Xavier Tartera

Software Lliure:

És la denominació del software que respecta la llibertat dels usuaris sobre el seu producte adquirit, i per tant, una vegada obtingut pot ser usat, copiat, estudiat, modificat, i redistribuït lliurement.

Segons la free software foundation, el software lliure es refereix a la llibertat dels usuaris per executar, copiar, distribuir, estudiar, o modificar el software i distribuir-lo modificat.

Software Lliure:

El software lliure sol estar disponible gratuitament, o al preu de cost de la distribució a través d'altres mitjans: tot i així no és obligatori que sigui així, per lo tant no s'ha de associar software lliure a software gratuit (l'anomenat generalment freeware).

Avantges del software lliure

- Fomenta de la lliure competència, al basar-se en serveis i no en llicències; aquest sistema permet que les empreses que donin el servei, competeixin en igualtat de condicions al no posseir la propietat del producte del qual donen servei.

Avantges del software lliure

- Suport i compatibilitat a llarg termini; la opció és treure un nou producte, produir software que faci servir noves tecnologies només per aquest nou producte i donar suport per a la resolució de errades.

Avantges del software lliure

- Formats estandart, aquests formats permeten una interoperativitat més alta entre sistemes, evitant imcompatibilitats.

- Sistemes sense portes del darrera i més segurs. L'accés al codi font permet que tant hackers com empreses de seguretat de tot el mon puguin auditar els programes.

Avantges del software lliure

- Correcció més ràpida i eficient de errades. El funcionament i interés conjunt de la comunitat ha demostrat solucionar més ràpidament errades de seguretat en el software lliure, una cosa que desgraciadament en el software propietari és més difícil i costós.

Desaventatges del software lliure

- Inexistència de garantia per part del autor, per això existeixen comunitats que ajuden i aporten tant en codi com en solucions.
- Poca estabilitat i flexibilitat en el camp de multimèdia i jocs.
- Menor compatibilitat amb el hardware.
- Dificultat en el canvi de fitxers: això es dona majoritariament en el documents de text (generalment creats amb Word) per exemple els formats es fan malbé quan s'utilitzen taules, per la resta sol funcionar perfectament.

Historia Backtrack

Backtrack Linux té una llarga història i està basat en moltes i diverses distribucions de Linux, fet que fins ara estigui basat en una distribució de Linux de slackware i les escriptures live-CD.

Cada paquet, configuració del nucli i escriptura s'optimitza per ser utilitzat pels auditors de penetració seguretat informàtica.

Característiques

- Actualment Backtrack Linux, és la més popular entre les distribucions Linux-Live-CD utilitzades en proves de seguretat informàtica, sense instal·lació prèvia.

- Backtrack ha adquirit una gran popularitat fins al punt de ser escollida la distribució Live-CD més segura del 2006 per insecure.org (organització considerada més important dins el món de la seguretat informàtica).

característiques

- Actualment Backtrack, compta amb mñes de 300 eines diferents actualitzades, les quals es troben estructurades i ordenades lògicament seguint el flux de treball que realitzaria un expert en seguretat informàtica.

- Aquesta estructura permet que inclús els acabats de iniciar en seguretat puguin trobar amb facilitat l'eina adequada.

Versions publicades

Data	Llançament
05/febrer/2006	Backtrack 1.0 beta
26/maig/2006	The backtrack 1.0 final
13/octubre/2006	Backtrack 2 primera beta
19/novembre/2006	Backtrack 2 segunda beta
06/març/2007	Backtrack 2 final
17/desembre/2007	Backtrack 3 beta
19/juny/2008	Backtrack 3 final

Data	Llançament
19/juny/2009	Backtrack 4 final
09/Gener/2010	Backtrack 4 final
08/maig/2010	Backtrack 4 R1 final
22/novembre/2010	Backtrack 4 R2 final
10/maig/2011	Backtrack 5 final (kernel2.6.38)
18/agost/2011	Backtrack 5 R1 final (kernel 2.6.39.49)
01/març/2012	Backtrack 5 R2 final (kernel 3.2.6)
13/agost/2012	Backtrack 5 R3 final (kernel 3.2.6)

Backtrack 5

El nom en codi del llançament és “revolution”, ja que es donen un sèrie de canvis molt importants dins de la distribució:

- Backtrack 5 està basat en Ubuntu 10.04 LTS, i per primera vegada ofereix suport per arquitectures de 32 i 64 bits, novetat en la distribució, ja que fins fa poc només s'oferia en arquitectura de 32 bits.

Backtrack 5

- És oficialment suportat en l'entorn de escriptori KDE4, Gnome i Flux box, el qual permet a l'usuari descarregar la edició amb l'entorn d'escriptori de la seva preferència.

- És també la primera versió de Backtrack que inclou el codi font complert dins dels seus repositoris, aclarint així qualsevol problema de llicències que hi hagi hagut en anteriors versions.

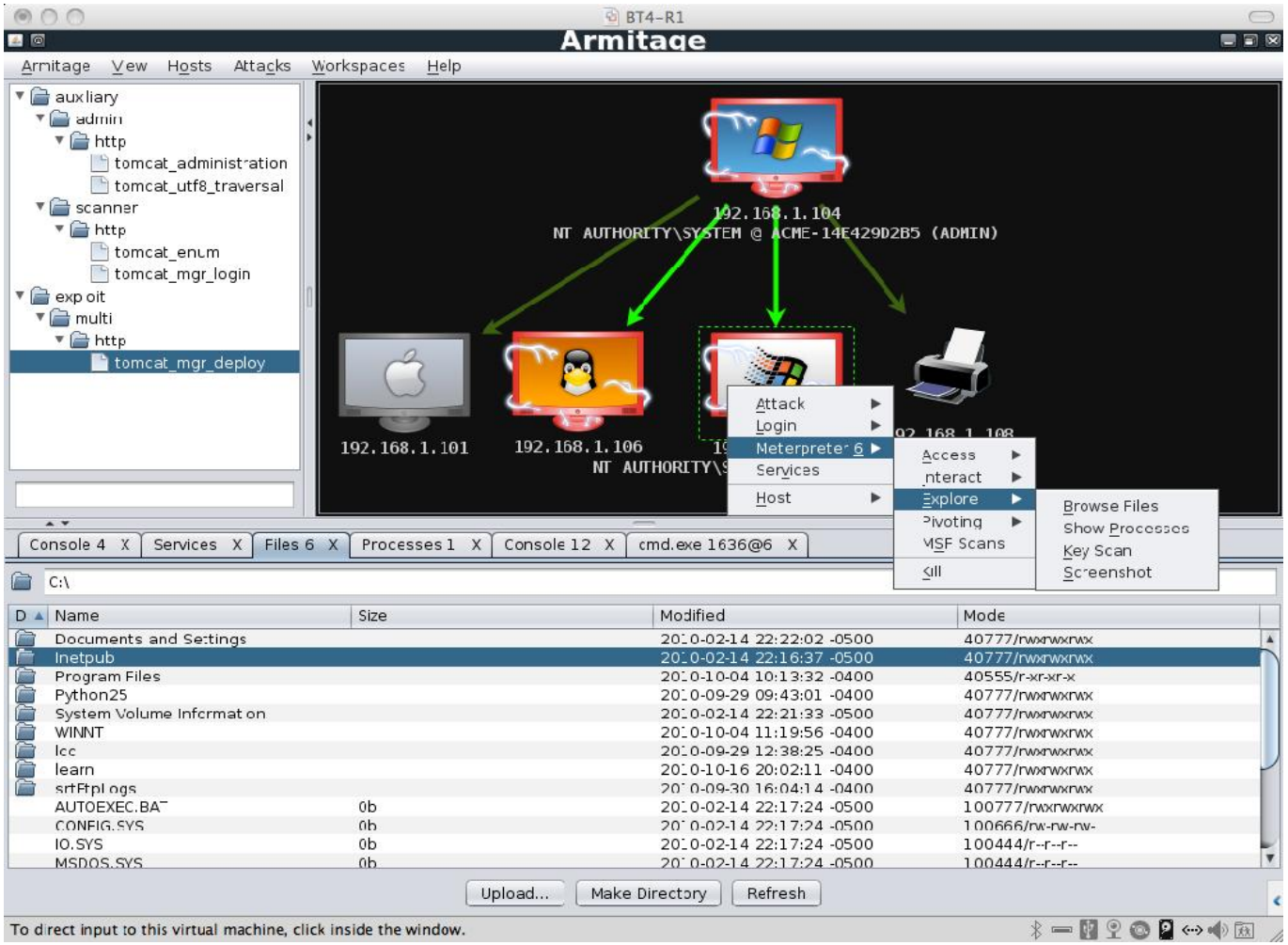
Algunes aplicacions incloses

Què és Armitage?

Armitage, és un administrador gràfic de ciber-atacs per Metasploit, que serveix per visualitzar gràficament els teus objectius, el mateix programa et recomana exploits a usar, exposa les opcions avançades del Framework, ens dona facilitat d'ús i execució dels propis exploits del metaexploit, i al mateix temps podem iniciar un anàlisi amb Nmap, inclús es pot usar el mòdul de força bruta per descobrir els usuaris i passwords.

L'objectiu de Armitage és fer Metasploit útil pels professionals de seguretat que saben hacking, però no l'ús del metasploit a fons.

Armitage


BT4-R1
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
admin
http
tomcat_administration
tomcat_utf8_traversal
scanner
http
tomcat_enum
tomcat_mgr_login
exploit
multi
http
tomcat_mgr_deploy
192.168.1.104
NT AUTHORITY\SYSTEM @ ACME-14E429D2B5 (ADMIN)
192.168.1.101
192.168.1.106
Attack
Login
Meterpreter 6
Services
Host
Access
Interact
Explore
Pivoting
MSF Scans
Kill
Browse Files
Show Processes
Key Scan
Screenshot
Console 4
Services
Files 6
Processes 1
Console 12
cmd.exe 1636@6
C:\
D
Name
Size
Modified
Mode
Documents and Settings
Inetpub
Program Files
Python25
System Volume Information
WINNT
Icc
learn
AUTOEXEC.BAT
CONFIG.SYS
IO.SYS
MSDOS.SYS
Upload...
Make Directory
Refresh
To direct input to this virtual machine, click inside the window.

Administració d'un atac amb Armitage

- Armitage organitza les capacitats de metasploit al voltant de un procés de hacking. Hi ha característiques per descobrir, accedir, post-explotació i interacció.

- Per descobrir, Armitage, disposa de vàries eines per gestionar les capacitats dels metasploits; pot importar i llançar escaneigos per obtenir tota una sèrie de objectius; també es pot visualitzar molt gràficament els hosts o màquines atacades, així com les sessions obertes d'atac.

Administració d'un atac amb Armitage

- Armitage ajuda amb la pxplotació remota, proporcionant ajut al recomanar exploits automàticament, o fins hi tot revisar activament per tal de determinar quins exploits poden funcionar. Si aquestes opcions fallen, es pot usar el mètode “Hail Mary” força més contundent i a vegades satisfactori en la exploració de possibles exploits.

- Una vegada dins de la vistima, Armitage, proporciona moltes eines de post-explotació basades en l'agent meterpreter.

Administració d'un atac amb Armitage

- Amb un click, es podran fer moltes operacions: escalar privilegis, volcar fitxers de hash en una base de dades local de credencials, navegar pel sistema, i llançar consoles de comandes, i molt més....
- Finalment, Armitage ajuda en el procés de creació de pivots, una capacitat que li permet de usar els hosts compromesos (atacats) com una plataforma per atacar d'altres hosts i seguir investigant en la xarxa.
- Armitage inclús disposa de un mòdul (SOCKS) proxy de metasploit, el qual permet que eines externes prenguin característiques i/o controls d'aquests pivots.

Vocabulari associat:

Fer servir Armitage, ajuda a entendre Metasploit. A continuació hi ha algunes cosetes que cal conèixer en referència al vocabulari que s'usa:

Metasploit, és una aplicació per consola. Qualsevol cosa que es faci a través de Armitage, és traduït a una comanda que metasploit entengui. També es pot passar per alt Armitage, i escriure les comandes directament en el terminal de Metasploit que també és inclòs en el Backtrack.

Vocabulari associat:

Metasploit presenta diversos mòduls, i cada escaneig, exploit (algoritme) i payload (injecció de codi de càrrega, variables i paràmetres), està disponible com un mòdul (exploit; algoritme).

Abans de llançar a executar un mòdul exploit, caldrà ajustar una o més variables i llançar-lo;

Vocabulari associat:

Armitage, dona molta facilitat en realitzar aquest procés d'una manera més automatitzada.

Si l'exploit té èxit, tens una sessió en el host, i Armitage sap com interactuar amb shell (consola) i amb sessions de Windows meterpreter.

Meterpreter, és un interpret de comandes, que posa a disposició del hacker de moltes funcionalitats per a la post-explotació.

Armitage està construït per treure profit de meterpreter.

Vocabulari associat:

- Exploit: és un tros de programa, script, o seqüència de comandes que té la finalitat de aprofitar una vulnerabilitat d'un altre sistema, o programa per prendre el control. Alteren el funcionament d'un programa per obtenir el seu objectiu (obtenir el control).

- Bug: És un error de programa, que com a conseqüència permet la manipulació total o permanent de certes dades.

Alguns exemples d'atac

- Backtrack 5 R2 i Windows XP SP2
  - En el següent video es mostra la importància de tenir els sistemes operatius actualitzats, ja que en el cas del Windows XP SP2, es presentava un bug important que permetia un atac i intrusió en el sistema operatiu transparent al usuari atacat:

    https://www.youtube.com/watch?v=hUxLErIc6Fc

Alguns exemples d'atac

- Backtrack 5 R3 i Windows 7

  - En el següent videoo es mostra com es pot fer un atac a un Windows 7, a través de injectar un “troià” que ens obri una porta d'entrada al sistema operatiu, ens aprofitem de la curiositat del usuari per entrar nosaltres (pharming).

https://www.youtube.com/watch?v=bKB_PC1MmIA