Épreuve E6 - Infrastructure dédié au Pentesting

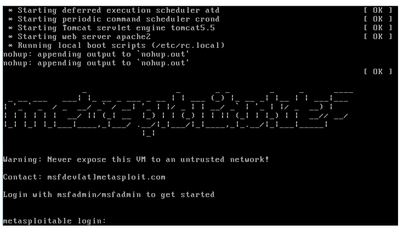
1. Présentation de l'Infrastructure

L'architecture réseau est composée des éléments suivants :

- **Routeur** : 192.168.2.2 (Accès au LAN)
- **Pare-feu OpnSense** : 192.168.2.1 (Sécurisation et routage interne)
- **Réseaux VLANs** :
  - **VLAN 4** : 192.168.4.0/24
  - **VLAN 10** : 192.168.10.0/24 (Hyperviseurs Proxmox & environnements de production)
  - **VLAN 50** : 192.168.50.0/24 (Clients)

Schéma Réseau

2. Environnement de Pentesting



2.1 Metasploitable 2

- **Adresse IP** : 192.168.10.40
- **Description** : Metasploitable 2 est une machine virtuelle intentionnellement vulnérable utilisée pour les tests de pénétration et la formation en cybersécurité.
- **Services vulnérables** :
  - SSH (faiblesse dans l'authentification)
  - VSFTPD (faille d'exécution de code)
  - Apache Tomcat (accès administrateur par défaut)
  - Base de données MySQL avec des credentials faibles

```
root@kali:~# nmap -p- -sV 10.0.2.6

Starting Nmap 7.25BETA1 ( https://nmap.org ) at 2017-08-28 00:48 EDT
Stats: 0:00:29 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 00:49 (0:00:01 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 00:49 (0:00:02 remaining)
Stats: 0:02:04 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 00:50 (0:00:04 remaining)
Nmap scan report for 10.0.2.6
Host is up (0.00013s latency).
Not shown: 65505 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  rmiregistry GNU Classpath grmiregistry
1524/tcp  open  shell       Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         Unreal ircd
6697/tcp  open  irc         Unreal ircd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
```

2.2 Kali Linux

- **Adresse IP** : 192.168.10.41
- **Description** : Kali Linux est une distribution Linux spécialisée en cybersécurité et en tests d'intrusion.
- **Outils intégrés** :
  - **Metasploit** (cadre d'exploitation de vulnérabilités)
  - **Nmap** (scanner de ports et de réseau)
  - **Burp Suite** (analyse de requêtes HTTP)
  - **John The Ripper** (brute-force de mots de passe)

2.3 Suricata (IDS)

- **Adresse IP** : 192.168.10.42
- **Description** : Suricata est un système de détection d'intrusion (IDS) qui surveille le trafic réseau en temps réel pour détecter les attaques et les menaces potentielles.
- **Rôle** :
  - Analyse du trafic réseau pour identifier des modèles d'attaques
  - Alertes en cas d'activités suspectes
  - Journalisation des événements de sécurité

Exemple d'intégration d'une capture d'écran :

3. Conclusion

Ce laboratoire de pentesting permet de simuler des attaques, d'analyser le comportement des outils et de renforcer la sécurité des systèmes. L'utilisation de Metasploitable 2 comme cible, Kali Linux comme machine d'attaque, et Suricata comme IDS offre une approche complète d'apprentissage.