



Unix / linux

Ethical hacking - Sys/linux



ISEN AP4
Master 2 IPIIJulien Hochart – jul@hochart.fr

“

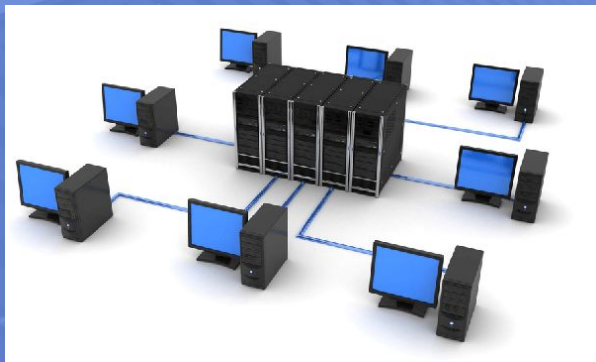


Kevin Mitnick: Why am I here and you are not?
Tsutomu Shimomura: I mean, how lame are you?
Takedown (2000)



Scénario

- Scénario du **test interne en boîte noire**
 - Connexion au LAN
 - Intrusion en utilisant les briques d'infra
 - 1 login employé connu





Scénario

1. Connexion au LAN (ici au hotspot)
2. Découverte des hosts up sur le réseau
3. Identification d'un service SSH
4. Brute force (dict) d'un compte connu → shell unprivileged
5. Elevation de privilèges (linux) → local root
6. Capture des hashes du serveur
7. Brute force (dict) des hash → "domain" admin



Remarques

- Merci de ne pas reboot / RM la VM quand vous êtes root :)



1 - Connexion au LAN / WLAN

- SSID + WPA PSK sur l'AP
- Check IP DHCP OK, ping GW



2-3 - Découverte des services

- Scanner le subnet en TCP ou ICMP pour trouver les hosts UP [**ping, hping, ...**]
- Scanner les hosts UP pour trouver un service ssh (OpenSSH 7.4p1 Debian 10+deb9u5) [**nmmap, nc, hping, ...**], ou tout faire en 1 fois
- Objectif: 1 host, 1 port



4 - Bruteforce SSH online

- 1 user employé connu: "jho"
 - La phase de reconnaissance à permis d'apprendre que "jho" utilise des passwords à 3 chiffres (ex: 666)
 - Construire un dico contenant les MDP possibles
- [bash]**
- Bruteforcer le service ssh **[hydra, medusa, ...]**
 - Objectif: shell (unprivileged)



5 - PrivEsc

- 2 pistes ici
 - **“Badly configured sudo”**
 - **“Bad perms on root owned executables / cronjobs”**
- Objectif: Shell root



6 - Hashes et rebond

- Récupérer les hashes système
- Les casser en local (offline) sur votre kali avec un bruteforcer **ljohn, hashcat, ...]**
- Objectif: 2 comptes du master d'install, admincorp et adminoracle
- → **Rebond sur le SI**



7 - Bonus

Le compte root a un password numérique (quelques chiffres).

Comparer l'efficacité d'un password cracker offline et du bruteforce d'un service en ligne

[john // incremental]