Intro to Penetration Testing: Exploitation

October 18, 2017

Brown Bag Talks

Friday at 11:00 AM

State Farm

October 25th, 2017

What is Exploitation?

Getting what you shouldn’t get

Changing what you should change

Goal

In general, the goal is to compromise the objective. This could be accessing a building, becoming the website admin, etc.

For systems, remote shells allow you execute arbitrary commands, and are overall a convenient way to access a remote systems

Getting what you shouldn’t get

- Fuzzing applications
- Gaining access to the file system
- Getting system and service configuration
- Accessing protected pages

Linux File System Access

- /etc - General configuration directory
- /var/log - Log directory
- /etc/passwd - List of all users
- /etc/group - List of all groups
- /etc/shadow - List of all users and passwords (should require root)
- /etc/os-release - Information about the running OS

Getting what you shouldn’t get

Enumeration on steroids

Gaining enough information to change what you shouldn’t change

Changing what you shouldn’t change

- Breaking applications
- Command execution
- Changing permissions
- Modifying system configuration

Inline shell

'grep -m 1 ' + service + ' /etc/services'

'grep -m 1; whoami # /etc/services'

'grep -m 1 `ls > /tmp/test && echo 80`/etc/services'

Linux Shell Escapes

- # to comment out the rest of a line
- ; to enter another command
- > to redirect output
- < to redirect input
- | to chain commands
- `` to execute commands

Changing what you shouldn’t change

Action on objectives

Making it as easy as possible for you to continue getting what you shouldn’t get

Exploitation Cycle

- Getting enough information to change something
- Changing enough to get more information
- Repeat
- ???
- Profit (get shell; have fun)

Payloads (or, why a shell?)

- Pivoting from an application exploit to a malicious payload give an attacker better persistence, more flexibility, and an overall more usable experience.
- Multiple shells can easily be controlled at once
- Shells can be incorporated into scripts and botnets, allowing automated control

Fun shells, if they aren’t on your machine

- Web shell
- Bind shell
- Reverse shell

Fun shells, if they aren’t on your machine

- Web shell - only require access to an application, no session
- Bind shell - require access through firewall, session
- Reverse shell - require local session handler, session

Shell payload generation

- Premade payloads (c99 shell, etc.)
- Payloads made with a builder (msfvenom, etc.)
- Handmade payloads

C99Shell v. 1.0 pre-release build #17

Software: Apache. PHP/5.2.17-0.ic-vip.0
uname -a: Linux [redacted] #1 SMP Wed Aug 3 07:36:31 CEST 2011 x86_64

Safe-mode: ON (secure)
/home/[redacted]/root/ drwxr-xr-x
Free 199.68 GB of 920.01 GB (21.7%)

[Home] [Back] [Forward] [UPDIR] [Refresh] [Search] [Buffer] [Encoder] [Tools] [Proc.] [FTP brute] [Sec.] [SQL] [PHP-code] [Self remove] [Logout]

Binding port:
Port: 31373 Password: c99 Using PERL Bind

Back connection:
HOST: 10.10.30.20 Port: 31373 Using PERL Connect

Click "Connect" only after open port for it. You should use NetCat©, run "**nc -l -n -v -p 31373**"!

Datapipe:
HOST: irc.dalnet.ru:6667 Local port: 8081 Using PERL Run

Note: sources will be downloaded from remote server.

:: Command execute ::

Enter:
Execute

Select:

Execute