NETWORK EXPLOITATION USING METASPLOIT FRAMEWORK

MRS.B.SINDHIYA M.PHIL
ASSISTANT PROFESSOR
DEPARTMENT OF COMPUTER SCIENCE
SRI KRISHNA ARTS AND SCIENCE COLLEGE
COIMBATORE, INDIA.
mail4sini.1@gmail.com

E.VIJAY
MSC SHOLAR
DEPARTMENT OF COMPUTER SCIENCE
SRI KRISHNA ARTS AND SCIENCE COLLEGE
COIMBATORE, INDIA.
evijaysurya@gmail.com

ABSTRACT

In computer networks, network attack is referred as "any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

The proposed Network Exploitation using Metasploit framework aims at finding the weakness of any network (LAN) and working towards the main objective of compromising the target network for exploitation. This helps in identifying how network are configured weakly which are prone to network attacks by third parties or anonymous people and what measures can be done in order to overcome these types of attacks,

The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool. The framework includes hundreds of working remote exploits for a variety of platforms. Payloads, encoders, and nop slide generators can be mixed and matched with exploit modules to solve almost any exploit-related task. Exploit is a piece of code that exploits a software bug leading to a security hole There is a never ending race between the attackers, who try to find loopholes, and the vendors, who develop patches for them. The countermeasures for each and every attack have to be precise in order to keep information security intact.

1. INTRODUCTION

An exploit is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). Such behavior frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial-of-service attack.

Computer Network Exploitation (CNE): Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks.

Metasploit Framework is an open source attack framework first developed by H. D. Moore in 2003. Metasploit is used for hacking into systems for testing purposes. Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research. With the latest Metasploit 3.0 release, the project has moved to an all Ruby programming base.Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shell code archive and related research. The Metasploit Project is well known for its anti-forensic and evasion tools, some of which are built into the Metasploit Framework.

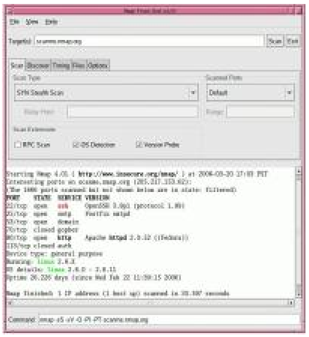
Choosing and configuring an exploit (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and Mac OS X systems are included); Optionally checking whether the intended target system is susceptible to the chosen exploit; Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server); Choosing the encoding technique so that the intrusion-prevention system (IPS) ignores the encoded payload;

Executing the exploit,

1. This modular approach – allowing the combination of any exploit with any payload – is the major advantage of the Framework. It facilitates the tasks of attackers, exploit writers and payload writers.

2. Metasploit runs on UNIX (including Linux and Mac OS X) and on Windows. It includes two command-line interfaces, a web-based interface and a native GUI. The web interface is intended to be run from the attacker's computer. The Metasploit Framework can be extended to use add-ons in multiple languages. To choose an exploit and payload, some information about the target system is needed, such as operating system version and installed network services. This information can be gleaned with port scanning and OS fingerprinting tools such as Nmap. Vulnerability scanners such as Expose or Nesses can detect target system vulnerabilities. Metasploit can import vulnerability scan data and compare the identified vulnerabilities to existing exploit modules for accurate exploitation.

3. Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available forLinux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).



Target(s): scanme.nmap.org

Scan Type: SYN Stealth Scan

Scanned Ports: Default

Scan Extensions: □ RPC Scan ☑ OS Detection ☑ Version Probe

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 17:05 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1668 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  open   smtp    Postfix smtpd
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.226 days (since Wed Feb 22 11:59:15 2006)

Nmap finished: 1 IP address (1 host up) scanned in 20.187 seconds
```

Command: nmap -sS -sV -O -P0 -PT scanme.nmap.org

2. SYSTEM STUDY

Nowadays, wired networks, especially the In

2.1 EXISTING SYSTEM

In broad sense, hacking toolkits include not only the s

2.1.1DRAWBACKS

To start, a program cannot be installed unless you ha

- A sniffer can only sniff around where the victim'
- Data which sniffer tries to capture is often filter
- Usually the presence of a sniffer on the networl

2.2. PROPOSED SYSTEM

The proposed system recommends the usag

2.2.1 FEATURES

Metasploit framework has many extensive featu

Msfconsole - Metasploit interactive session

Msfcli- execute exploit without interactive sessic

Msfd- a daemon to share a single session

Msfgui- the Metasploit GUI application

Msfweb- the Metasploit web interface

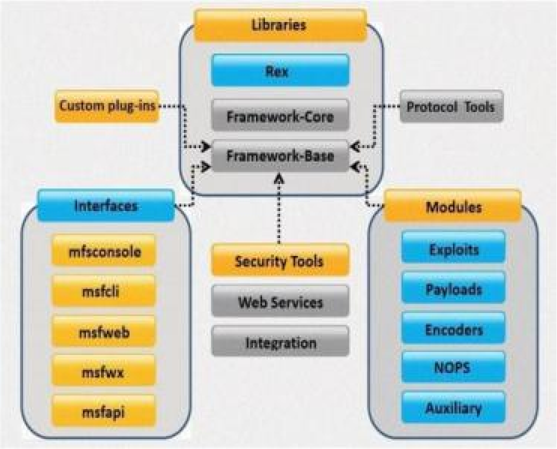
Msfpayload - list supported payloads

Msfencode- use Metasploit encoder

msfopcode- an interface to the opcode database

msfelfscan- search an ELF for a specific opcode

msfpescan- search a PE for a specific opcode



NMAP facilitates the following features

Flexible: Supports dozens of advanced techniques for mapping out networksfilled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more.

Powerful: Nmap has been used to scan huge networks of literally hundreds ofthousands of machines.

Portable: Most operating systems are supported, including Linux, MicrosoftWindows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, SunOS, Amiga, and more.

Easy: While Nmap offers a rich set of advanced features for power users,you can start out as simply as "nmap -v -A targethost". Both traditional command line and graphical (GUI) versions are available to suit our preference. Binaries are available for those who do not wish to compile Nmap from source.

Free: The primary goals of the Nmap Project is to help make the Internet a

Littlemore secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.

3.2 INPUT DESIGN

Installing the Framework is as easy as extracting the tar ball, changing into the created directory, and executing your preferred user interface. We strongly recommend that you use a version of the Ruby interpreter that was built with support for the GNU read line library. If you are using the Framework on Mac OS X, you will need to install GNU read line and then recompile the Ruby interpreter. Using a version of Ruby with read line support enables tab completion of the console interface. The msfconsole user interface is preferred for everyday use, but the msfweb interface can be useful for live demonstrations. To perform a system-wide installation, we recommend that you copy the entire Framework directory into a globally accessible location (/usr/local/msf) and then create symbolic links from the msf* applications to a directory in the system path (/usr/local/bin). User-specific modules can be placed into HOME/.msf3/modules directory. The structure of this directory should mirror that of the global modules directory found in the framework distributionThe Metasploit Framework is only partially supported on the Windows platform. If you would like to access most of the Framework features from Windows, we recommend using a virtualization environment, such as VMWare, with a supported Linux distribution. If this is not possible, you can also use the Framework from within Cygwin. To use the Framework from within Cygwin, follow the instructions for installation on a UNIX system. For more information on Cygwin, please see the Cygwin web site at http://www.cygwin.com/To install the Framework on Windows, download the latest version of the Windows installer from http://framework.metasploit.com/, perform an online update, and launch the msfweb interface. Once msfweb is running, access the http://127.0.0.1:55555/URL from within your browser. At this time, only Mozilla and Internet Explorer are fully supported.

3.3 OUTPUT DESIGN

From the msfconsole interface, you can view the list of modules that are available for you to interact with. You can see all available modules through the show all command. To see the list of modules of a particular type you can use the show module type command, where module type is any one of exploits, encoders, payloads, and so on. You can select a module with the use command by specifying the module‟s name as the argument. The info command can be used to view information about a module without using it. Unlike Metasploit 2.x, the new version of Metasploit supports interacting with each different module types through the use command. In Metasploit 2.x, only exploit modules could be interacted with.

3.4. DATABASE DESIGN

Opcode Database

The Opcode Database is an important resource for writers of new exploits. Buffer overflow exploits on Windows often require precise knowledge of the position of certain machine language opcodes in the attacked program or included DLLs. These positions differ in the various versions and patch-levels of a given operating system, and they are all documented and conveniently searchable in the Opcode Database. This allows coders to write buffer overflow exploits that work across different versions of the target

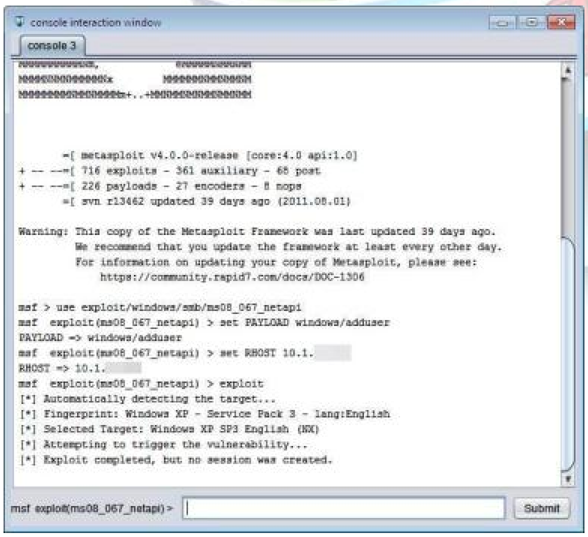
Shellcode Database

The Shellcode database contains the payloads (also known as shellcode) used by the Metasploit Framework. These are written in assembly language. Full source code is available.

3.5 SYSTEM DEVELOPMENT

Metasploit offers many types of payloads, including:

Command shell enables users to run collection scripts or run arbitrary commands against the host. Meterpreter enables users to control the screen of a device using VNC and to browse, upload and download files.



```
MMMMMMMMMMMMM,          MMMMMMMMMMMMM
MMMMMMMMMMMMMMx        MMMMMMMMMMMMMM
MMMMMMMMMMMMMMMMm+..+MMMMMMMMMMMMMMMMM



       =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
       =[ svn r13462 updated 39 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 39 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > set PAYLOAD windows/adduser
PAYLOAD => windows/adduser
msf  exploit(ms08_067_netapi) > set RHOST 10.1.[redacted]
RHOST => 10.1.[redacted]
msf  exploit(ms08_067_netapi) > exploit
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
```

```
msf exploit(ms08_067_netapi) >
```

3.5.1. DESCRIPTION OF MODELS

METASPLOIT INTERFACES

There are several interfaces for Metasploit available. The most popular are maintained by Rapid7 and Strategic Cyber LLC.[8]

Metasploit Framework Edition

The free version. It contains a command line interface, third-party import, manual exploitation and manual brute forcing.[8]

Metasploit Community Edition

In October 2011, Rapid7 released Metasploit Community Edition, a free, web-based user interface for Metasploit. Metasploit Community is based on the commercial functionality of the paid-for editions with a reduced set of features, including network discovery, module browsing and manual exploitation.Metasploit Community is included in the main installer.

Metasploit Express

In April 2010, Rapid7 released Metasploit Express, an open-core commercial edition for security teams who need to verify vulnerabilities. It offers a graphical user interface, integrates nmap for discovery, and adds smart brute forcing as well as automated evidence collection.

Metasploit Pro

In October 2010, Rapid7 added Metasploit Pro, an open-core commercial Metasploit edition for penetration testers. Metasploit Pro includes all features of Metasploit Express and adds web application scanning and exploitation, social engineering campaigns and VPN pivoting.

Armitage

Armitage is a graphical cyber attack management tool for the Metasploit Project that visualizes targets and recommends exploits. It is a free and open source network security tool notable for its contributions to red team collaboration allowing for, shared sessions, data, and communication through a single Metasploit instance.[9]

Cobalt Strike

Cobalt Strike is a collection of threat emulation tools provided by Strategic Cyber LLC to work with the Metasploit Framework. Cobalt Strike includes all features of Armitage and add post-exploitation tools, in addition to report generation features.

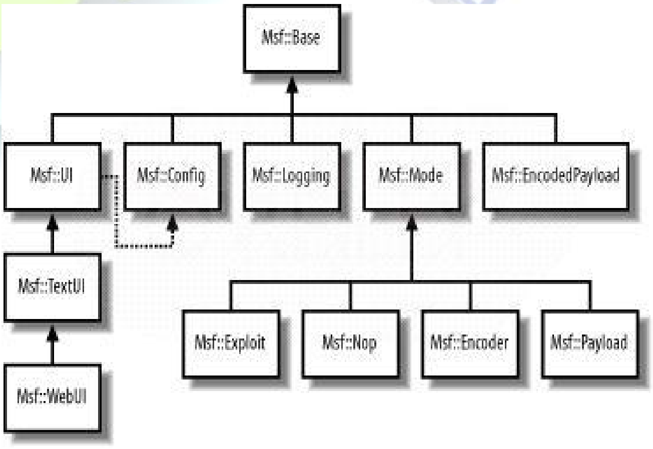
5. CONCULSION

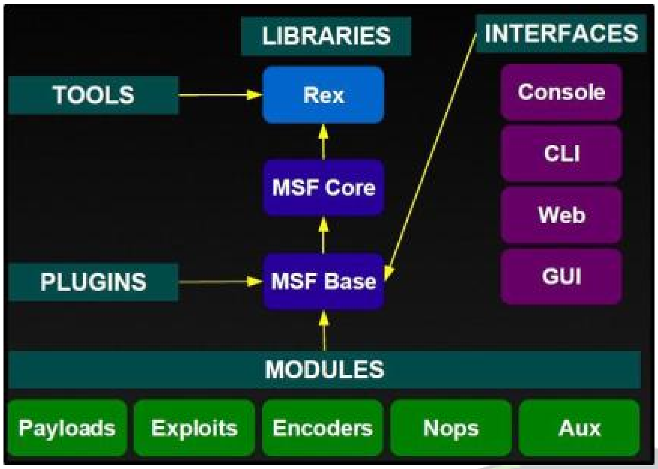
The proposed system which is uses the remote desktop vulnerability for operating system works accurately. It is tested for its effectives, flexibility, accuracy and user friendliness.Like many security tools, the Metasploit framework has great potential with all of the features that have been presented. But again like many security tools there is the possibility of misuse. It is up to the individual end user to decide how it will be used. Security practitioners need to know how those same bad guys might attack and what is possible. Layered security is not just „ACLs, firewalls, network segregation, IDS, etc. The most important layer in the security process is the human layer. What that human layer can bring to the table is every bit as important as the rule base on the firewall and being armed with the Metasploit Framework will only add to that human value.

6.BIBLIOGRAPHY

- etasploit: The Penetration Tester's Guide- David Kennedy
- Metasploit Toolkit for Penetration Testing, Exploit Development, and
- ulnerability Research- David Maynor
- enetration testing mit Metasploit- Frank Neugebauer.The Fundamentals of Network Security- John E. Canavan
- aximum Security (3rd Edition)- Greg Shipley

7. DFD




LIBRARIES
INTERFACES
TOOLS
Rex
Console
CLI
MSF Core
Web
PLUGINS
MSF Base
GUI
MODULES
Payloads
Exploits
Encoders
Nops
Aux