Tests d’intrusion de machines virtuelles

SEC2

A. Brouste
T. Gennuso

VM1 - Analyse

- **OS obsolète**

```
~$ sudo nmap -O 192.168.122.204
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-05 19:17 CET
Nmap scan report for 192.168.122.204
Host is up (0.00037s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
631/tcp  open  ipp
3306/tcp open  mysql
MAC Address: 52:54:00:E2:2F:E8 (QEMU virtual NIC)
Device type: general purpose|media device
Running: Linux 2.6.X, Star Track embedded
OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.6.23 cpe:/h:star_track:srt2014hd
OS details: Linux 2.6.9 - 2.6.30, Star Track SRT2014HD satellite receiver (Linux 2.6.23)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.45 seconds
```

VM1 - Analyse

- **OS obsolète**
- **Pas de Par-Feu**

VM1 - Analyse

- **OS obsolète**
- **Pas de Pare-Feu**
- **Identification des services sur la machine**

```
user@Kali:~$ nmap 192.168.122.204 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-23 10:01 CET
Nmap scan report for 192.168.122.204
Host is up (0.0015s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 3.9p1 (protocol 1.99)
80/tcp   open  http       Apache httpd 2.0.52 ((CentOS))
111/tcp  open  rpcbind    2 (RPC #100000)
443/tcp  open  ssl/https?
631/tcp  open  ipp        CUPS 1.1
3306/tcp open  mysql      MySQL (unauthorized)
```

VM1 - Analyse

- **OS obsolète**
- **Pas de Pare-Feu**
- **Identification des services sur la machine**
- **Trafic web en clair**

VM1 - Analyse

- **OS obsolète**
- **Pas de Pare-Feu**
- **Identification des services sur la machine**
- **Trafic web en clair**
- **Bibliothèques de chiffrement obsolète**
  - Interception de flux par attaque man-in-the-middle

VM1 - Analyse

- **OS obsolète**
- **Pas de Pare-Feu**
- **Identification des services sur la machine**
- **Trafic web en clair**
- **Bibliothèques de chiffrement obsolète**
- **Mauvais certificats de sécurité**

VM1 - Analyse

- **OS obsolète**
- **Pas de Pare-Feu**
- **Identification des services sur la machine**
- **Trafic web en clair**
- **Bibliothèques de chiffrement obsolète**
- **Mauvais certificats de sécurité**
- **Injections SQL**

VM1 - Analyse

- **OS obsolète**
- **Pas de Pare-Feu**
- **Identification des services sur la machine**
- **Trafic web en clair**
- **Bibliothèques de chiffrement obsolète**
- **Mauvais certificats de sécurité**
- **Injections SQL**
- **Exécution de commandes depuis l’interface d’administration**

VM1 – Exploitation

Approche par le service web

→ page de login

→ injection SQL : « root » & « ' OR 1=1 # »

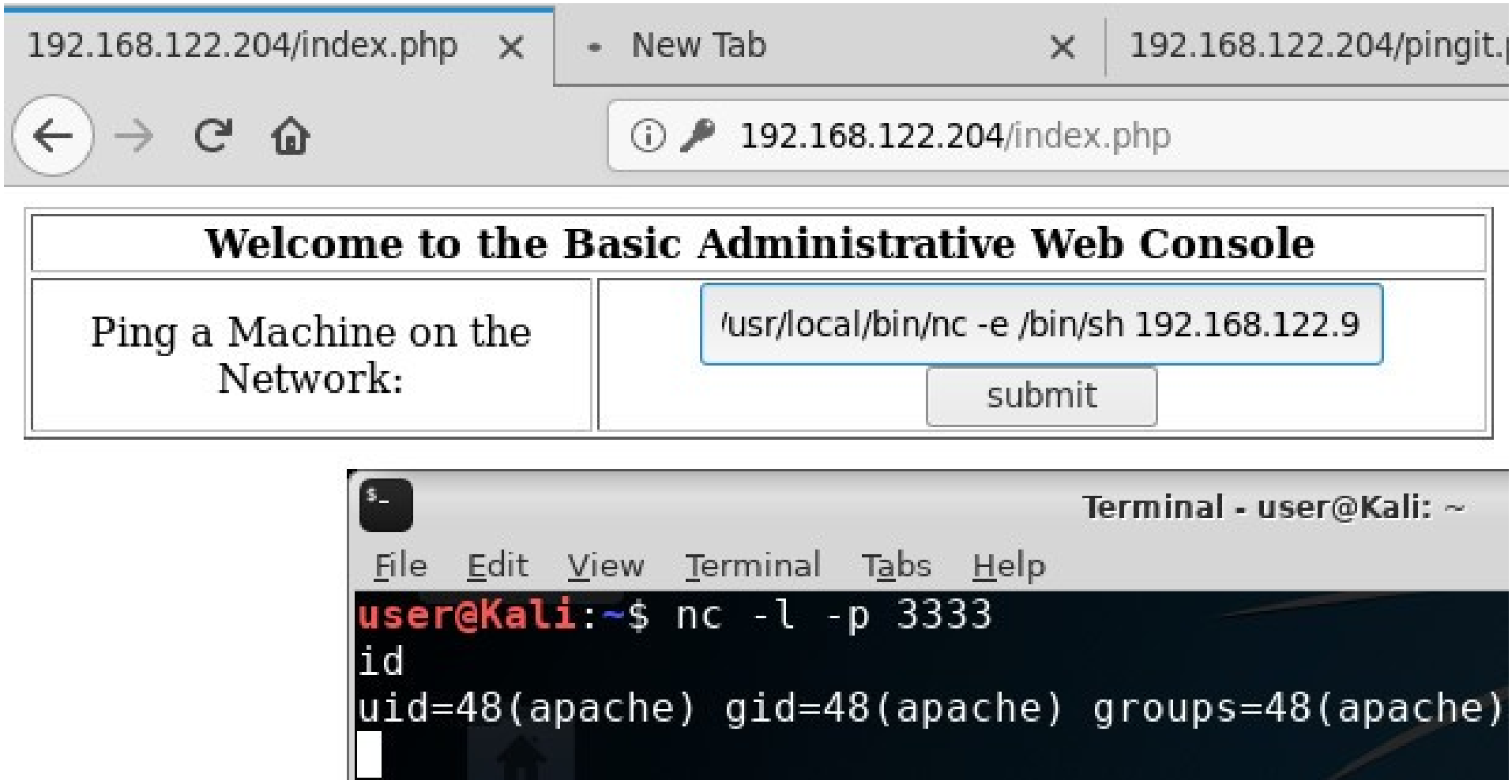
→ accès à l'interface d'administration

Possibilité d'exécuter un ping

→ d'autres commandes peuvent être exécutées

→ obtention d'un accès distant à la machine

VM1 – Exploitation (obtention d'un accès distant)



VM1 – Exploitation

Approche par le service web

→ page de login

→ injection SQL : « root » & « ' OR 1=1 # »

→ accès à l'interface d'administration

Possibilité d'exécuter un ping

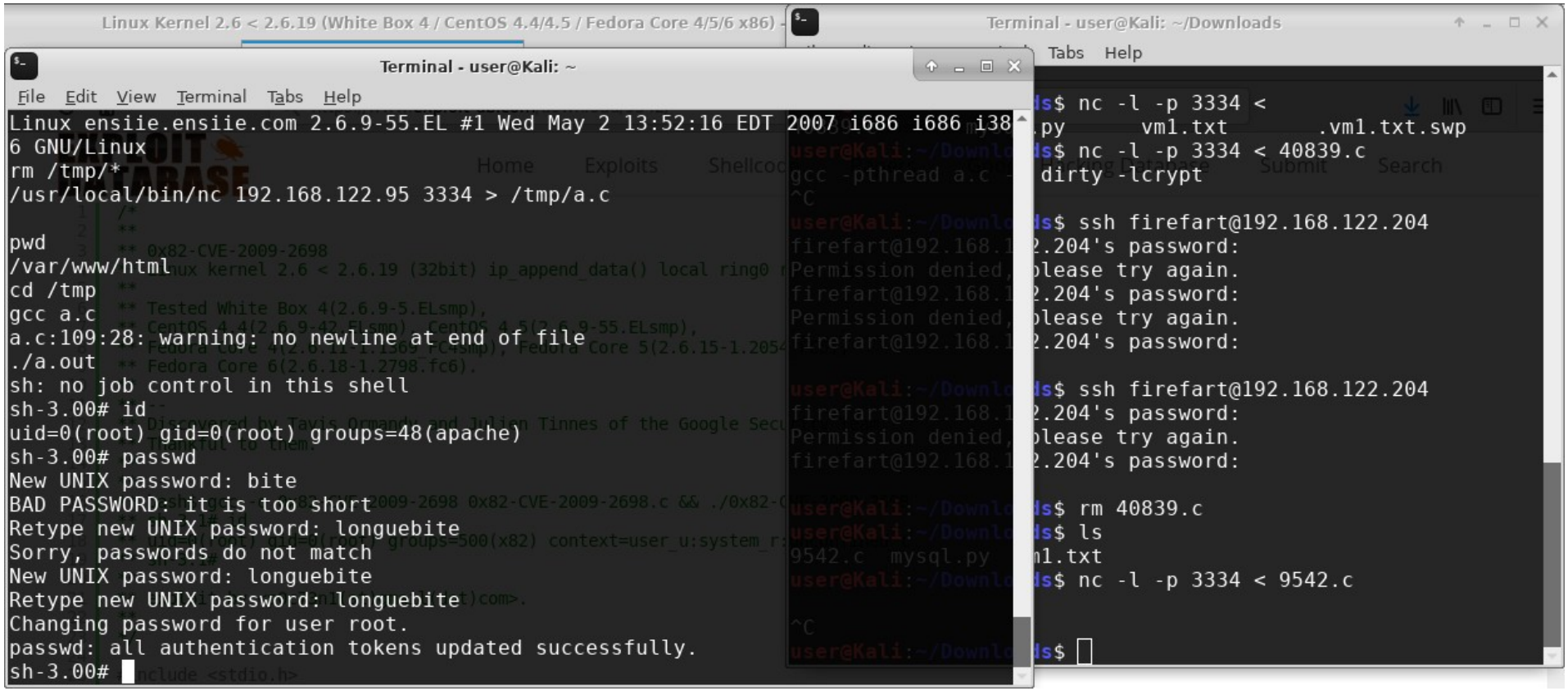
→ d'autres commandes peuvent être exécutées

→ obtention d'un accès distant à la machine

Avec un shell sur la machine

→ un exploit à compiler permet de changer le mdp root

VM1 – Exploitation (accès root)



VM1 - Recommandations proposées

- **Mise à jour du système**

VM1 - Recommandations proposées

- **Mise à jour du système**
- **Mise en place d’un Par-Feu**
  - Iptables

VM1 - Recommandations proposées

- **Mise à jour du système**
- **Mise en place d’un Par-Feu**
- **Améliorer la configuration des services**
  - Pas besoin d’être ouverts en TCP à l’extérieur

VM1 - Recommandations proposées

- **Mise à jour du système**
- **Mise en place d’un Par-Feu**
- **Améliorer la configuration des services**
- **Durcir le serveur web**
  - HTTPS, désactiver la méthode TRACE, désactiver le directory listing

VM1 - Recommandations proposées

- **Mise à jour du système**
- **Mise en place d’un Par-Feu**
- **Améliorer la configuration des services**
- **Durcir le serveur web**
- **Mise à jour des Bibliothèques de chiffrement**

VM1 - Recommandations proposées

- **Mise à jour du système**
- **Mise en place d’un Par-Feu**
- **Améliorer la configuration des services**
- **Durcir le serveur web**
- **Mise à jour des Bibliothèques de chiffrement**
- **Générer de nouveaux certificats de sécurité**

VM1 - Recommandations proposées

- **Mise à jour du système**
- **Mise en place d’un Par-Feu**
- **Améliorer la configuration des services**
- **Durcir le serveur web**
- **Mise à jour des Bibliothèques de chiffrement**
- **Générer de nouveaux certificats de sécurité**
- **Nettoyer les chaînes entrées pour éviter les injections SQL**

VM2 - Analyse

- **OS obsolète**

```
user@Kali:~$ nmap -sV 192.168.122.227
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-23 12:12 CET
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 16.67% done; ETC: 12:12 (0:00:30 remaining)
Nmap scan report for 192.168.122.227
Host is up (0.0020s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE     VERSION
22/tcp    open  ssh         OpenSSH 2.9p2 (protocol 1.99)
80/tcp    open  http        Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl
/2.8.4 OpenSSL/0.9.6b)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https   Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4
OpenSSL/0.9.6b
32768/tcp open  status      1 (RPC #100024)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.98 seconds
```

VM2 - Analyse

- **OS obsolète**
- **Service d’accès à distance accessible**

VM2 - Analyse

- **OS obsolète**
- **Service d’accès à distance accessible**
- **Serveur web Apache non configuré**

VM2 - Analyse

- **OS obsolète**
- **Service d’accès à distance accessible**
- **Serveur web Apache non configuré**
- **Faille dans Samba permettant un accès à distance privilégié**

VM2 – Exploitation

Approche par le service Samba

→ version de samba obsolète

→ un exploit à compiler permet d'obtenir une invite de commande root

VM2 – Recommandations proposées

- **Mise à jour du système**

VM2 – Recommandations proposées

- **Mise à jour du système**
- **Mise en place d’un par-feu**

VM2 – Recommandations proposées

- **Mise à jour du système**
- **Mise en place d’un pare-feu**
- **Configurer Apache correctement**

VM2 – Recommandations proposées

- **Mise à jour du système**
- **Mise en place d’un pare-feu**
- **Configurer Apache correctement**
- **Mise à niveau de Samba**

VM3 - Analyse

- **Trafic web en clair**
- **Faille de type injection SQL**
- **Compte administrateur avec nom trop générique**
- **Inclusion arbitraire de fichier dans l’espace membre**
- **Mots de passe en clair**
- **Évasion du shell captif**
- **Système hôte obsolète**

VM3 - Exploitation

Approche par serveur web

→ injection SQL

Possibilité d'afficher des fichiers

→ affichage de fichiers systèmes : /etc/passwd

→ connexion en SSH avec les id fournits

Accès à un shell captif

→ exploitation pour accéder à un shell normal

→ transfert d'un exploit déjà compilé par le port 443 pour obtenir un accès root

VM3 – Recommandations proposées

- **Modifier la configuration sur serveur Apache et générer des certificats de sécurité**
- **Nettoyer les entrées utilisateurs de l'application web**
- **Changement du nom du compte Administrateur**
- **Changer de méthode d'affichage d'information sur les membres**
- **Conserver des hash des mots de passe dans la base de données**
- **Mettre à jour le shell captif**
- **Mise à jour du système**