International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)
Impact Factor: 3.45 (SJIF-2015), e-ISSN: 2455-2585
Volume 4, Issue 5, May-2018

Network Security Implementation using Penetration Testing

Ms. Komal[1]

[1] *Department of Computer Science, Amity University Haryana, Komal.sang@gmail.com,*

Abstract— ***There are plethora of tools and techniques utilized by network administrators to ensure better network security including firewalls, Intrusion Detection/ Prevention Systems, Multi-layered Demilitarized zones, proxy servers, traffic analysis tools, logging capabilities etc. Vulnerability assessment still holds a critical role to evaluate the deployed security and suggest mitigation measures for the concerns. Penetration testing is a step further that emulates the attacker actions to completely exploit system services. It generates a snapshot of actual impact on network when the multiple vulnerabilities are exploited. Pen testing has provided a new dimension to network security and its deployment. BackTrack Linux as well as Kali Linux has numerous tools to assist in the process of penetration testing. This paper provides an overview of essentials of penetration testing and password cracking along with experimental results.***

Keywords— Penetration Testing, Pen Test, BackTrack Linux, Kali Linux, Password Cracking.

I. INTRODUCTION

The security hazards for organizations, associations, and agencies that work with delicate information are more than obvious. As a rule, these organizations are not ready to comprehend the augmentation of the genuine complex correspondence structures and have only a next to zero control of them. Besides, these dangers are significantly greater when applications that keep running on their processing infra-structures are contemplated. The dangers that are not controlled may expand the magnitude of security assaults that can turn out to be enormous money related misfortunes.

For the most part, security can be ensured by some insurance components: prevention, detection and reaction techniques[1]. Preventive action is the way toward attempting to prevent gatecrashers from accessing the assets of the framework. Detection happens when the attacker has succeeded or is in the procedure of accessing framework. At long last, reaction is an eventual outcome instrument that tries to react to the disappointment of the initial two systems. It works by endeavouring to stop and additionally avert future harm or access to network infrastructure. In any case, evaluating the security state is nonstop and important errands to comprehend the dangers there exist. This evaluating is typically performed through security tests[2]. In this way, the utilization of the correct systems for security testing is a critical assignment to limit the current security hazards in any enterprise [3].

One of the known structures to survey the condition of security and potential security dangers is called penetration test (Pen-test). Pen-test is a controlled provisional to infiltrate into a framework or system with a specific end goal to recognize vulnerabilities. Pen-test applies similar methods that are utilized as a part of a normal assault by a programmer. This option permits that suitable measures are taken keeping in mind the end goal to dispense with the vulnerabilities before they can be investigated by unapproved individuals [4].

The paper is further organized as follows: Section II explains different approaches to penetration testing and their required process/tools. Section III presents implementation results of penetration testing along with password cracking using dictionary /database keywords. Section IV concludes the results and findings.

II. APPROACHES TO PENETRATION TESTING

The procedure to apply penetration testing can be an approach to assess the security level of a framework. The more vigorous the Pen-test is, the deeper is the assessment of the shortcoming/quality of security framework. Penetration testing can be categorized into white box, black box and gray box testing [5] .It can be performed manually, automated or in a combination of manual and automation testing. Tools used by automation testing include NMap, Nessus, Wireshark, Veracode and Metasploit [6].Following sequence of operations is applied to perform penetration testing[2][7][8]:

A. *Reconnaissance*-Reconnaissance is the systematic approach where you attempt to locate and gather information on your target; others may refer to this part as ‘foot-printing’. The techniques involved in foot-printing include, social engineering (great fun), internet research and ‘Dumpster-Diving’. Some of the open-source and free tools that can be used for this purpose are- nslookup, traceroute, ping, wois, google and social networking. Nslookup is an awesome tool to use when using Kali and is used to resolve a fully qualified domain name into an IP address. Traceroute is a great tool for seeing where your ‘ping’ goes before it hits the system you are actually trying to ping, it displays the path between you and your target. Traceroute is a great tool for seeing where your ‘ping’ goes before it hits the system you are actually trying to ping, it displays the path between you and your target. Whois provides information on the owner of the domain itself with information like, server addresses, phone numbers, owners name, owners addresses. Google is the best source for finding information on a company and can give you all the open source information that you could wish for. Social media (Facebook, LinkedIn, Twitter, etc.) is an absolute gold mine for information and great way to launch spear phishing campaigns against personal targets at the targeted company. The vast information collected from these tools can be used to craft legitimate looking phishing attacks.

B. *Vulnerability and Risk Assessment-Based* on the data collected via first step, security weakness in the target system can be identified with ease. This helps penetration testers to launch attacks using identified entry points *in the system.*

C. *Actual Exploitation*-This being the crucial step, it requires special skills and techniques to launch attack on target system. Experienced penetration testers can use their skills to launch attack on the system. Password cracking[8] is also a way to penetrate into system or exploit the system.

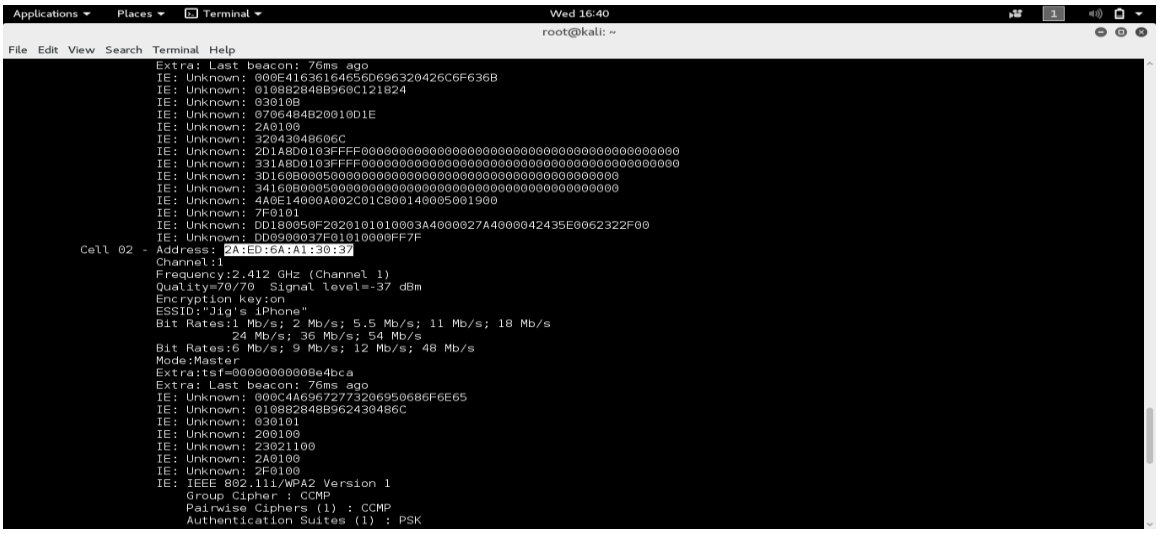
D. *Post-Exploitation* –In this phase [1], we will learn to exploit our targets further, escalating privileges and penetrating the internal network even more. Meterpreter scripts which is the heart of this chapter, makes the post-exploration phase quite easier. Meterpreter contains many built-in scripts written in ruby; we can also add and modify Meterpreter scripts based on our requirements or just for exploration.

E. *Analysis and reporting*- This phase gathers the facts and the extent of impact on network. Finally, penetration testing reports can be prepared to provide insights to the management about the severity of security weaknesses and their impact on business loss.

III. RESULTS

A. Password Cracking

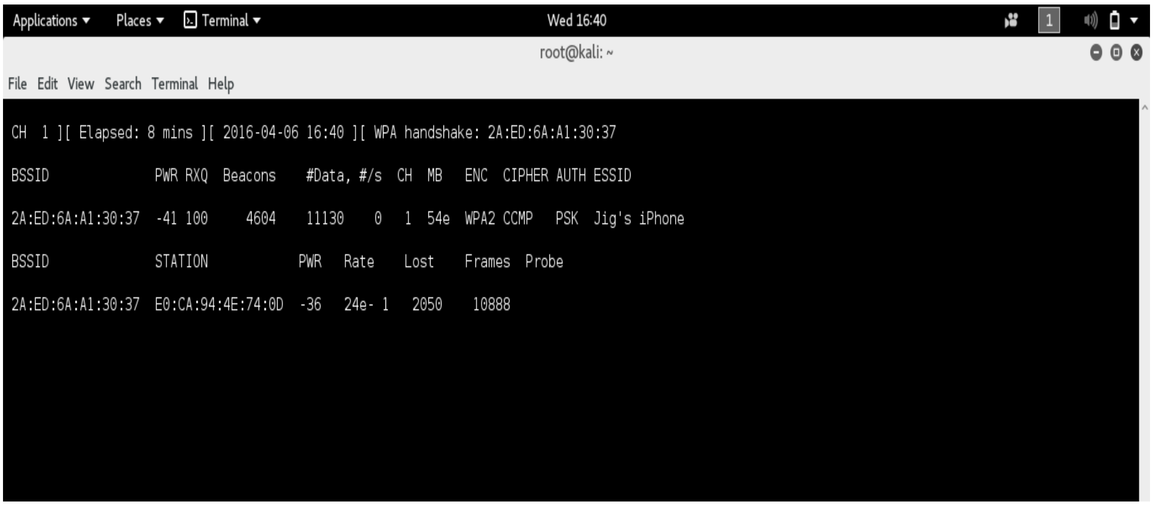
With this type of Attacks, Hackers create a database including possible passwords used by clients, Facebook account names, Dictionary words with combination of numbers and special characters. A command is run to discover Access points or available networks details of devices as shown in Fig 1.



```
                    Extra: Last beacon: 76ms ago
                    IE: Unknown: 000E41636164656D696320426C6F636B
                    IE: Unknown: 010882848B960C121824
                    IE: Unknown: 03010B
                    IE: Unknown: 0706484B20010D1E
                    IE: Unknown: 2A0100
                    IE: Unknown: 32043048606C
                    IE: Unknown: 2D1A8D0103FFFF000000000000000000000000000000000000000000
                    IE: Unknown: 331A8D0103FFFF000000000000000000000000000000000000000000
                    IE: Unknown: 3D160B000500000000000000000000000000000000000000
                    IE: Unknown: 34160B000500000000000000000000000000000000000000
                    IE: Unknown: 4A0E14000A002C01C800140005001900
                    IE: Unknown: 7F0101
                    IE: Unknown: DD180050F2020101010003A4000027A4000042435E0062322F00
                    IE: Unknown: DD0900037F01010000FF7F
          Cell 02 - Address: 2A:ED:6A:A1:30:37
                    Channel:1
                    Frequency:2.412 GHz (Channel 1)
                    Quality=70/70  Signal level=-37 dBm
                    Encryption key:on
                    ESSID:"Jig's iPhone"
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 18 Mb/s
                              24 Mb/s; 36 Mb/s; 54 Mb/s
                    Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 48 Mb/s
                    Mode:Master
                    Extra:tsf=00000000008e4bca
                    Extra: Last beacon: 76ms ago
                    IE: Unknown: 000C4A6967277320695068 6F6E65
                    IE: Unknown: 010882848B962430486C
                    IE: Unknown: 030101
                    IE: Unknown: 200100
                    IE: Unknown: 23021100
                    IE: Unknown: 2A0100
                    IE: Unknown: 2F0100
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
```

Fig. 1 Capturing Information of a Device within a Network

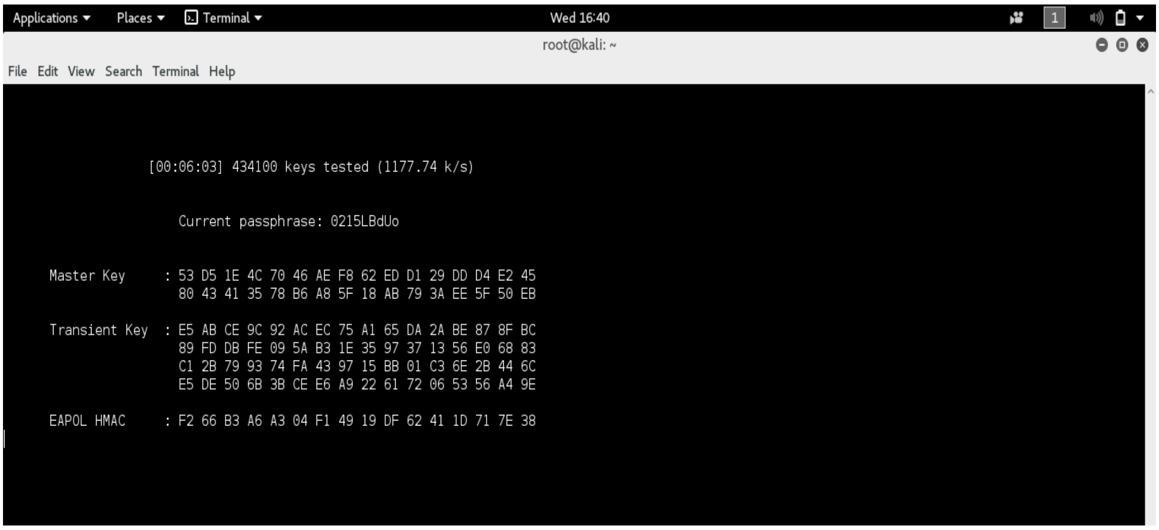
The handshake between the device and another device is then captured as shown in Figure 2.



```
CH  1 ][ Elapsed: 8 mins ][ 2016-04-06 16:40 ][ WPA handshake: 2A:ED:6A:A1:30:37

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

2A:ED:6A:A1:30:37  -41 100     4604    11130    0   1  54e  WPA2 CCMP   PSK  Jig's iPhone

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

2A:ED:6A:A1:30:37  E0:CA:94:4E:74:0D  -36   24e- 1   2050    10888
```

Fig. 2 Capturing the Handshake

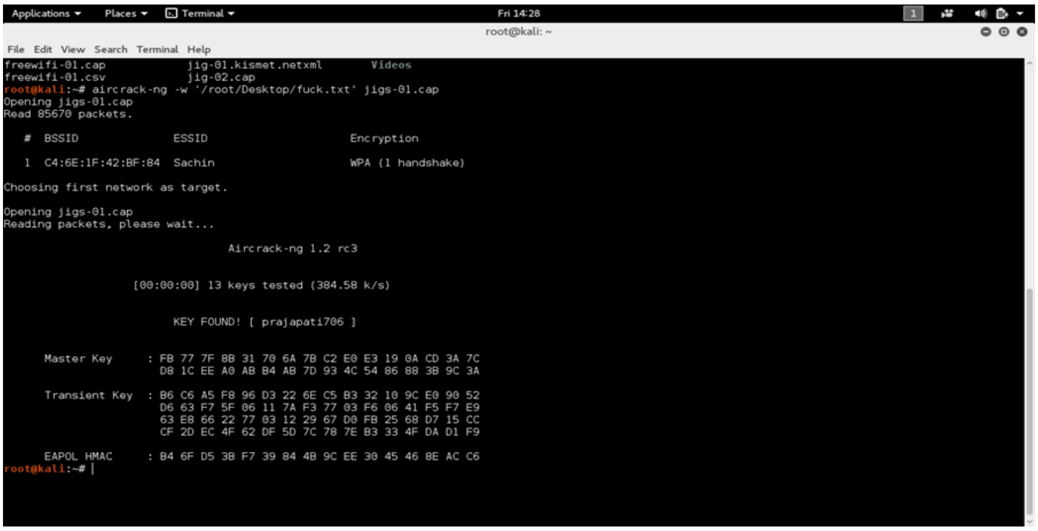
A script is run and if the password matches with any of the set of strings in the database, the password can be found as shown in Fig. 3.



```
                   [00:06:03] 434100 keys tested (1177.74 k/s)


                       Current passphrase: 0215LBdUo


      Master Key     : 53 D5 1E 4C 70 46 AE F8 62 ED D1 29 DD D4 E2 45
                       80 43 41 35 78 B6 A8 5F 18 AB 79 3A EE 5F 50 EB

      Transient Key  : E5 AB CE 9C 92 AC EC 75 A1 65 DA 2A BE 87 8F BC
                       89 FD DB FE 09 5A B3 1E 35 97 37 13 56 E0 68 83
                       C1 2B 79 93 74 FA 43 97 15 BB 01 C3 6E 2B 44 6C
                       E5 DE 50 6B 3B CE E6 A9 22 61 72 06 53 56 A4 9E

      EAPOL HMAC     : F2 66 B3 A6 A3 04 F1 49 19 DF 62 41 1D 71 7E 38
```

Fig. 3 Matching the Password against database

After running the script of the database, if the password is found in the database it has been cracked as shown in figure 4.

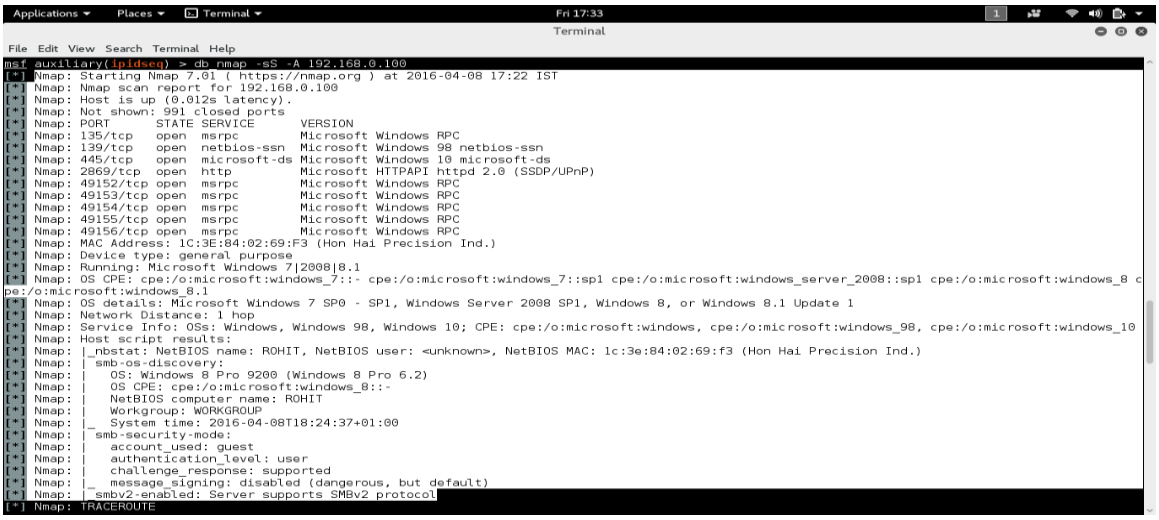


```
freewifi-01.cap            jig-01.kismet.netxml       Videos
freewifi-01.csv            jig-02.cap
root@kali:~# aircrack-ng -w '/root/Desktop/fuck.txt' jigs-01.cap
Opening jigs-01.cap
Read 85670 packets.

   #  BSSID              ESSID                     Encryption

   1  C4:6E:1F:42:BF:84  Sachin                    WPA (1 handshake)

Choosing first network as target.

Opening jigs-01.cap
Reading packets, please wait...

                                 Aircrack-ng 1.2 rc3


                   [00:00:00] 13 keys tested (384.58 k/s)


                          KEY FOUND! [ prajapati706 ]


      Master Key     : FB 77 7F 8B 31 70 6A 7B C2 E0 E3 19 0A CD 3A 7C
                       D8 1C EE A0 AB B4 AB 7D 93 4C 54 86 88 3B 9C 3A

      Transient Key  : B6 C6 A5 F8 96 D3 22 6E C5 B3 32 10 9C E0 90 52
                       D6 63 F7 5F 06 11 7A F3 77 03 F6 06 41 F5 F7 E9
                       63 E8 66 22 77 03 12 29 67 D0 FB 25 68 D7 15 CC
                       CF 2D EC 4F 62 DF 5D 7C 78 7E B3 33 4F DA D1 F9

      EAPOL HMAC     : B4 6F D5 3B F7 39 84 4B 9C EE 30 45 46 8E AC C6
root@kali:~# |
```

Fig.4 Results of Password Cracking

B. Penetration Testing

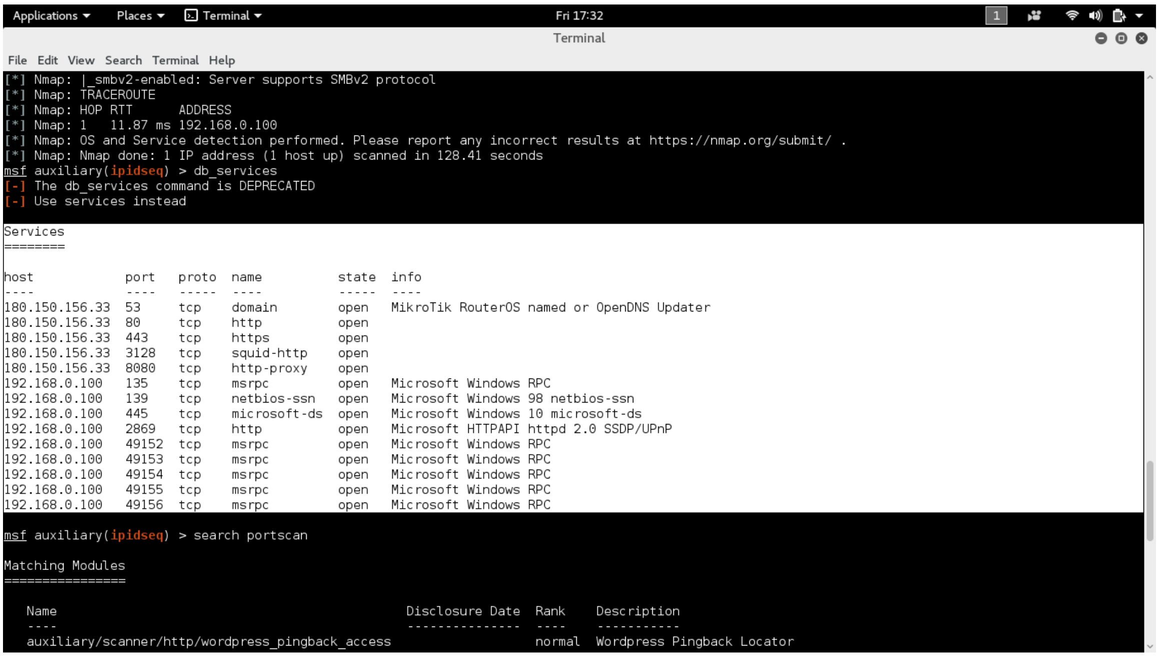
Vulnerability Scanning was done as part of the penetration test. This was implemented on a Kali Linux platform. A series of open ports, network distance, operating system details, NetBIOS name, workgroup name and authentication level of the system can be captured as in figure 5.



```
msf auxiliary(ipidseq) > db_nmap -sS -A 192.168.0.100
[*] Nmap: Starting Nmap 7.01 ( https://nmap.org ) at 2016-04-08 17:22 IST
[*] Nmap: Nmap scan report for 192.168.0.100
[*] Nmap: Host is up (0.012s latency).
[*] Nmap: Not shown: 991 closed ports
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 135/tcp   open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp   open  netbios-ssn  Microsoft Windows 98 netbios-ssn
[*] Nmap: 445/tcp   open  microsoft-ds Microsoft Windows 10 microsoft-ds
[*] Nmap: 2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
[*] Nmap: 49152/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49153/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49154/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49155/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: 49156/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: MAC Address: 1C:3E:84:02:69:F3 (Hon Hai Precision Ind.)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Microsoft Windows 7|2008|8.1
[*] Nmap: OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8 c
pe:/o:microsoft:windows_8.1
[*] Nmap: OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows 8, or Windows 8.1 Update 1
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: OSs: Windows, Windows 98, Windows 10; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_98, cpe:/o:microsoft:windows_10
[*] Nmap: Host script results:
[*] Nmap: |_nbstat: NetBIOS name: ROHIT, NetBIOS user: <unknown>, NetBIOS MAC: 1c:3e:84:02:69:f3 (Hon Hai Precision Ind.)
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Windows 8 Pro 9200 (Windows 8 Pro 6.2)
[*] Nmap: |   OS CPE: cpe:/o:microsoft:windows_8::-
[*] Nmap: |   NetBIOS computer name: ROHIT
[*] Nmap: |   Workgroup: WORKGROUP
[*] Nmap: |_  System time: 2016-04-08T18:24:37+01:00
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: guest
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
[*] Nmap: |_  message_signing: disabled (dangerous, but default)
[*] Nmap: |_smbv2-enabled: Server supports SMBv2 protocol
[*] Nmap: TRACEROUTE
```

Fig. 5 Nmap Results

Figure 6 is a check to show the results from the scan are stored in the database.



```
[*] Nmap: |_smbv2-enabled: Server supports SMBv2 protocol
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1   11.87 ms 192.168.0.100
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 128.41 seconds
msf auxiliary(ipidseq) > db_services
[-] The db_services command is DEPRECATED
[-] Use services instead

Services
========

host            port   proto  name          state  info
----            ----   -----  ----          -----  ----
180.150.156.33  53     tcp    domain        open   MikroTik RouterOS named or OpenDNS Updater
180.150.156.33  80     tcp    http          open
180.150.156.33  443    tcp    https         open
180.150.156.33  3128   tcp    squid-http    open
180.150.156.33  8080   tcp    http-proxy    open
192.168.0.100   135    tcp    msrpc         open   Microsoft Windows RPC
192.168.0.100   139    tcp    netbios-ssn   open   Microsoft Windows 98 netbios-ssn
192.168.0.100   445    tcp    microsoft-ds  open   Microsoft Windows 10 microsoft-ds
192.168.0.100   2869   tcp    http          open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.0.100   49152  tcp    msrpc         open   Microsoft Windows RPC
192.168.0.100   49153  tcp    msrpc         open   Microsoft Windows RPC
192.168.0.100   49154  tcp    msrpc         open   Microsoft Windows RPC
192.168.0.100   49155  tcp    msrpc         open   Microsoft Windows RPC
192.168.0.100   49156  tcp    msrpc         open   Microsoft Windows RPC

msf auxiliary(ipidseq) > search portscan

Matching Modules
================

   Name                                            Disclosure Date  Rank    Description
   ----                                            ---------------  ----    -----------
   auxiliary/scanner/http/wordpress_pingback_access                 normal  Wordpress Pingback Locator
```

Fig. 6 Results as shown in Database

IV. Conclusions

The pertinence of the penetration testing (Pen-test) is clear from the perspective of network and application security. This area has been generally focused by analysts of testing and security, essentially since the quantity of imperfections and vulnerabilities has expanded in the most recent years. This paper concentrated on performing the Penetration testing using nslookup, Nmap, Metasploit tool and password cracking hacks. It was conceivable to reach a few inferences on how some of the unattended issues in network settings and security can be utilized to perform scans, examining, pre-intrusion, hacking and post-attack consequences. From that, the outcomes can assist analyzers with defining, inside their testing extension, better security controls. In this way, a proposed set of suggestions would address the qualities and confinements of the models and furthermore would give an adaptable, dynamic, and numerous exercises decisions, steps, and different viewpoints intrinsic to a penetration testing approach.

REFERENCES

[1] R. Baloch, *Ethical Hacking and Penetration Testing Guide,*, CRC Press, 2015.

[2] G. Weidman, *Penetration Testing: A Hands-on Introduction to Hacking*, No Starch Press, 2014.

[3] A. Narang, "A review-Cloud and cloud security", *International journal of Computer Science and mobile Computing*, vol. 6, issue 1,pp. 178-181, 2017.

[4] D.D. Bertoglio, A.F. Zorzo, "Overview and open issues on penetration test", *Journal of Brazilian Computer Society*, pp. 1-16, 2017.

[5] S Kaushal, J.K. Bajwa, "Analytical Review of User Perceived Testing Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, issue 10, 2012.

[6] Komal, "Design and Deployment of Secure Enterprise Network Framework*", International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 7, Issue 5, pp.200-203, 2017.

[7] Online source, [Available] https://www.360logica.com/blog/different-methodologies-penetration-testing/, 2018.

[8] D. Holdsworth, "Penetration Testing Methodology",https://medium.com/dvlpr/penetration-testing-methodology-part-1-6-recon-9296c4d07c8a, 2018.

[9] S. Martin, and M. Tokutomi, "Password Cracking", https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic7-final/report.pdf, 2018.