Ministerul Educației și Cercetării al Republicii Moldova
IP Colegiul “Iulia Hasdeu” din Cahul

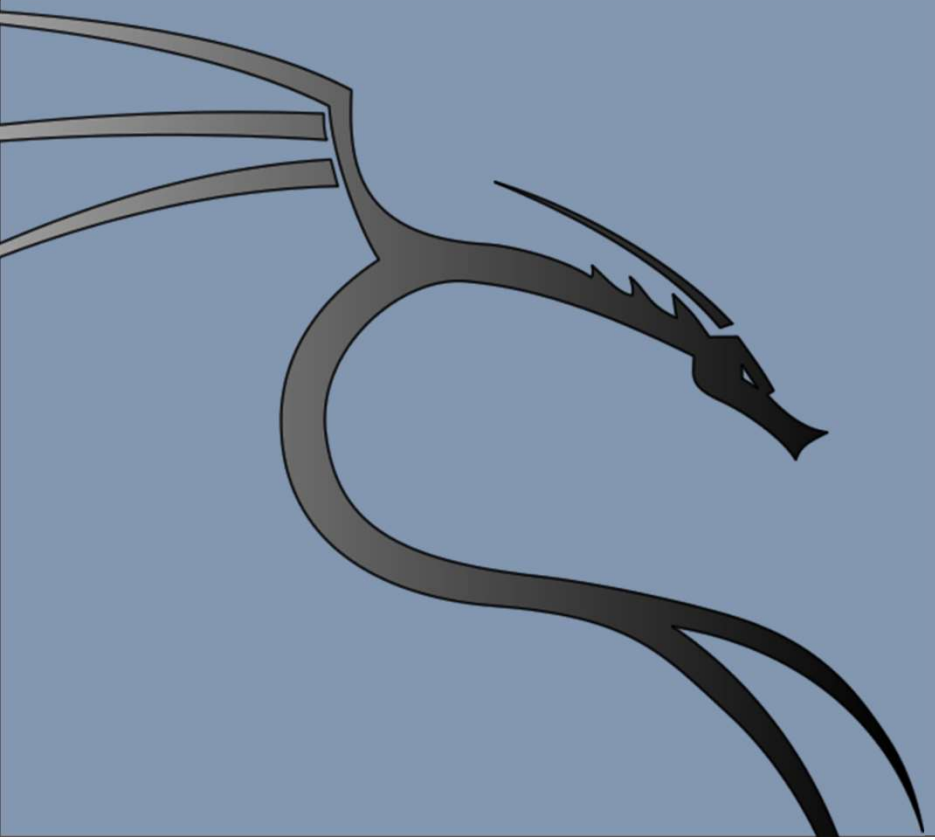
Utilizarea sistemelor de operare în rețea
Lucru individual nr. 1

Explorând Kali Linux:
un instrument puternic pentru securitatea cibernetica

Elevă: Apareci Aurica
Grupa: AAW 2042
Profesor: Tornea Victor

Introducere în Kali Linux

- Ce este Kali Linux?
- Scopul Kali Linux în securitatea cibernetică.
- Relevanța și importanța subiectului.



Kali Linux este o distribuție de sistem de operare bazată pe Linux, specializată în securitate cibernetică și testare de penetrare. Este utilizată de profesioniștii în domeniul securității pentru a evalua vulnerabilitățile și a efectua teste de securitate asupra rețelelor și sistemelor informatice, oferind o suită largă de instrumente pentru aceste scopuri.

Scopul principal al Kali Linux în securitatea cibernetică este de a servi ca o platformă specializată pentru testarea şi evaluarea securităţii reţelelor şi sistemelor informatice. Aceasta include:

Testarea de penetrare: Kali Linux furnizează o suită de instrumente şi aplicaţii preinstalate pentru a identifica şi exploata vulnerabilităţile sistemelor, simulând atacuri cibernetice într-un mediu controlat.

Evaluarea securităţii: Profesioniştii în securitate cibernetică pot utiliza Kali Linux pentru a efectua scanări şi audituri de securitate pentru a descoperi potenţialele ameninţări şi probleme de securitate într-un sistem sau reţea.

Dezvoltarea şi testarea de aplicaţii securizate: Kali Linux oferă resurse pentru dezvoltatorii de software pentru a testa aplicaţiile în ceea ce priveşte vulnerabilităţile de securitate şi pentru a asigura securitatea acestora.

Instruire şi educaţie: Este, de asemenea, utilizat ca instrument de instruire şi educaţie în domeniul securităţii cibernetice, pentru a ajuta profesioniştii şi studenţii să înţeleagă mai bine ameninţările şi tehnicile de protecţie.

Istoricul Kali Linux

- Originea şi evoluţia distribuţiei.
- De la BackTrack la Kali Linux.

1

Kali Linux este o distribuție de sistem de operare bazată pe Linux, specializată în securitate cibernetică. Dezvoltarea distribuției Kali Linux a început cu BackTrack, o distribuție Linux specializată în testarea de securitate. BackTrack a fost dezvoltat inițial de către Mati Aharoni și Max Moser în 2006 și s-a bucurat de o popularitate semnificativă în comunitatea securității cibernetice.

2

Cu toate acestea, pe măsură ce cerințele au crescut și tehnologia a avansat, echipa din spatele BackTrack a decis să dezvolte o distribuție nouă și mai robustă, care să poată satisface nevoile tot mai complexe ale specialiștilor în securitate cibernetică.

3

Astfel, în 2013, BackTrack a fost înlocuit oficial de Kali Linux, care a fost conceput pentru a fi o platformă mai avansată, cu un ecosistem mai bogat de instrumente și resurse pentru testarea de securitate. Această tranziție a permis comunității de securitate cibernetică să aibă la dispoziție o soluție de ultimă generație pentru investigarea și evaluarea securității rețelelor și sistemelor.

4

Cu actualizări constante și o creștere continuă a popularității, Kali Linux a devenit distribuția preferată a profesioniștilor în securitate cibernetică

Caracteristici-cheie ale Kali Linux

- Enumerarea principalelor caracteristici ale Kali Linux.
- Accent pe instrumentele de testare a securităţii şi forensice.

Kali Linux, o distribuție Linux specializată în securitate cibernetică, se evidențiază prin mai multe caracteristici-cheie:

1. Instrumente de testare a securității: Kali Linux oferă o gamă variată de instrumente pentru testarea securității rețelelor și sistemelor. Acestea includ scannere de vulnerabilități, suite de testare de penetrare, analizatoare de pachete și multe altele. Acest focus pe securitate îl face o alegere ideală pentru specialiștii în securitate cibernetică.

2. Instrumente de testare forensica: Distribuția include și o serie de instrumente pentru testarea forensica, care permit specialiștilor să investigheze incidente de securitate, să recupereze date și să efectueze analize detaliate asupra sistemelor compromise.

3. Actualizări constante: Kali Linux beneficiază de actualizări constante, lucru care asigură că utilizatorii au întotdeauna acces la cele mai recente instrumente și patch-uri de securitate.

4. Compatibilitate și suport hardware larg: Kali Linux poate fi instalat pe o varietate de platforme hardware și arhitecturi, lucru care oferă o flexibilitate considerabilă în alegerea mediului de testare.

5. Medii multiple de instalare: Kali Linux poate fi instalat ca o distribuție independentă, într-o mașină virtuală sau pe dispozitive hardware dedicate, cum ar fi Raspberry Pi. Acest lucru oferă utilizatorilor flexibilitate în funcție de nevoile lor.

Interfața utilizatorului în Kali Linux

- Prezentarea interfeței grafice și a liniei de comandă.


Home — Dolphin
Search
Preview
Split
Control
Places
Home
Desktop
Documents
Downloads
Trash
Remote
Network
Recently Saved
Today
Yesterday
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
6 Folders
888.8 MiB free
kali
Search...
All Applications
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
Favorites
Applications
Computer
History
Leave
File Edit View Bookmarks Settings Help
cpu
11:39:42 PM
i5-6400 2.7 GHz
CPU
Core1
Core2
Core3
Core4
mem
Memory: 1.94 GiB
Used: 1.19 GiB
59%
Avail: 805 MiB
40%
Cache: 651 MiB
Free: 209 MiB
Swap: 1.99 GiB
Used: 37.6 MiB
Free: 1.96 GiB
disks
root 12.2 GiB
Used: 10.2 GiB
93%
Free: 889 MiB
7%
net
Download
Byte: 0 Byte/s
Bit: 0 bitps
Total: 14.4 MiB
Upload
Byte: 0 Byte/s
Total: 670 KiB
processes
filter
cpu lazy
Pid: Program: Tr: User: Mem% %Cpu%
15642 stress 1 kali 0.0 24.9
2591 konqueror 29 kali 17.8 0.0
883 kwin_x11 34 kali 12.3 0.3
12326 bash 1 kali 0.3 0.9
895 Xorg 28 root 5.7 0.1
891 plasmashell 26 kali 18.4 0.2
12297 konsole 11 kali 4.9 0.0
1584 dolphin 12 kali 3.9 0.0
1701 konsole 11 kali 4.7 0.0
select
1/8 pg
File Edit View Bookmarks Settings Help
OS: Kali GNU/Linux Rolling x86_64
Host: VirtualBox 1.2
Kernel: 5.5.0-kali2-amd64
Uptime: 7 mins
Packages: 2660 (dpkg)
Shell: zsh 5.8
Resolution: 1920x1080
DE: Plasma
WM: KWin
Theme: Kali-Dark [Plasma], Breeze [GTK2/
Icons: Flat-Remix-Blue-Dark [Plasma], br
Terminal: konsole
CPU: Intel i5-6400 (4) @ 2.711GHz
GPU: 00:02.0 VMware SVGA II Adapter
Memory: 795MiB / 1991MiB
Home — Dolphin
kali : zsh — Konsole
tmp : bash — Konsole
11:39 PM

Instrumente în Kali Linux

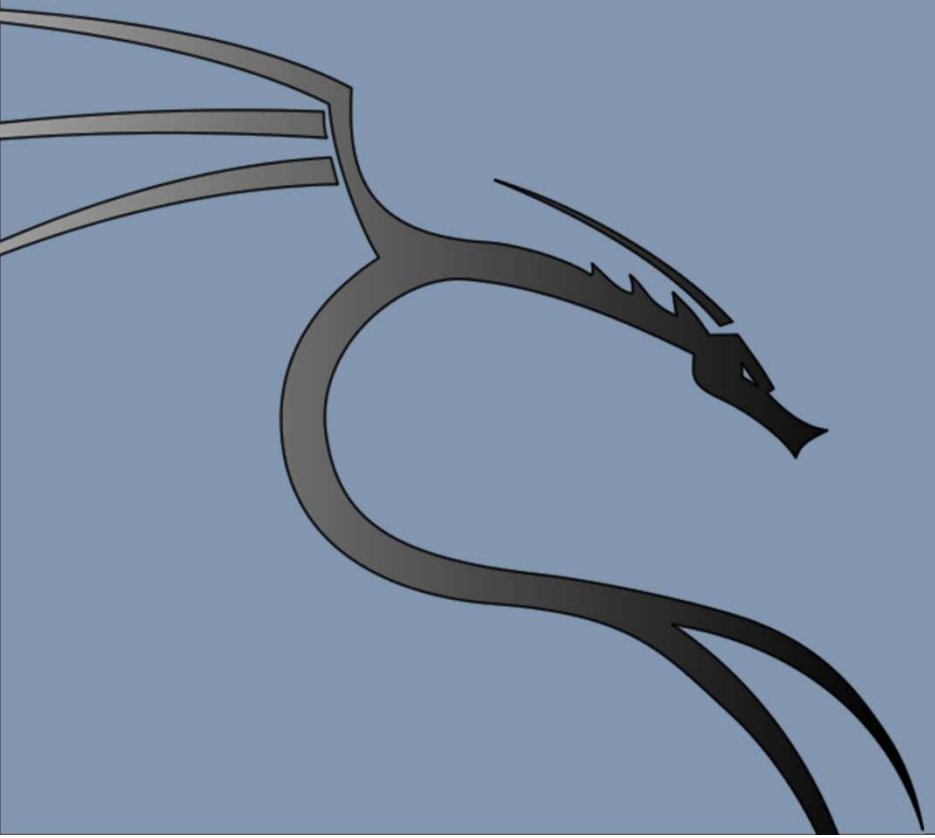
- Instrumente de testare a securității oferite de Kali Linux.
- Prezentarea instrumentelor de analiză forensica disponibile.

Kali Linux vine cu o gamă largă de instrumente și programe utile pentru testarea securității rețelelor, identificarea vulnerabilităților și efectuarea altor sarcini legate de securitate.

- **NMAP** - Un scanner de rețea folosit pentru descoperirea și evaluarea dispozitivelor conectate la o rețea.
- **Wireshark** - Un analizator de pachete care permite interceptarea și analiza traficului de rețea.
- **Metasploit** - Un cadru de testare de penetrare care include un set larg de module de exploatare și instrumente pentru testarea vulnerabilităților.
- **Hydra** - Un program pentru testarea brute-force pentru a sparge parolele.
- **John the Ripper** - Un alt instrument pentru spargerea parolelor.
- **OWASP ZAP** - Un proxy de securitate pentru testarea aplicațiilor web.
- **Sqlmap** - Un instrument pentru exploatarea și testarea vulnerabilităților de injecție SQL.
- **Recon-ng** - Un cadru de rețea pentru colectarea de informații de securitate.
- **Gobuster** - Un instrument pentru forțarea resurselor ascunse pe serverele web.
- **Nikto** - Un scaner pentru identificarea vulnerabilităților comune în serverele web.
- **Wifite** - Un instrument pentru testarea securității rețelelor Wi-Fi.
- **Dirb** - Un instrument pentru forțarea directoarelor pe serverele web.
- **Ettercap** - Un instrument pentru atacuri de tip "Man-in-the-Middle" pe rețele locale.

Actualizarea și Întreținerea Kali Linux

- Menținerea Kali Linux actualizat și securizat.



Pentru a menţine **Kali Linux** într-o stare actualizată şi secură, este esenţială aplicarea mai multor practici cheie. În primul rând, efectuează în mod regulat actualizări ale sistemului şi instalează pachetele de securitate disponibile. Asigură-te că kernel-ul este la cea mai recentă versiune. Implementează un firewall pentru a limita traficul neautorizat şi dezactivează serviciile de reţea neutilizate. Evită să rulezi aplicaţii cu drepturi de root, criptează datele şi sistemul de fişiere. Realizează copii de siguranţă periodice ale datelor. În plus, asigură-te că ai permisiunea pentru testarea securităţii dacă utilizezi Kali Linux în acest scop şi stai conectat la comunitatea Kali Linux pentru a rămâne informat cu privire la cele mai recente actualizări şi sfaturi de securitate.

Vă mulțumesc pentru atenție !