Introduction à Hack the Box

Hack The Box

HACKTHEBOX

- 470K joueurs
- Machines (boxes)
  - Easy, medium : vulnérabilités web, CVE, buffer overflows, Active Directory, ...
  - Hard, insane: custom exploitation en C++, binary exploitation, reverse engineering, failles cryptographiques, exploitation Windows/Linux avancée ...
- Challenges de CTF: web, crypto, reverse engineering, forensics, OSINT, ...
- Organisation de CTF publics et privés
- Battlegrounds: blue v. red team
- Pro Labs: réseau complexe à hacker
- Academy: exercices pratiques pour apprendre (concurrence à TryHackMe)
- Zone de recrutement (jobs)
- Meetups communautaires (20 pays)
- Préparation OSCP

Ce qu’il n’y a pas sur les machines HTB

- Bruteforce le service SSH
- Denial of Service
- Contourner les firewalls
- Pivoter dans un réseau
- Intercepter le trafic réseau avec Wireshark

177 MACHINES IN TOTAL

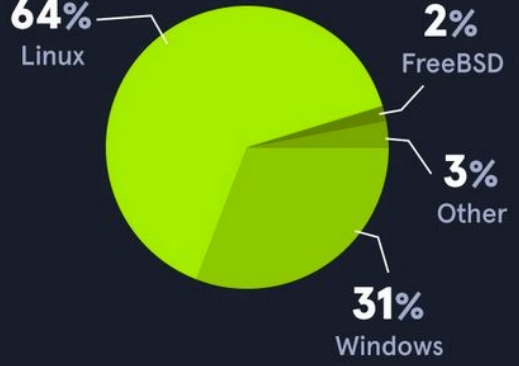
20 ACTIVE (ALWAYS FREE) | **157 RETIRED** (VIP WITH WRITE-UPS)

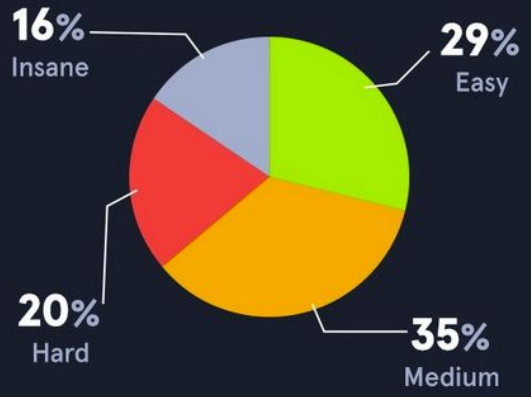
| **1 NEW EVERY WEEK!**



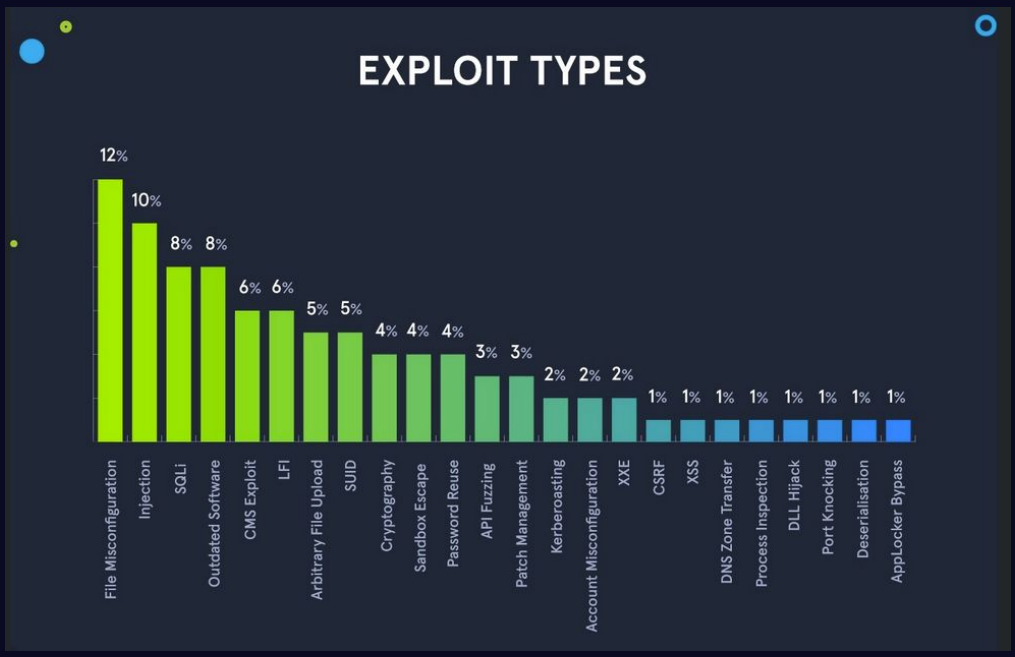



OS AND DIFFICULTY

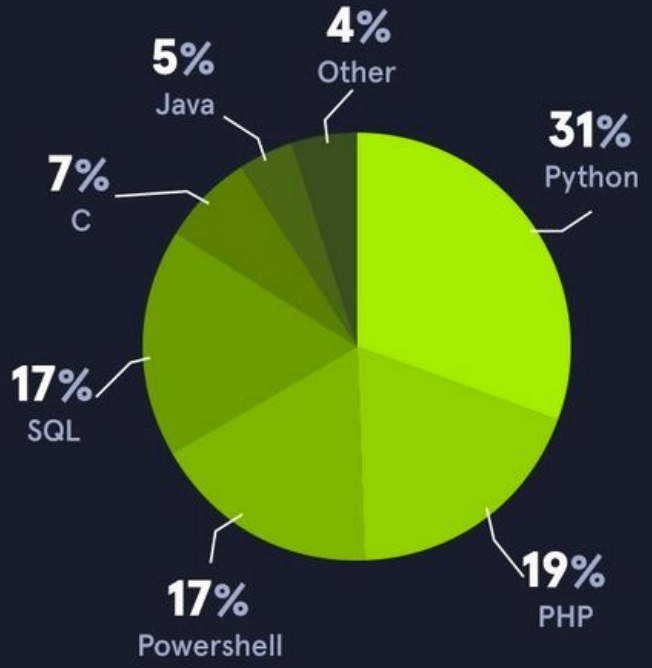





ATTACK ENTRY POINT
FTP
1%
Network
2%
Active Directory
7%
Binary Exploitation
15%
Web
75%


EXPLOIT TYPES
12%
10%
8% 8%
6% 6%
5% 5%
4% 4% 4%
3% 3%
2% 2% 2%
1% 1% 1% 1% 1% 1% 1% 1%
File Misconfiguration
Injection
SQLi
Outdated Software
CMS Exploit
LFI
Arbitrary File Upload
SUID
Cryptography
Sandbox Escape
Password Reuse
API Fuzzing
Patch Management
Kerberoasting
Account Misconfiguration
XXE
CSRF
XSS
DNS Zone Transfer
Process Inspection
DLL Hijack
Port Knocking
Deserialisation
AppLocker Bypass

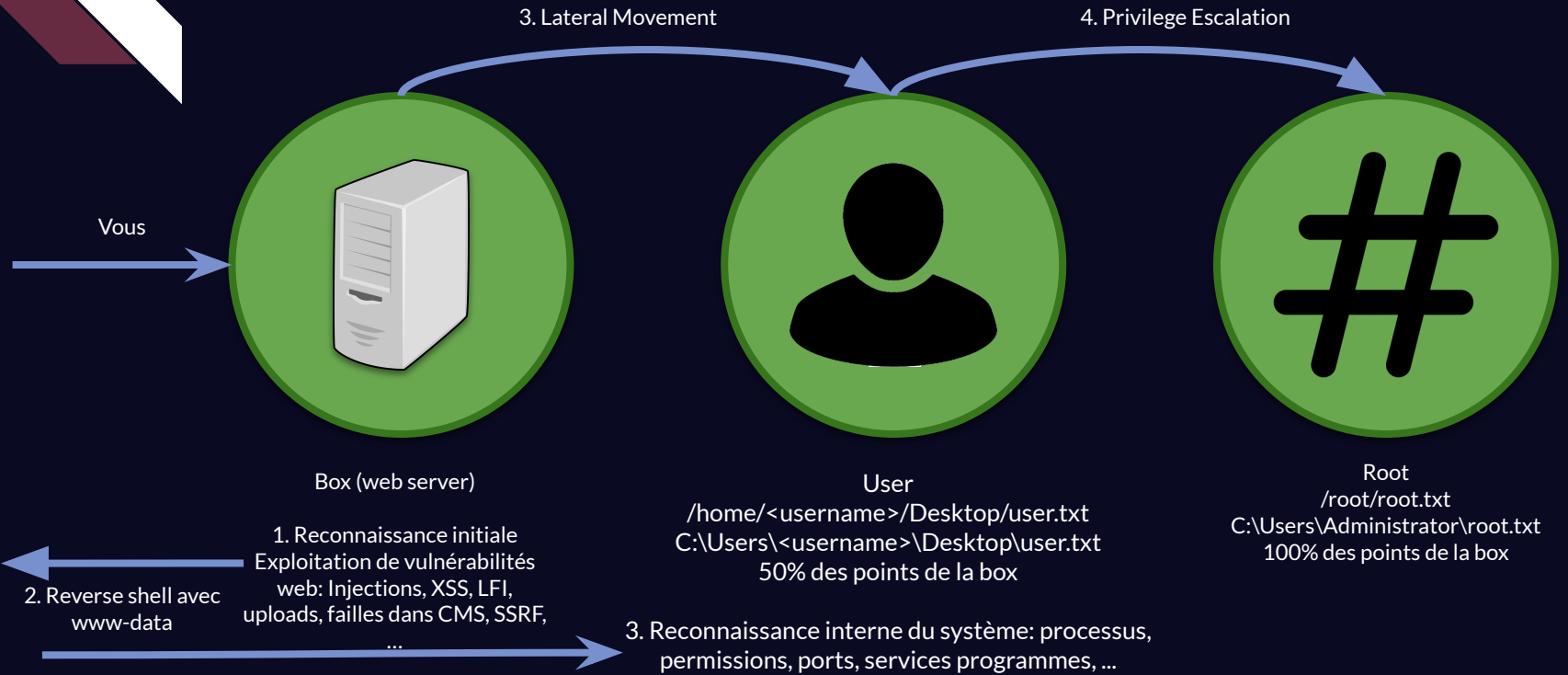
EXPLOIT LANGUAGES



Les outils communs

- Nmap, masscan Reconnaissance des ports
- Gobuster, wfuzz, dirbuster Énumération de sites web
- Smbclient, smbmap, ftp Dossiers partagés sur le réseau
- Dirb, cewl, nikto, burp, sqlmap Reconnaissance de sites web
- Msfconsole, msfvenom, searchsploit Exploits
- Hashcat, crackstation.net Crackage
- Commandes linux de base: dig, nslookup, curl, nc, netstat, find, crontab, id, ps, systemctl, ssh, scp, python, ...
- Outils Windows: impackets, crackmapexec, ldapsearch, rpcclient, powerview

Idée générale avec un serveur web



La reconnaissance initiale

1. Scan des ports avec nmap (TCP, UDP, 0-65535)
2. Banner grabbing des ports (telnet, netcat)
3. Énumération des dossiers et fichiers (gobuster)
4. Afficher le code source
5. Subdomain enumeration (gobuster, certificats HTTPS)
6. Recon des services (http, smtp, …) (et leur version)
7. Numéros de version avoir le réflexe de rechercher sur le web pour des vulnérabilités
8. Utiliser les bons outils pour communiquer avec les ports ouverts
9. Infos sur les utilisateurs: nom, emails, username
10. Mots de passe par défaut des services, connexion anonyme, combinaisons communes (admin:admin), bruteforce (peu probable)
11. Documents publics (smb, ftp, rsync…)

Privilege escalation

1. Utilisateurs du système: leurs fichiers personnels, leurs privilèges, leur historique,
2. Numéro de version (système, logiciels, services, …)
3. Si la machine tournait un serveur web, inspectez son dossier de base
4. Répertoires et fichiers communs: /var/www/html, C:\Program Files\, /etc/passwd, ...
5. Ports ouverts seulement à l'interne (ex. :127.0.0.1:3000)
6. Processus actifs, services, tâches programmées, logiciels installés
7. Les clés privés de l'utilisateur (~/.ssh/authorized_keys) ou y écrire sa propre clé privée SSH
8. Configuration système: $PATH, SUID binaries, sudo rights (sudo -l)
9. Configuration des services
10. Writable files, récemment modifiés et non standards
11. Vecteur d'attaque communs: buffer overflows, ...

LinPEAS/WinPEAS scripts, GTFO bins, LinEnum.sh

Essentiel: prendre des notes

- CherryTree
- Joplin
- Output des commandes
- Tmux
- ....

Bloqué.e?

1. RTFM
2. Google Fu (Github Fu)
3. Vérifier les paramètres de vos commandes pour avoir la formule adéquate
4. Ippsec sur Youtube, ippsec.rocks
5. Write-ups des machines retirées
6. Porter attention aux nouvelles technologies (HTTP/2, WebSocket, blockchain ...)
7. Lire les blogs sur des vulnérabilités récents
8. Faire plus de recon
9. Forums officiels HTB
10. Discord officiel HTB

Good to know...

- Quand vous trouvez un mot de passe valide, n'hésitez pas à l'essayer avec d'autres services (password reuse)
- Reverse shell: Pentest Monkeys
- Web shells
- Upgrade shell for more flexibility
- SecLists pour de bonnes wordlists
- SSH (or wtv) to John
- Avoir une VM sous Windows pour s'avérer utile pour les boxes Windows
- Exfiltration de données via SMB, HTTP (voir Ippsec)
- `Python -m http.server 80` pour transférer des fichiers de votre host à la box
- Compiler des binaires pour Windows sous Linux avec Mingw-w64