Network Pentesting

Vivek Ramachandran

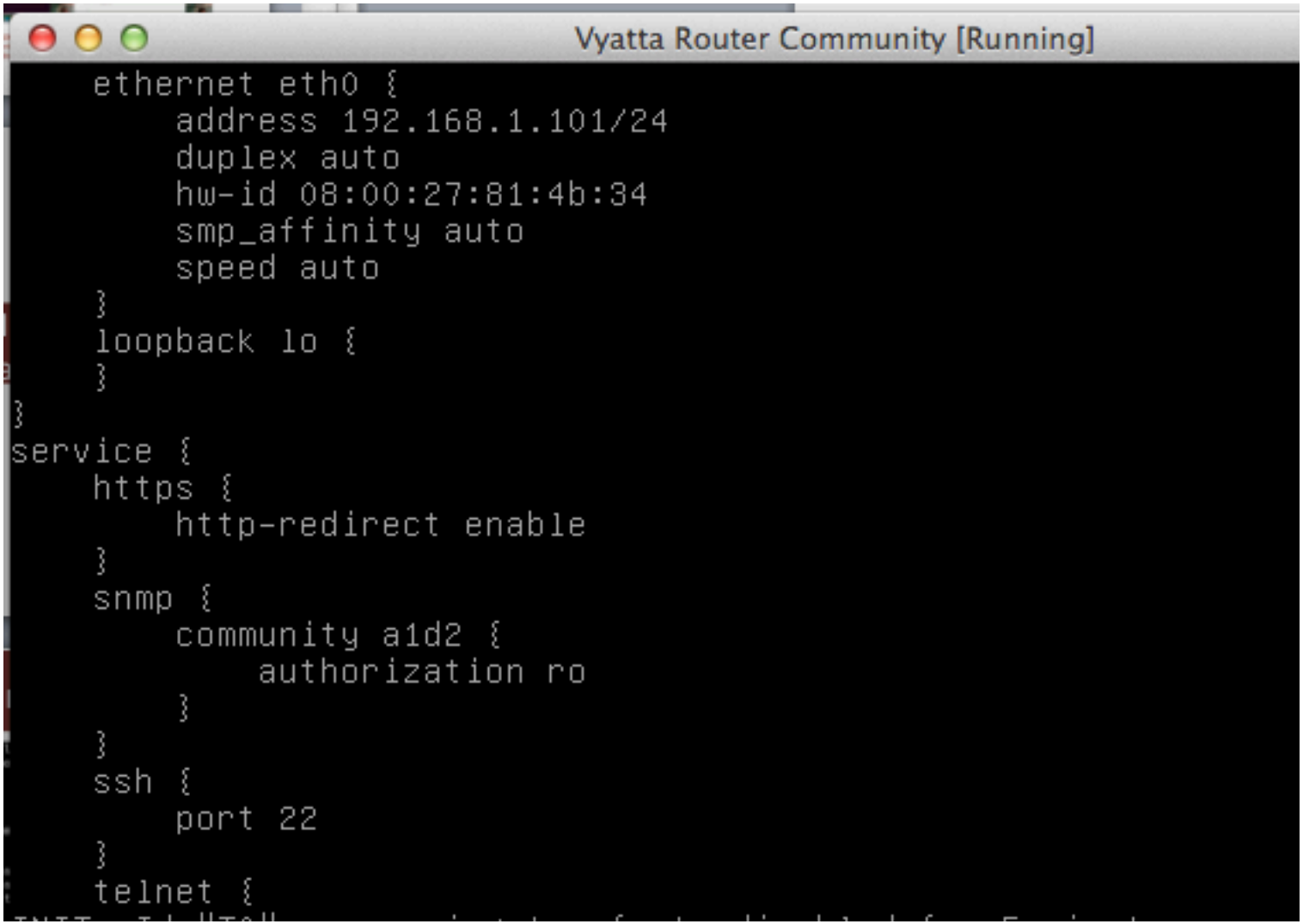
SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

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

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

Pentesting Routers: SNMP audit with Metasploit, Snmpcheck and Onesixtyone

Vyatta SNMP Configuration



Onesixtyone

```
PentesterAcademy# crunch 4 4 ad12 > snmp_list
Crunch will now generate the following amount of data: 1280 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 256
PentesterAcademy#
PentesterAcademy# onesixtyone
onesixtyone 0.3.2 [options] <host> <community>
  -c <communityfile> file with community names to try
  -i <inputfile>     file with target hosts
  -o <outputfile>    output log
  -d                 debug mode, use twice for more information

  -w n               wait n milliseconds (1/1000 of a second) between s
  -q                 quiet mode, do not print log to stdout, use with -
examples: ./s -c dict.txt 192.168.4.1 public
          ./s -c dict.txt -i hosts -o my.log -w 100

PentesterAcademy# onesixtyone -c snmp_list 192.168.1.101
Scanning 1 hosts, 256 communities
192.168.1.101 [a1d2] Vyatta VC6.6R1
PentesterAcademy#
```

Snmpcheck

```
PentesterAcademy# snmpcheck -c a1d2 -t 192.168.1.101
```

```
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

 [*] Try to connect to 192.168.1.101
 [*] Connected to 192.168.1.101
 [*] Starting enumeration at 2013-10-19 21:15:33

 [*] System information
 -------------------------------------------------------------------------------

 Hostname              : vyatta
 Description           : Vyatta VC6.6R1
 Uptime system         : 10 hours, 21:56.39
 Uptime SNMP daemon    : 10 hours, 21:37.70
 Contact               : root
 Location              : Unknown
 Motd                  : -

 [*] Devices information
 -------------------------------------------------------------------------------

    Id                Type   Status  Description

 196608           Processor  Running  GenuineIntel: Intel(R) Core(TM) i5-2520M CPU @ 2.50GHz
 262145             Network  Running  network interface lo
 262146             Network  Running  network interface eth0
 786432         Coprocessor  Unknown  Guessing that there's a floating point co-processor

 [*] Storage information
 -------------------------------------------------------------------------------

 Physical memory
       Device id       : 1
```

Metasploit – snmp_enum

```
msf > use auxiliary/scanner/snmp/snmp_enum
msf auxiliary(snmp_enum) > show options

Module options (auxiliary/scanner/snmp/snmp_enum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
   RETRIES    1                yes       SNMP Retries
   RHOSTS                      yes       The target address ra
   RPORT      161              yes       The target port
   THREADS    1                yes       The number of concurr
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>

msf auxiliary(snmp_enum) > set COMMUNITY a1d2
COMMUNITY => a1d2
msf auxiliary(snmp_enum) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf auxiliary(snmp_enum) > run

[+] 192.168.1.101, Connected.

[*] System information:

Host IP                     : 192.168.1.101
Hostname                    : vyatta
Description                 : Vyatta VC6.6R1
Contact                     : root
Location                    : Unknown
Uptime snmp                 : 10:27:20.14
Uptime system               : 10:27:01.45
System date                 : 2013-10-20 01:20:56.0
```

Vyatta – set RW community string

```
vyatta@vyatta:~$ configure
[edit]
vyatta@vyatta# set service snmp community a1d3 authorization rw
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyatta@vyatta# _
```

Metasploit – snmp_set

```
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
   OID                         yes       The object identifier (numeric notation)
   OIDVALUE                    yes       The value to set
   RETRIES    1                yes       SNMP Retries
   RHOSTS                      yes       The target address range or CIDR identifier
   RPORT      161              yes       The target port
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    1                yes       SNMP Timeout
   VERSION    1                yes       SNMP Version <1/2c>

msf auxiliary(snmp_set) > set COMMUNITY a1d3
COMMUNITY => a1d3
msf auxiliary(snmp_set) > set OID iso.3.6.1.2.1.1.5.0
OID => iso.3.6.1.2.1.1.5.0
msf auxiliary(snmp_set) > set OIDVALUE Demo
OIDVALUE => Demo
msf auxiliary(snmp_set) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf auxiliary(snmp_set) > run

[*] Try to connect to 192.168.1.101...
[-] 192.168.1.101 Error: ArgumentError ["iso", "3", "6", "1", "2", "1", "1", "5", "0"]:Array not a
valid object ID ["/opt/metasploit/apps/pro/msf3/lib/snmp/varbind.rb:161:in `rescue in initialize'",
 "/opt/metasploit/apps/pro/msf3/lib/snmp/varbind.rb:153:in `initialize'", "/opt/metasploit/apps/pro
/msf3/lib/snmp/mib.rb:243:in `new'", "/opt/metasploit/apps/pro/msf3/lib/snmp/mib.rb:243:in `parse_o
id'", "/opt/metasploit/apps/pro/msf3/lib/snmp/mib.rb:218:in `oid'", "/opt/metasploit/apps/pro/msf3/
lib/snmp/mib.rb:167:in `varbind_list'", "/opt/metasploit/apps/pro/msf3/lib/snmp/manager.rb:238:in `
get'", "/opt/metasploit/apps/pro/msf3/lib/snmp/manager.rb:261:in `get_value'", "/opt/metasploit/app
s/pro/msf3/modules/auxiliary/scanner/snmp/snmp_set.rb:53:in `run_host'", "/opt/metasploit/apps/pro/
msf3/lib/msf/core/auxiliary/scanner.rb:94:in `block in run'", "/opt/metasploit/apps/pro/msf3/lib/ms
f/core/thread_manager.rb:100:in `call'", "/opt/metasploit/apps/pro/msf3/lib/msf/core/thread_manager
```

Metasploit - snmptranslate

```
PentesterAcademy# snmptranslate -On iso.3.6.1.2.1.1.5.0
.1.3.6.1.2.1.1.5.0
PentesterAcademy#
```

```
msf> use auxiliary/scanner/snmp/snmp_set
msf auxiliary(snmp_set) > set COMMUNITY a1d3
COMMUNITY => a1d3
msf auxiliary(snmp_set) > set RHOSTS
RHOSTS => 192.168.1.101
msf auxiliary(snmp_set) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf auxiliary(snmp_set) > set OID 1.3.6.1.2.1.1.5.0
OID => 1.3.6.1.2.1.1.5.0
msf auxiliary(snmp_set) > set OIDVALUE Demo
OIDVALUE => Demo
msf auxiliary(snmp_set) > run

[*] Try to connect to 192.168.1.101...
[*] Check initial value : OID 1.3.6.1.2.1.1.5.0 => vyatta
[*] Set new value : OID 1.3.6.1.2.1.1.5.0 => Demo
[*] Check new value : OID 1.3.6.1.2.1.1.5.0 => Demo
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(snmp_set) >
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

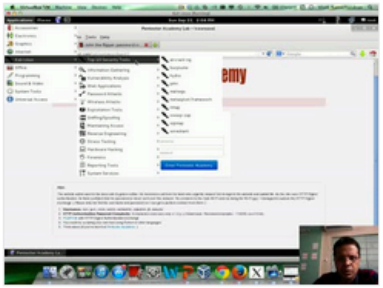
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

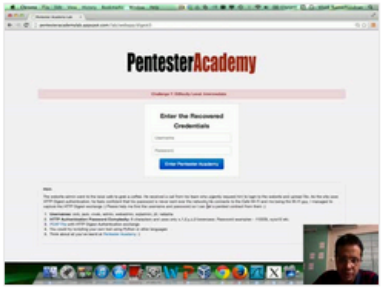
Start Learning Today!

Latest Videos

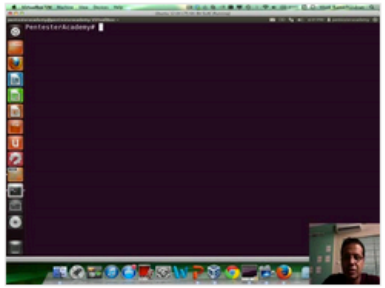
New content added weekly!



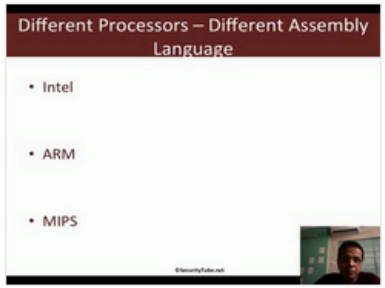
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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