**Advanced Penetration Testing for Highly Secured Environments**

Asif Nawaz1

1Department of Computer Sciences

University of Wah

[Prince\_club55@yahoo.com](mailto:Prince_club55@yahoo.com)

ABSTRACT

Perform an effective, organized, and effective assessment test from begin to end. Gain hands-on hacking and assessment test experienced by building a virtual lab setup that includes commonly known security problems such as IDS/IPS and firewalls misconfiguration or vulnerabilities. Take the challenging task and perform a virtual assessment test process against a fictional organization from begin to end and then verify your results by walking through step-by-step solutions. Fully Detailed step-by-step guidance on managing tests results and writing clearly organized and effective penetration testing reports for highly secure environment. Understand in detail how assessment process works from begin to end, not just how to use specific tools and methods. Using advanced methods to bypass security measures and remain undetected while testing. Creating a segmented virtual environment with several targets, IDS/IPS and firewalls. Generating testing reports and statistics. This paper is proposed for someone that has a solid background in information security the step-by-step guidelines make it easy to follow for all skill levels.

**Keywords**: Penetration Testing, Advance Security Testing.

**1.** INTRODUCTION:

1. advance penetration testing

Penetration testing is necessary to conclude the true attack footprint of your setting. It may often be mixed up with vulnerability testing and thus  
it is important that the variances should be fully explained to your clients. [1]

**2. VULNERABILITY ASSESSMENT**

Vulnerability assessments are necessary for determining vulnerabilities throughout the environment. There are many tools available for this process so that security professional or administrator can effectively determine the security of their environment. Depending on scope, manual vulnerability testing may also be mandatory. Full exploitation of systems and services is not normally in scope for a standard vulnerability testing arrangement. Systems are usually enumerated and assessed for vulnerabilities/flaws, and testing can often be done with or without proper authentication. [1]

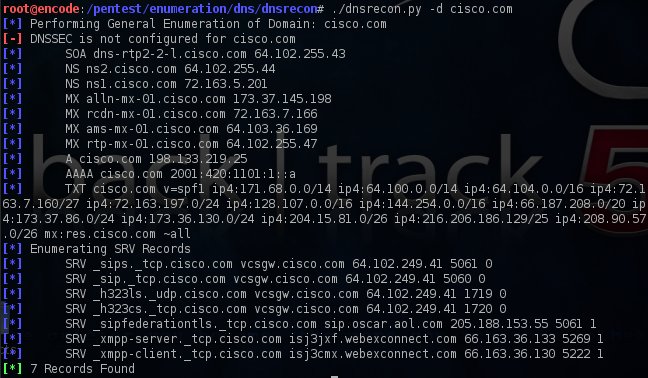
## ADVANCED RECONNAISSANCE TECHNIQUES

### INTRODUCTION TO RECONNAISSANCE

Information is the key to success when performing an assessment test.  
The amount of data that is available on the Internet is surprising, and filtering  
through it all to find useful information can be a frightening task. There are some available tools that assist us in gathering and categorization through this riches of knowledge. Now we will focus on how to use this kind of information to ensure your assessment tests are efficient and effective. [2]

### DNS RECON

DNS recon is an important part of the information gathering at the stage of assessment test .When a PENTESTER (Penetration Tester) is performing a DNS recon is trying to obtain as much as information as he can regarding the DNS servers and their logs. The information that can be collected it can disclose the network structure of the company without alerting the intrusion detection system/ Intrusion prevention system. This is due that most of the organizations are not checking their DNS server traffic. [2]

****

**Figure 1: DNS Recon**

### Domain Information Groper (Dig)

DIG is a network-administration tool for enquiring DNS name servers. It is useful for authenticating and troubleshooting Domain name server problems and also to perform Domain name server lookups and displays the results that are returned from the name server that were demanded. Dig is part of the BIND domain name server software suite. [2]

### GATHERING INFORMATION WITH WHOIS

The most common usage of WHO-IS is as follows:  
  
This will perform a quick lookup of the example.com domain and provide you with the following information:   
• WHO-IS usage agreements and legal headers.  
• Domain name information.   
• Registrar information and the domain name is registered with.  
• WHOIS server that was used  
the primary DNS domain name servers associated with the domain  
• Domain creation and expiration dates  
• Registrant information e-mail, name, contact number, organization name.  
• Assigned domain administrator information such as First Name, Last Name, Organization, physical address, contact number, and mailing address.  
• Domain billing contact information such as First Name, Last Name,  
Organization, physical address, phone number, and e-mail address.  
• Domain technical contact information such as First Name, Last Name,  
Organization, geological address, contact number, and mailing address. [2]

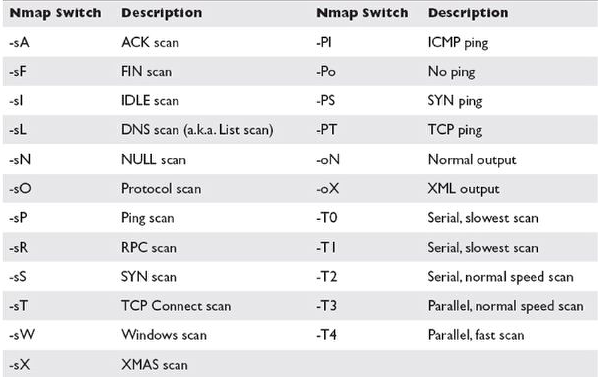
# Enumeration: Choosing TArget

To successfully penetrate a highly secured environment you must have a better understanding of what you are facing. The enumeration data assembled will assist in defining  
target prioritizing. You should be able to choose which targets are ideal candidates for your initial attack process. Certain attack types make more "noise" than others, thus a best selected targeted attack will be less likely to be noticed. We have a large selection of tools available to that are use enumerate target.

### NMAP

NMAP is a scanner originally used to discover hosts and services on a computer network, and create a complete map of the targeted network. NMAP provides various types of scans to perform this task. Some of them might be less noisy.

Different switches are used to perform different type of scan. [5]



**Figure 2: NMAP Switches**

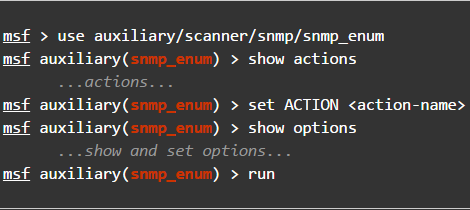
NMAP results contains information:

* Open Ports on targeted system
* Services running
* Operating system of System (in some cases)

### SNMP ENUM

Allows enumeration of any device that are using SNMP protocol. It supports hardware, software, and network information.

For this paper I am using MSF framework at Ubuntu Platform. [3]



**Figure 3: SNMP Auxiliary Scanner**

This auxiliary module results contains:

* System information.
* Network information.
* Services running on devices.
  1. **VULNERABILITY ASSESSMENT**

Vulnerability Mapping is a process of identifying the critical security  
flaws in the target system. This terminology is also known as  
vulnerability assessment. It is one of the key areas of the vulnerability management program through which the security controls of an IT structure can be analyzed against known and unknown vulnerabilities. Once the processes of information collecting, discovery, and enumeration have been completed, it is time to investigate the vulnerabilities that may exist in the targeted infrastructure which could lead  
to a compromise of the target and violation of the confidentiality, integrity, and availability of a business system.

### LOCAL VULNERABILITIES

A system on which the attacker need local access in order to trigger the  
vulnerability by executing a piece of code is known as Local Vulnerability. Considering this type of flaw, an attacker can increase the access privileges to gain unrestricted access to the system.

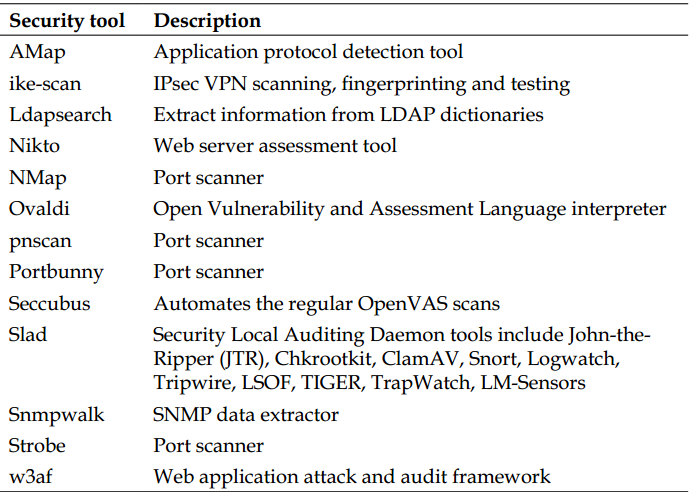
### REMOTE VULNERABILITIES

### A system to which the attacker has no previous local access but the vulnerability of which can still be exploited by triggering the malicious piece of code (exploit) remotely or over the network is known as "remote vulnerability". This type of vulnerability allows an attacker (Hacker) to get remote access to the system without facing any physical or local obstacles.

### OPENVAS

### The OPENVAS is a collection of security tools and services that offer a powerful platform for vulnerability assessment. It has been developed on the foundation of client-server architecture, where the client requests a specific set of network vulnerability tests in contradiction of its target from the server. Its modular and robust design allows us to track the security tests in parallel and also available for almost all of operating systems (Linux/Win32). [7]

Tools available in OPENVAS:



**Figure 4: OPENVAS Tools List**

OPENVAS gives us classifying information about target system. Also return us security flaw available in target system that can be exploited locally or remotely.

### NESSUS

### Nessus is an open-source vulnerability scanner that uses the common Vulnerabilities and Exposures architecture for easy cross-linking between security tools. Nessus works on Nessus Attack Scripting Language (NASL), a simple language that describes threats and potential attacks.

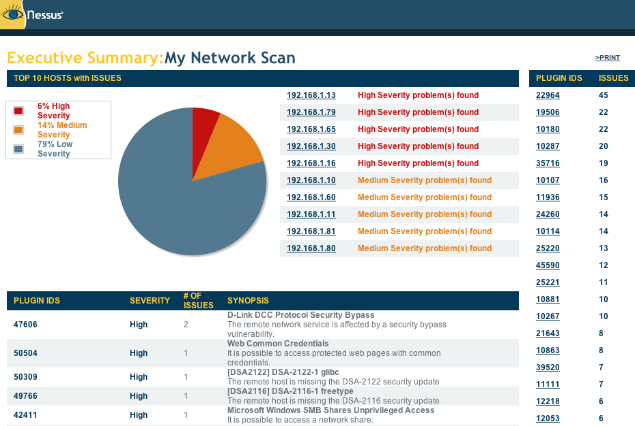
Nessus gives us lots of options when it executing the actual vulnerability scan process. We’ll be able to scan signal computer, ranges of IP address, complete network/subnet. There are large range of vulnerability plugins with Nessus using which we’ll be able to specify individual or set of vulnerabilities to test. In contrast to other tools Nessus won’t assume for explicit services running on common ports instead it will try to exploit the vulnerabilities. Nessus provide large number for policies for target testing. [4]



**Figure 5: NESSUS Environment**

At the end of the process Nessus will generate a report showing critical/non-critical vulnerabilities that are present in system and can be exploited to compromise the system security.

Nessus Report Example:



**Figure 6: NESSUS Final Report**

Clearly it indicates all critical/ non- critical vulnerabilities.

* 1. **EXPLOITATION VULNERABILITIES**

After completing our vulnerability scanning steps, we now have the complete knowledge necessary to attempt to launch exploits against our target system. So the exploitation process start. Exploitation is process of in which attacker can use malicious piece of code (Exploit) to get access to a system by taking advantage of vulnerabilities present in system.

### METASPLOIT FRAMEWORK (MSF)

The Metasploit framework is more than a huge exploit dump. It’s a framework that you can build upon and utilize for your needs. This allows you to focus on your environment, and not have to reinvent the wheel. I consider the MSF to be one of the single most useful auditing tools for security professionals. From a wide array of commercial grade exploits (piece of code) and an extensive exploit development environment, all the way to network information gathering tools and web vulnerability/assessment plugins, the Metasploit Framework provides a truly impressive work environment. MSF provide different type of stubs. [3]

#### *SHELLCODE*

A SHELLCODE is a piece of code (stub) used as the payload in the exploitation process of a system vulnerability. It is called SHELLCODE because it normally starts a command shell (reverse shell/ bind shell) from which the attacker can control the compromised machine. [3]

***1.4.1.2 PAYLOAD***

A payload refers to the component of a computer virus that executes a malicious activity. Apart from the speed in which a virus spreads, the threat level of a virus is calculated by the damages it causes. Viruses with more powerful payloads tend to be more harmful. Although not all viruses carry a payload, a few payloads are considered extremely dangerous. Some of the payloads are data destruction, offensive messages and the delivery of spam emails through the infected user's account. A payload is also known as a destructive payload. [3]

***1.4.1.3 Exploits***

A tool developed by attackers that is used to perform malicious attacks on any computer system. They are commonly scripts/codes that are designed to exploit weaknesses (vulnerabilities) in software over a network, most commonly the Internet. [3]

***1.4.2 ATTACKING***

For this paper I have choose window XP as victim machine. I have window XP installed in my VM Ware box. For Attacking Purpose I am using Ubuntu as Attacker Machine.

Some information I have used in attack:

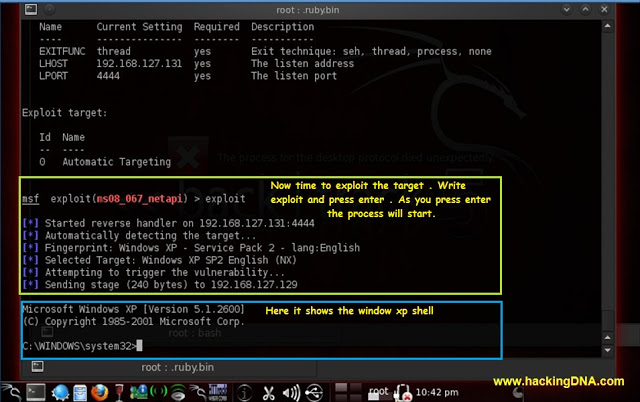
Vulnerability: Netapi

Exploit: ms08\_067\_netapi

Payload: windows/meterpreter/reverse\_tcp

Target: WINDOWS XP SP1 (English)

After executing the exploit payload runs on victim machine, payload launch reverse shell that can provides reverse connection with attacker.



**Figure 7: Attack with MSF**

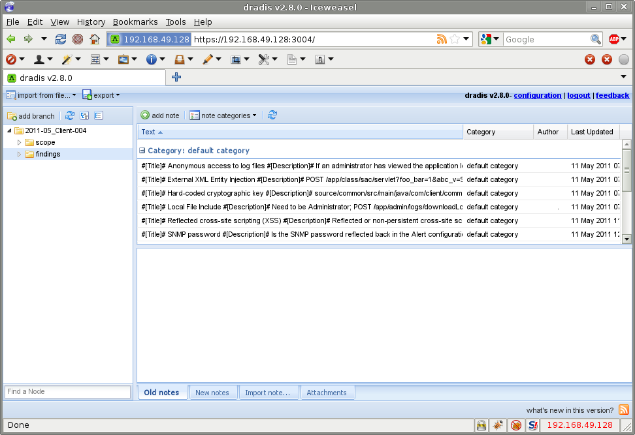
Now we are inside the target system.

* 1. **REPORTING**

Penetration testing report presents the approach used in test and the results of the vulnerability assessment test and penetration test of a system with a detailed recommendation of how to avoid the risks. Different type of tools are available that can present information and generate reports at the end of Penetration testing process. [6]

### DRADIS FRAMEWORK

### The DRADIS is an open-source collaboration and reporting platform for IT security experts. DRADIS is a self-contained web application that provides a centralized source of information to keep track of information that has been done so far, and what is still ahead.



**Figure 8: DRADIS Environment**

DRADIS provide large range of reporting features for storing, classifying, reorganizing and presenting information to customers.

1. **CONCLUSION**

Penetration testing offer insight into an organization’s security efficiency as well as a road map for improving security and avoiding risk. By hiring cyber professionals to simulate a cyber-attack, vulnerabilities can be identified and patched before they are exploited by a hackers (bad guy) or malicious insider.

# 3. REFERENCES

References in the text should be by author for example Li [1], with the reference number in square brackets.

For Communities:

1. ***Offensive Security***.

<http://www.offensive-security.com>

1. ***Sans.org*.**

<http://www.sans.org/>

1. **Rapid7.**

[Metasploit Framwrok](http://www.metasploit.com/)

1. **Tenable Network Security:**

[http://www.tenable.com/](http://www.tenable.com/%20)

[5] **Gordon Lyon,** 1997.

<https://nmap.org/>

[6] **EC-Council CEH v6**

<http://www.eccouncil.org/>

### [7] Greenbone Security Manager 2014

<http://www.openvas.org/>