

## *Tutorials of how to use Metasploit, Nessus and Nmap*

*Obed A. Adames Méndez  
Computer Engineering  
Jeffrey L. Duffany, Ph.D.  
Computer Engineering  
Polytechnic University of Puerto Rico*

---

**Abstract** — *This paper is in support of three newly created tutorials, focused on different Security and Penetration testing tools. The tutorials have been selected to cover three different areas in the security and penetration field. These tutorials are will provide basic understanding on the functionalities and capabilities of each particular tool.*

*Currently there are many different ways to protect our systems. However none of them are 100% secure. We may have severe vulnerabilities in our system and may not be aware of it. Testing our systems for vulnerabilities is something that we should not overlook.*

*The purposed of these tutorials is to give an overview of the free security tools that are available and that we can use to verify the integrity and the security of a network. We will also demonstrate how vulnerabilities can be exploited using this tools.*

**Key Terms** — *Computer Security, Network Scan, Penetration Testing, Vulnerability.*

### **INTRODUCTION**

The term computer security is used frequently, but the content of a computer is vulnerable to few risks unless the computer is connected to other computers on a network. As the use of computer networks, especially the Internet, has become pervasive, the concept of computer security has expanded to denote issues pertaining to the networked use of computers and their resources.

The major technical areas of computer security are usually represented by the initials CIA: confidentiality, integrity, and authentication or availability. Confidentiality means that information cannot be access by unauthorized parties.

Confidentiality is also known as secrecy or privacy; breaches of confidentiality range from the embarrassing to the disastrous. Integrity means that information is protected against unauthorized changes that are not detectable to authorized users; many incidents of hacking compromise the integrity of databases and other resources. Authentication means that users are who they claim to be. Availability means that resources are accessible by authorized parties; "denial of service" attacks, which are sometimes the topic of national news, are attacks against availability. Other important concerns of computer security professionals are access control and nonrepudiation. Maintaining access control means not only that users can access only those resources and services to which they are entitled, but also that they are not denied resources that they legitimately can expect to access. Nonrepudiation implies that a person who sends a message cannot deny that he sent it and, conversely, that a person who has received a message cannot deny that he received it. In addition to these technical aspects, the conceptual reach of computer security is broad and multifaceted. Computer security touches draws from disciplines as ethics and risk analysis, and is concerned with topics such as computer crime; the prevention, detection, and remediation of attacks; and identity and anonymity in cyberspace.

What is penetration testing? Penetration testing, often called "pentesting", "pen testing", or "security testing", is the practice of attacking your own or your clients' IT systems in the same way a hacker would to identify security holes. Of course, you do this without actually harming the network. The person carrying out a penetration test is called a penetration tester or pentester.[1]

The purpose of the newly created tutorials is to provide a basic understanding to new computer security tools users on how computer security works. The tutorials will provide users with the description of the graphical user interface, console applications, examples of how to employ the tool, and practical exercises.

The tutorials are designed around three security tools which are described as follows:

- **Nmap:** (Network Mapper) is a security scanner used to discover hosts and services on a computer network, thus creating a "map" of the network.
- **Nessus:** is a proprietary comprehensive vulnerability scanning program. It is free of charge for personal use in a non-enterprise environment. Its goal is to detect potential vulnerabilities on the tested systems.
- **Metasploit:** is an open-source, computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its most well-known sub-project is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive, and security research.

The Metasploit Project is also well known for anti-forensic and evasion tools, some of which are built into the Metasploit Framework.

## NMAP

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich)[2] used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target

interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

Nmap features include:

- Host Discovery - Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.
- Port Scanning - Enumerating the open ports on one or more target hosts.
- Version Detection - Interrogating listening network services listening on remote devices to determine the application name and version number.
- OS Detection - Remotely determining the operating system and some hardware characteristics of network devices.
- Scriptable interaction with the target - using Nmap Scripting Engine (NSE) and Lua programming language, customized queries can be made.

In addition to these, Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

Typical uses of Nmap:

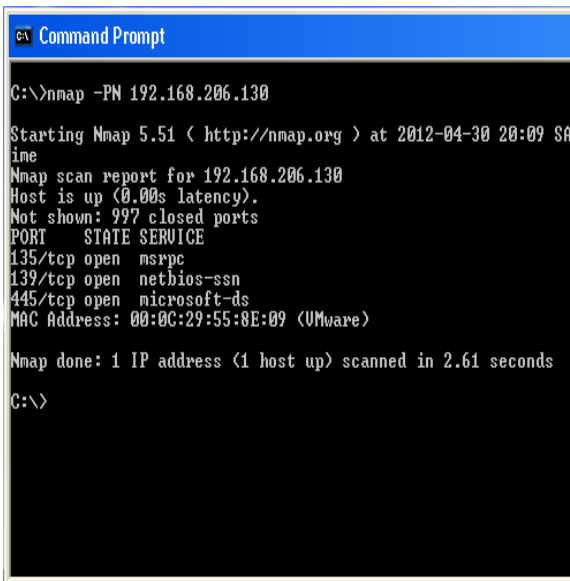
- Auditing the security of a device by identifying the network connections which can be made to it.
- Identifying open ports on a target host in preparation for auditing.
- Network inventory, Network mapping, maintenance, and asset management.
- Auditing the security of a network by identifying unexpected new servers.

Nmap is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port

scanners, Nmap is capable of discovering passive services on a network, despite the fact that such services aren't advertising themselves with a service discovery protocol. In addition, Nmap may be able to determine various details about the remote computers.

Like most tools used in computer security, Nmap can be used for black hat hacking, or attempting to gain unauthorized access to computer systems. It would typically be used to discover open ports which are likely to be running vulnerable services, in preparation for attacking those services with another program.[3] System administrators often use Nmap to search for unauthorized servers on their network, or for computers which don't meet the organization's minimum level of security.[4] Nmap is often confused with host vulnerability assessment tools such as Nessus, which go further in their exploration of a target by testing for common vulnerabilities in the open ports found. In some jurisdictions unauthorized port scanning may be illegal.

To use Nmap you must open the command prompt windows with administrator privilege see Figure 1.



```
Command Prompt
C:\>nmap -PN 192.168.206.130
Starting Nmap 5.51 ( http://nmap.org ) at 2012-04-30 20:09 SA
ime
Nmap scan report for 192.168.206.130
Host is up (0.00s 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:29:55:8E:09 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.61 seconds
C:\>
```

Figure 1  
Running Nmap in command prompt

## NESSUS

Nessus is the world's most widely-deployed vulnerability and configuration assessment product with more than five million downloads to date. Nessus 5[5] features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis of your security posture with features that enhance usability, effectiveness, efficiency, and communication with all parts of your organization.

The Nessus tool works a little differently than other scanners. Rather than purporting to offer a single, all-encompassing vulnerability database that gets updated regularly, Nessus supports the Nessus Attack Scripting Language (NASL), which allows security professionals to use a simple language to describe individual attacks. Nessus administrators then simply include the NASL descriptions of all desired vulnerabilities to develop their own customized scans.

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

Nessus has a modular architecture consisting of centralized servers that conduct scanning, and remote clients that allow for administrator interaction. Administrators can include NASL descriptions of all suspected vulnerabilities to develop customized scans.[6]

Significant capabilities of Nessus include:

- Compatibility with computers and servers of all sizes.
- Detection of security holes in local or remote hosts.
- Detection of missing security updates and patches.
- Simulated attacks to pinpoint vulnerabilities.
- Execution of security tests in a contained environment and Scheduled security audits.

The Nessus 5 has five levels of information, Informational (Blue), Low Risk (Green), Medium Risk (Orange), High Risk (Red), and Critical Risk (Violet) in his report view see Figure 2.

Plugin ID	Count	Severity	Name
18502	1	Critical	MS05-027: Vulnerability in SMB Could Allow Remote Code Execution (896
22194	1	Critical	MS06-040: Vulnerability in Server Service Could Allow Remote Code Exe
34477	1	Critical	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handl
35362	1	Critical	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution
22034	1	High	MS06-035: Vulnerability in Server Service Could Allow Remote Code Exe
26920	1	Medium	Microsoft Windows SMB NULL Session Authentication
57608	1	Medium	SMB Signing Disabled
11219	3	Info	Nessus SYN scanner
11011	2	Info	Microsoft Windows SMB Service Detection
10114	1	Info	ICMP Timestamp Request Remote Date Disclosure
10150	1	Info	Windows NetBIOS / SMB Remote Host Information Disclosure
10287	1	Info	Traceroute Information
10394	1	Info	Microsoft Windows SMB Log In Possible
10397	1	Info	Microsoft Windows SMB LanMan Pipe Server Listing Disclosure

**Figure 2**  
Nessus – This is a report view

## METASPLOIT

I consider the MSF to be one of the single most useful auditing tools freely available to security professionals today. From a wide array of commercial grade exploits and an extensive exploit development environment, all the way to network information gathering tools and web vulnerability plugins. The Metasploit Framework provides a truly impressive work environment. The MSF is far more than just a collection of exploits, it's an infrastructure that you can build upon and utilize for your custom needs. This allows you to concentrate on your unique environment, and not have to reinvent the wheel.

The Metasploit Project [7] is an open source project that provides a public resource for researching security vulnerabilities and developing code that allows a network administrator to break into his own network to identify security risks and document which vulnerabilities need to be addressed first.

The Metasploit Project offers penetration (pen) testing software and provides tools for automating the comparison of a program's vulnerability and its

repaired (patched) version. Anti-forensic and advanced evasion tools are also offered, some of them built into the Metasploit Framework.

Metasploit Framework, the Metasploit Project's best-known creation, is a software platform for developing, testing, and executing exploits. It can be used to create security testing tools and exploit modules and also as a penetration testing system. It was originally created as a portable network tool in 2003 by HD Moore.

The Metasploit Project also offers Metasploit Express, Metasploit Pro, the Opcode Database (currently out of date) and a shellcode database. Shellcode is a type of exploit code in which bytecode is inserted to accomplish a particular objective. Common shellcode objectives include adding a rootkit or performing a reverse telnet back to the attacker's machine. Metasploit also offers a payload database, allowing the pen tester to mix and match exploit code and objectives.

In 2009, the Metasploit Project was acquired by computer security company Rapid7. Metasploit Express and Metasploit Pro are "open core" versions of the Metasploit Framework, with more features added. (Open core is an approach to delivering products that combine open source and proprietary software.) Rapid7 continues to develop Metasploit in collaboration with the open source community.

Metasploit Framework follows some key steps for exploiting a system that include,

- The Select and configure the exploit to be targeted. This is the code that will be targeted toward a system with the intention of taking advantage of a defect in the software.
- Validate whether the chosen system is susceptible to the chosen exploit.
- Select and configures a payload that will be used. This payload represents the code that will be run on a system after a loop-hole has been found in the system and an entry point is set.
- Select and configure the encoding schema to be used to make sure that the payload can evade Intrusion Detection Systems with ease.
- Execute the exploit.

Metasploit is simple to use and is designed with ease-of-use in mind to aid Penetration Testers. Metasploit is commonly used in BackTrack OS. BackTrack is a Linux-based penetration testing arsenal that aids security professionals in the ability to perform assessments in a purely native environment dedicated to hacking. Regardless if you're making BackTrack you Install BackTrack, boot it from a Live DVD or thumbdrive, the penetration distribution has been customized down to every package, kernel configuration, script and patch solely for the purpose of the penetration tester. [8]

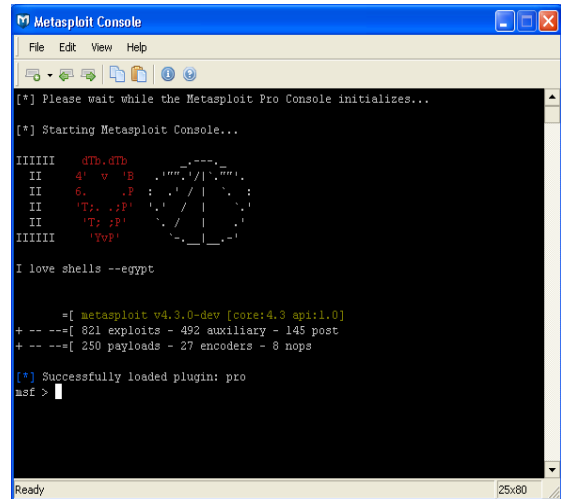
Metasploit framework has three work environments, the msfconsole see Figure 3, the msfcli interface and the msfweb interface. However, the primary and the most preferred work area is the 'msfconsole' [9]. It is an efficient command-line interface that has its own command set and environment system.

In the tutorials I will give a detailed description on usage of Metasploit Framework to execute exploits with graphical illustrations and commands. Potential Uses of the Metasploit Framework:

- Metasploit can be used during penetration testing to validate the reports by other automatic vulnerability assessment tools to prove that the vulnerability is not a false positive and can be exploited. Care has to take because not only does it disprove false positives, but it can also breaks things.
- Metasploit can be used to test the new exploits that come up nearly every day on your locally hosted test servers to understand the effectiveness of the exploit.
- Metasploit is also a great testing tool for your intrusion detection systems to test whether the IDS is successful in preventing the attacks that we use to bypass it.

Metasploit has a new GUI interface called Armitage and is a comprehensive red team collaboration tool for Metasploit that visualizes targets, recommends exploits, and exposes the

advanced post-exploitation features in the framework. [10]



**Figure 3**  
**Metasploit Console**

## CONCLUSION

There are hundreds of Penetration testing and security Tools available on the Internet. Most of these tools are specialized tools in a particular area of computer security. By selecting the correct tool, any new user or experimented investigator will be able to do a security assessment or penetration. Since the security field is so wide, there is not a simple tool that would do all types of analysis or vulnerability test

There are many security problems for which penetration tests will not be able to identify. Penetration tests are generally carried out as "black box" exercises, where the penetration tester does not have complete information about the system being tested.

A test may not identify a vulnerability that is obvious to anyone with access to internal information about the machine. A penetration test can only identify those problems that it is designed to look for. If a service is not tested then there will be no information about its security or insecurity. A penetration test is unlikely to provide information about new vulnerabilities, especially those discovered after the test is carried out.

It is important to make a distinction between penetration testing and network security assessments. A network security or vulnerability assessment may be useful to a degree, but do not always reflect the extent to which hackers will go to exploit a vulnerability. Penetration tests attempt to emulate a 'real world' attack to a certain degree. The penetration testers will generally compromise a system with vulnerabilities that they successfully exploited. If the penetration tester finds 5 holes in a system to get in this does not mean that hackers or external intruder will not be able to find 6 holes. Hackers and intruders need to find only one hole to exploit whereas penetration testers need to possibly find all if not as many as possible holes that exist. This is a daunting task as penetration tests are normally done in a certain time frame.

Finally, a penetration test alone provides no improvement in the security of a computer or network. Action to taken to address these vulnerabilities that is found as a result of conducting the penetration test.

## REFERENCES

- [1] "Pen-test Definition", Retrieve on May 1,2012, [www.metasploit.com/about/penetration-testing-basics/](http://www.metasploit.com/about/penetration-testing-basics/)
- [2] "Nmap Introduction", Retrieve on May 1, 2012, <http://nmap.org/p51-11.html>
- [3] "SANS Institute - Intrusion Detection FAQ: What is AMap and how does it fingerprint applications?", Retrieve on March 17, 2012, <http://www.sans.org/security-resources/idfaq/amap.php>
- [4] "Search | Gizmo's Tech Support Alert", Retrieve on April 10, 2012, <http://www.techsupportalert.com/search/t04123.pdf>
- [5] "Nessus Web Page", Retrieve on March 17, 2012, <http://www.nessus.org/products/nessus>
- [6] "Nessus Documents.", Retrieve on April 4, 2012 <http://www.nessus.org/products/nessus/documentation>
- [7] "Metasploit framework Web Page.", Retrieve on April 7, 2012 <http://www.metasploit.com/>
- [8] "Backtrack Web Page", Retrieve on May 9, 2012 <http://www.backtrack-linux.org/>
- [9] "Metasploit Tutorial", Retrieve on May 1, 2012, <http://www.ethicalhacker.net/content/view/29/24/>
- [10] "Armitage Web Page", Retrieve on May 9, 2012, <http://www.fastandeasyhacking.com/>