Pentest des infrastructures de MegaCorpOne

Rapport de pentest

Grégoire Roumache - Maxime Wallemme

21 Décembre 2021

Table des matières

Historique des versions

Date du document	Version	Description des changements
21-12-2021	1.0	Version initiale

1 Résumé

Nous avons reçu la tâche de réaliser un pentest des infrastructures de MegaCorpOne. Un pentest est une méthode d'évaluation de la sécurité d'un système d'information par la simulation d'attaques similaires à celles réalisées par des hackers dont l'objectif serait d'infiltrer MegaCorpOne. Les objectifs de ce test étaient d'identifier les infrastructures informatiques de l'entreprise et les failles qu'elles possèdent, de les exploiter, ainsi que de proposer des solutions pour les combler.

Lors de la réalisation de ce pentest, nous avons trouvés plusieurs vulnérabilités critiques dans le système d'information de MegaCorpOne. Nous avons pu accéder à plusieurs machines du réseau de l'entreprise et ce, avec un accès administrateur. Ceci est dû principalement à des configurations de sécurité faibles, des applications qui ne sont pas à jour et une politique de mots de passe trop faible.

Voici une liste des systèmes et le niveau d'accès que nous avons pu obtenir :

Adresse IP	Nom d'hôte	Système d'exploitation	Niveau d'accès
10.180.20.1	...	Windows 2016	Administrateur du domaine
10.180.20.2	...	Windows 2003	Administrateur
10.180.20.3	...	Windows 10	Administrateur
10.180.20.11	/	Linux	/
10.180.30.10	...	Linux	Accès root
10.180.30.15	...	Linux	/

Les adresses IP 10.180.20.254 et 10.180.30.254 étaient aussi utilisées mais ce sont les adresses des routeurs des sous-réseaux que nous avons attaqués.

Et voici la liste des service que nous avons découverts sur ces machines :

Adresse IP	Port	Protocol	Nom	Informations complémentaires
...	...	...	...	...

2 Recommendations

Nous recommandons de patcher les vulnérabilités identifiés lors de ce test et de renforcer la politique de mots de passe. Une fois ces tâches effectuées, nous pensons qu'il faut s'assurer qu'un attaquant ne pourra plus exécuter ces attaques en effectuant des tests. Il faudra aussi faire attention aux nouvelles vulnérabilités qui ne manqueront pas d'arriver dans le futur et continuer de protéger les systèmes au quotidien avec une stratégie de patching régulière.

3 Méthodologie utilisée

Nous avons utilisé une méthode souvent pratiquée par les hackers expérimentés pour s'attaquer à une entreprise. Elle est divisée en plusieurs étapes en commençant par la recherche d'informations sur l'entreprise afin de découvrir des vulnérabilités. Une fois trouvées, il faut les exploiter pour rentrer dans le système informatique de l'entreprise. Et finalement, on se déplace dans le système en attaquant d'autres machines de l'infrastructure et en essayant de prendre le contrôle de comptes administrateur.

3.1 Cadre du pentest

Dans le cadre de ce pentest, il a été décidé préalablement de chercher des informations pouvant conduire à une attaque de phishing ciblée mais de ne pas conduire cette attaque pour se concentrer sur l'aspect technique du système d'information. Concrètement, cela veut dire que nous avons réuni des informations sur les réseaux sociaux pour pouvoir nous faire passer pour un employé, comme le font certains hackers, afin de faire du social engineering mais nous n'avons pas conduit cette attaque.

3.2 Reconnaissance

Lors de cette étape très importante du pentest, nous avons cherché un maximum d'informations sur l'entreprise qui peuvent être utiles à des hackers dont l'objectif est de nuire à l'entreprise. L'objectif est de trouver et comprendre la surface d'attaque de l'entreprise autant d'un point de vue technique comme trouver le nombre de serveurs, domaines et sous-domaines internet; que des données qui pourraient être utiles à des fins de social engineering, comme des informations sur le CEO ou d'autres employés de l'entreprise. Ceci, sans outil de scan et énumération.

3.2.1 Informations sur quelques employés de la société

1. CEO, Joe Sheer :
   — né en 1968,
   — twitter : `https://twitter.com/joe_sheer/`,
   — email : `joe@megacorpone.com`.
2. Personne de contact technique (IT and Security Director), Alan Grofield :
   — travaille chez MegaCorp One depuis 1983,
   — linkedin : `https://www.linkedin.com/in/alan-grofield-32806468`,
   — email : `agrofield@megacorpone.com`.
3. Recruteur, Handy McKay :
   — twitter : `https://twitter.com/McKayHandy`.
4. Stagiaire, William Adler :
   — twitter : `https://twitter.com/RealWillAdler`.
5. WEB designer, Tom Hudson :
   — email : `thudson@megacorpone.com`,
   — twitter : `https://twitter.com/TomHudsonMCO`.
6. Développeur senior (Senior Developper), Tanya Rivera :
   — email : `trivera@megacorpone.com`,
   — twitter : `https://twitter.com/TanyaRiveraMCO`.
7. Directeur marketing (Marketing Director), Matt Smith :
   — email : `msmith@megacorpone.com`,
   — twitter : `https://twitter.com/MattSmithMCO`.
8. Vice-président des affaires juridiques (VP Of Legal), Mike Carlow :
   — email : `mcarlow@megacorpone.com`,
   — linkedin : `https://www.linkedin.com/in/mike-carlow-8128896a/`.

3.2.2 Informations sur le nom de domaine

1. Date d'enregistrement du nom de domaine :
   — 22-01-2013

2. Sous-domaines de megacorpone :
   — admin.megacorpone.com
   — beta.megacorpone.com
   — fs1.megacorpone.com
   — ftp.megacorpone.com
   — intranet.megacorpone.com
   — mail.megacorpone.com
   — mail2.megacorpone.com
   — manager.megacorpone.com
   — mgmt.megacorpone.com
   — michael.megacorpone.com
   — ns1.megacorpone.com
   — ns2.megacorpone.com
   — ns3.megacorpone.com
   — remote.megacorpone.com
   — router.megacorpone.com
   — siem.megacorpone.com
   — snmp.megacorpone.com
   — support.megacorpone.com
   — svn.megacorpone.com
   — syslog.megacorpone.com
   — test.megacorpone.com
   — vpn.megacorpone.com
   — webmail.megacorpone.com
   — www.megacorpone.com
   — www2.megacorpone.com

3.2.3 Informations sur le serveur WEB et les serveurs DNS

1. Hébergeur :
   — OVH
2. Pays d'hébergement du site web :
   — Montréal, Québec, Canada
3. Adresse IP publique du site web :
   — 149.56.244.87
4. Changement d'hébergement du site web :
   — Le site web n'a pas changé d'hébergement. Le statut du transfert de client est sur "interdit" (clientTransferProhibited).
5. Operating system du site web : Debian 10
6. Technologie du web server : apache/2.4.38
7. Vulnérabilités connues pour la version du web server :
   — CVE-2018-17189 : DoS for HTTP/2 connections via slow request bodies (low)
   — CVE-2018-17199 : mod_session_cookie does not respect expiry time (low)
   — CVE-2019-0190 : mod_ssl 2.4.37 remote DoS when used with OpenSSL 1.1.1 (important)
8. Technologies web utilisées : PHP/7.3.29-1
9. Name servers de la société :

- ns1.megacorpone.com
- ns2.megacorpone.com
- ns3.megacorpone.com

3.2.4 Informations sensibles

1. Hash du mot de passe de l'utilisateur trivera, trouvé sur le github de l'entreprise :
   - hash : `trivera:$apr1$A0vSKwao$GV3sgGAj53j.c3GkS4oUC0`
   - commande utilisée pour trouver le mot de passe à partir du hash : `john --wordlist=rockyou.txt hash.txt`
   - résultat : `trivera:Tanya4life`
2. Informations sur l'utilisateur William Adler : Nous supposons qu'il pourrait s'agir des identifiants de l'utilisateur pouvant lui servir à accéder à l'un des services interne de l'entreprise.
   - Nom d'utilisateur : Wadler
   - Mot de passe : TwitterStar2
   - Informations trouvées sur le twitter de l'employé William Adler

3.2.5 Autres informations

1. Adresse de l'entreprise : 2 Old Mill St, 89001 Rachel, Nevada US.
2. Numéro de téléphone : +1.9038836342.
3. Adresses mail des différents départements :
   - département des ressources humaines (Human Resources) : `hr@megacorpone.com`,
   - département commercial (Sales) : `sales@megacorpone.com`,
   - département logistique (Shipping) : `shipping@megacorpone.com`.
4. Réseaux sociaux de l'entreprise :
   - facebook (contenu indisponible) : `https://www.facebook.com/MegaCorp-One-393570024393695/`
   - linkedin (contenu indisponible) : `https://www.linkedin.com/company/18268898/`
   - github : `https://github.com/megacorpone`
5. Format d'adresses mails de la société :
   - Employés : 1ère lettre du prénom + nom de famille + @megacorpone.com
   - Département : Initiales ou nom complet du département + @megacorpone.com
   - PDG : Prénom + @megacorpone.com
6. Page web non référencée : `https://www.megacorpone.com/nanites.php`
7. Page web anciennement référencées :
   - `http://www.megacorpone.com/jobs2.html`
   - `https://cp.megacorpone.net/`

3.3 Scanning et énumération

Le scanning et l'énumération est la deuxième étape du pentest, elle s'inscrit dans la continuité de l'étape de reconnaissance parce qu'elle continue la recherche d'informations sur l'entreprise mais avec une différence majeure : l'utilisation d'outils de scanning automatisés. L'objectif est de trouver un maximum d'informations sur les services informatiques de l'entreprise accessibles depuis l'extérieur. Par exemple, nous avons scanné le site web de MegaCorpOne pour trouver des pages intéressantes comme une partie du site réservée aux administrateurs.

3.3.1 Identification des adresses IP d'intérêt

3.3.2 Scan du réseau

3.3.3 Nmap - TCP scanning

3.3.4 Nmap - UDP scanning

3.3.5 OS Fingerprinting

résultats :
- 10.180.30.10 : Linux 3.2 - 4.9
- 10.180.30.15 : Linux 4.15 - 5.6
- 10.180.30.254 : Linux 4.15 - 5.6
- 10.180.20.1 : Microsoft Windows Server 2016
- 10.180.20.2 : Microsoft Windows Server 2003 SP1 or SP2, Microsoft Windows Server 2003 SP2, Microsoft Windows Server 2008 Enterprise SP2
- 10.180.20.3 : Microsoft Windows 10 1709 - 1909
- 10.180.20.11 : Linux 4.15 - 5.6
- 10.180.20.254 : Linux 4.15 - 5.6

3.3.6 Énumeration SNMP

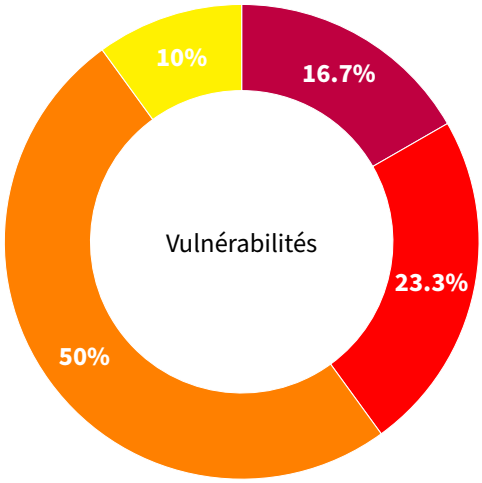
3.3.7 Énumeration WEB

3.3.8 Énumeration Wordpress

3.4 Analyse de vulnérabilités

3.4.1 Types de vulnérabilités

Voici les différents types de vulnérabilités trouvés, on remarque que les scores les plus élevés comme Critical, High et Medium sont présents en grand nombre.



• CRITICAL • HIGH • MEDIUM • LOW

3.4.2 Hôte - 10.180.20.1

...

3.4.3 Hôte - 10.180.20.2

...

3.5 Exploitation

3.5.1 Accès au réseau Wi-fi

...

3.5.2 Service SSH

...

3.5.3 ...

3.6 Élévation de privilèges

...

3.7 Mouvement latéral

...

3.8 Recommandations de sécurité

1. ...

4 Conclusion

...

A Annexes

...

Table des figures

Références