Réseau et Sécurité

TP 1 - Exploration réseau et collecte d'informations sur une cible

La première étape d'un test d'intrusion, l'étape de reconnaissance, consiste à collecter toutes les informations (noms DNS, adresses IP ou postales, services proposés, noms des responsables techniques, données des réseaux sociaux,...) pouvant être pertinentes pour réaliser une intrusion. On distingue la reconnaissance passive (collecter des informations sans interagir avec le système cible) de la reconnaissance active (interaction directe avec la cible). Lors de l'étape de reconnaissance on peut utiliser des outils généralistes comme dig ou whois ; ou conçus spécialement à cet effet comme ceux fournis par le serveur web de dnsdumpster.com

Exercise 1 Reconnaissance de la cible

dig C'est un client DNS. Sa syntaxe générale est la suivante :

```
$ dig @serveurDNS nom typeEnregistrement
```

L'argument `@serveurDNS` est optionnel. Dans ce cas, dig contactera le serveur indiqué dans `/etc/resolv.conf`. De même le `typeEnregistrement` est optionnel. Ce sera le type A par défaut.

Utilisez dig (avec l'option +short pour que dig ne soit pas trop bavard) pour récupérer les informations suivantes :

- Les IP des serveurs de nom de l'université Clermont Auvergne (domaine uca.fr).
- Les IP des serveurs de messagerie de l'université.
- Le FQDN du serveur web de l'ISIMA et de l'université et les IP qui leur sont associées.

1. Quel peut être l'intérêt d'avoir plusieurs IP associées à un seul nom pour un serveur web ?

whois C'est un service de recherche fourni par les registres internet (organismes qui allouent des blocs d'IP) ou par les registres de noms de domaine (organismes qui gèrent les informations relatives au domaines de premier niveau, par exemple, l'AFNIC pour le domaine .fr). whois est aussi le nom d'un outil permettant d'interroger un serveur whois.

Utilisez whois pour obtenir des informations sur le domaine de l'université :

```
$ whois isima.fr
```

1. Quel est le serveur whois qui a répondu ?
2. Quel est le nom du registrar (l'organisme qui a enregistré le nom de domaine) ?
3. Quelles informations sont utiles pour obtenir davantage d'informations sur le SI ou le personnel de l'université ?

Utilisez maintenant `whois` pour obtenir des informations sur le domaine `wikipedia.org`.

1. Y-a-t-il des informations utiles pour obtenir davantage d'informations sur le SI ou le personnel de wikipedia ? Essayer avec maintenant avec `wikipedia.org`. Que trouvez-vous ?

`whois` peut aussi être utilisé pour trouver le propriétaire d'une IP.

1. Quel est l'adresse du réseau de cette IP (champ `inetnum` ou `NetRange`) ?

dig peut ensuite découvrir d'autres hôtes de son réseau avec une résolution inverse (option -x de dig).

1. A l'aide de ces outils trouver à qui appartient l'IP `140.82.121.3`.

dnsdumpster Le serveur web dnsdumpster.com offre un service de découverte d'hôtes basé sur le protocole DNS. Ouvrez un navigateur web à l'adresse `https://dnsdumpster.com/`. Effectuez une recherche sur le domaine `gamekult.com`

2. Quelles sont les types d'enregistrements DNS trouvés (A, NS, CNAME, . . .) ?
3. Le site web gamekult fait appel à plusieurs compagnies pour héberger ses services. Lesquelles ?
4. Quelle compagnie posséde les serveurs DNS faisant autorité sur gamekult.com ?
5. Quelle compagnie posséde les serveurs d'envoi de mails vers des adresses en @gamekult.com ?
6. Quelle compagnie posséde le serveur web www.gamekult.com ?
7. Quel est l'intérêt pour gamekult, en terme de sécurité, d'avoir autant d'hébergeurs ?

Exercise 2 Identification des vulnérabilités

Cet exercice doit être réalisé sur le serveur pédagogique **Ada**.

Une fois la reconnaissance achevée, le pentester peut ensuite analyser la cible (par exemple, avec nmap) et, à l'aide d'une base de données comme CVE (Common Vulnerabilities Exposures), identifier ses vulnérabilités. CVE recence de nombreuses vulnérabilités détectées dans des logiciels (serveur, client web,...), systèmes d'exploitation ou équipements (switchs, routeurs, pare-feux,...). Pour des raisons évidentes de sécurité une vulnérabilité n'est publiée qu'une fois qu'un correctif a été trouvé. À titre d'exemple, nous allons identifier quelques vulnérabilités de l'hôte scanme.nmap.org mis à disposition par les développeurs de nmap à des fins de test ou pédagogiques. Vous avez donc le droit de lancer des opérations de balayage sur cet hôte.

Lancez un balayage nmap sur scanme.nmap.org pour connaître la version du service http qu'elle propose : `nmap -sV -p80 -P0 scanme.nmap.org`

Recherchez sur `www.cvedetails.com` les vulnérabilités de cette version.

1. Combien de vulnérabilités avez-vous trouvées ? Donnez les identifiants (CVE ID) des trois premières vulnérabilités découvertes.
2. À quel(s) type(s) d'attaque(s) (Vulnerability Type(s)) ces vulnérabilités expose(nt)-elle(s) ?
3. Décrire ces type(s) en quelques mots.

Exercise 3 L'outil recon-ng

Recon-ng est un outil en ligne de commande permettant de collecter de nombreuses informations sur une cible en consultant des bases de données publiques (whois, serveurs DNS, shodan, réseaux sociaux,...). Il a l'avantage de fournir une unique interface pour consulter plusieurs sources. De plus les données collectées sont stockées dans une base de données structurée, ce qui facilite la récupération et l'analyse de ces données.

Installez le paquet recon-ng puis utilisez le pour collecter les informations suivantes sur une cible de votre choix (ex., une compagnie ou un organisme public) :

— IP des hôtes dans le domaine ;
— noms et adresses mail de contacts ;
— adresses postales ;
— et toute autre information pertinente.