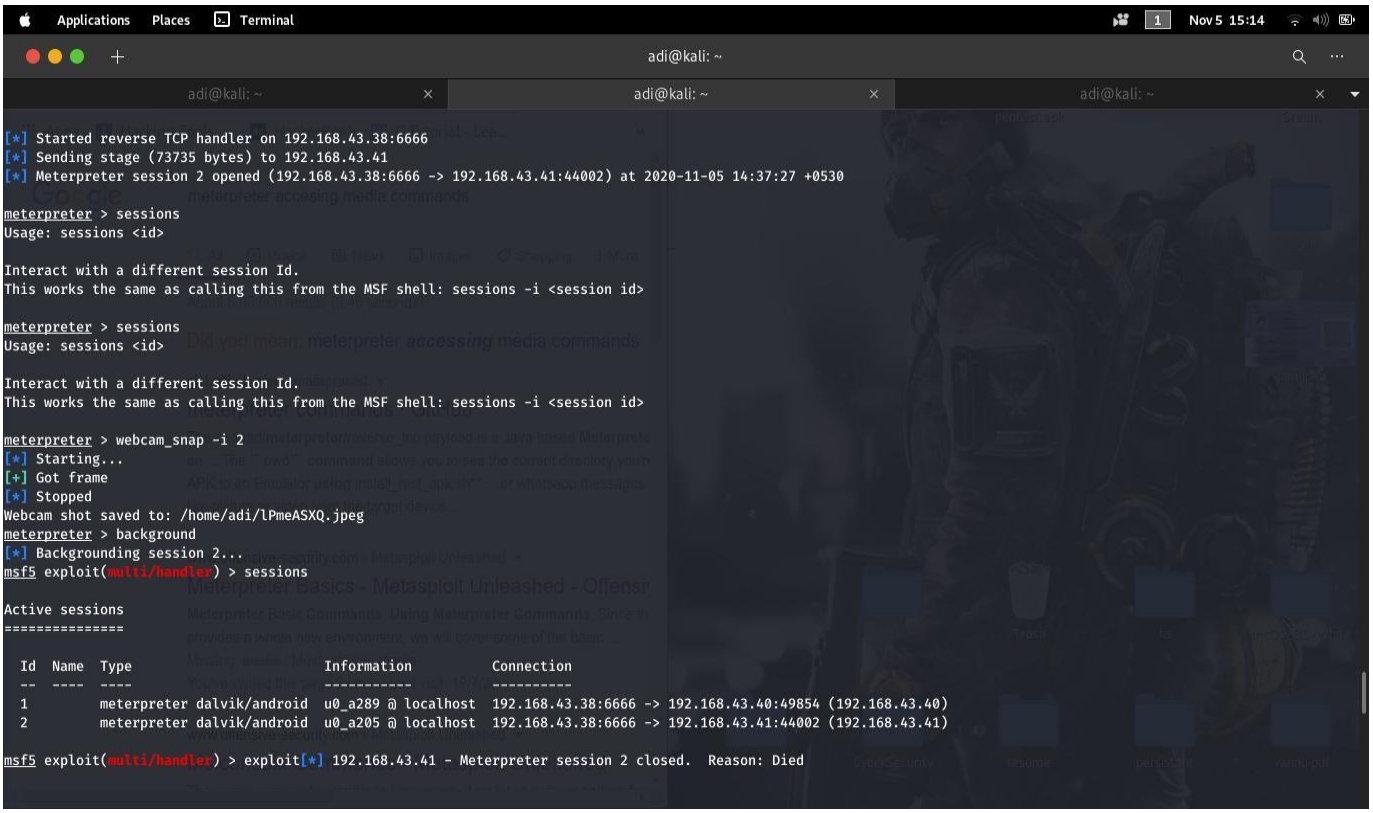

Figure 5 - Deploying Malicious APK File on an Android Device

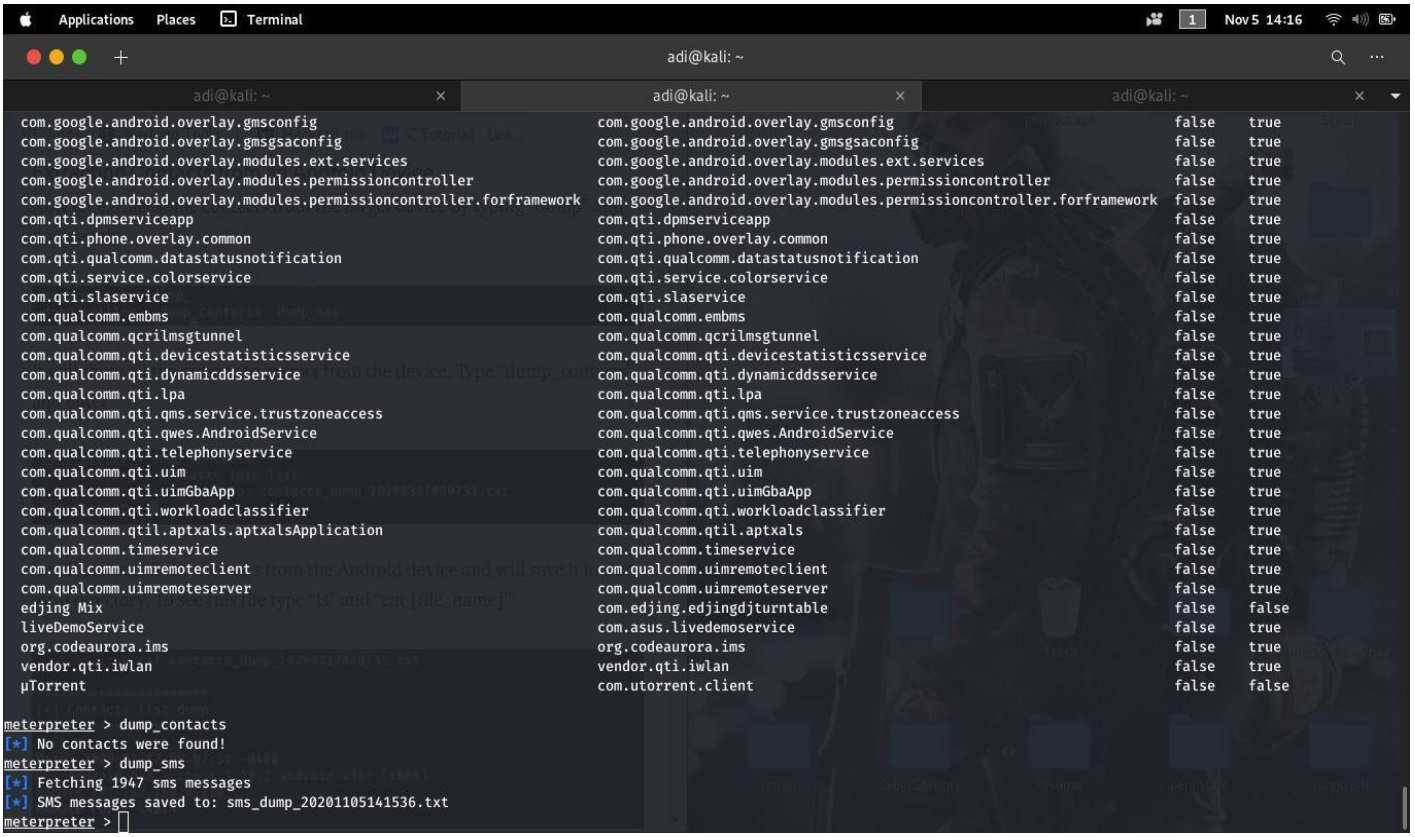

Figure 6 - Accessing maliciously infected device

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Oprating System Used - Kali Linux.

Kali linux is a debian oprating system which is majorly used for cyber security purpose . kali linux provides various tools for testing purposes and virtual setups for hacking labs. In our project we have used msfvenom tool for creating manual payload with backdoor in it . Their are multiple tools like spyderfoot , nessus , nmap which helps to find vulnrabilities in the system . For exploiting windows and to know its vulnrabilities we first run a basic scan on windows machine with the help of nmap scans after running the scan we know about the open ports present in the victims system . after that we just need to find out the proper payloads and exploits to Hack the system and then we can provide the solution on that particular vulnrability.

Creating Payload with Msfvenom.

Figure 2 shows the creation of malware infected file with the help of msfvenom tool. In This we have created a manual payload with the help of MSF venom tool of Kali Linux it will create a backdoor APK file or Windows malicious file which after planting and the victims device will give the access of his information , while creating this payload we have mention local port and localhost in the command which sets back the listener to the attacker machine.

Vulnerabilities in Android and Windows.

Figure 3 and 4 shows the existing payload and exploits available for android and windows. Their are multiple vulnrabilities in android/windows we need to identify the existing ones in the victims device . we can see the exploits and payloads list in the msfconsole which will be furthter used for creating payload and exploits as per need. Both the platform have their security methodologies which tries to protect their systems with regular patch update.

Deploying Malicious APK File on an Android Device.

Figure 5 shows the deployment of malware into victims device with the help of simlehttp server. For deploying the infected Payalod on the victims device we can generate a link for downloading infected file aur create simple http server so that victim can download it. In Another ways we can create a adware and bind the infected file on its back end. In Android we can bind our infected APK to the original APK so that victim is unable to identify that there is a Malware backdoor in the apk.

Accessing maliciously infected device.

Figure 6 shows how we can access the device. Once work time downloaded the malicious APK file or any exe file . After opening the file back door will establish a connection with attackers pc with the help of reverse TCP shell bat shell is known as meterpreter shell it will provide the complete access of victim system in such way we can download victims personal data .

CONCLUSION

The presented work on the penetration testing of Windows and Android. The access to open source platform make it easier for unauthorized users to have the advantage of this, if not properly handled. The researched work comes to conclusion that all software has some security vulnerabilities. In order to reduce the exposure of the device to unauthorized access, one must take into consideration that user should protect and secure their device using different ways: Introduce password and lock screen to device. Before installing any application to the device, please go throw application review and permission access. As once the ports are accessible then device is exposed to unauthorized users. Never download applications or open any shared files from unknown users. After testing the payloads on both the platform we observe that both the platform have their weaknesses. On some measure security tests android is secured in sense of its application Security and windows is for protecting the system from viruses and malicious file Make sure to use anti-virus and constantly update the device.

REFRENCES

[1] Bishop, M. (2007) “About Penetration Testing,” IEEE Security & Privacy, November/December 2007, pp. 84-87.

[2] Vulnerability Assessment and Penetration Testing http://www.aretecon.com/aretesoftwares/ vapt.html

[3]Pfleeger, C. P., Pfleeger, S. L., and Theofanos, M. F. (1989) “A Methodology for Penetration Testing,” Computers &Security, 8(1989) pp. 613-620.

[4] Neumann, P. (1977) “Computer System Security Evaluation,” Proceedings of AFIPS 1977 Natl. Computer Conf., Vol. 46, pp. 1087-1095.

[5] Arkin, B., Stender, S., and McGraw, G. “Software Penetration Testing,” IEEE Security & Privacy, January/Feburary 2005, pp. 32-35.

[6] “Penetraion Testing Guide”, http://www.penetration-testing.com/

[7] iVolution Security Technologies, “Benefits of Penetration Testing,”

Copyright © Authors

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731