Préparation a la certification OSCP

Gauvain Roussel-Tarbouriech

Plan/déroulé du cours

Pourquoi l'OSCP

- Certification de relativement bon niveau

Pourquoi l'OSCP

- Certification de relativement bon niveau
- La certification la plus connue d'Offensive Security (les créateurs de Kali Linux)

Pourquoi l'OSCP

- Certification de relativement bon niveau
- La certification la plus connue d'Offensive Security (les créateurs de Kali Linux)
- Pas une cert "bullshit" a la CISSP, CEH

Pourquoi l'OSCP

- Certification de relativement bon niveau
- La certification la plus connue d'Offensive Security (les créateurs de Kali Linux)
- Pas une cert "bullshit" a la CISSP, CEH
- Introduit pas mal de concepts vu et revu dans le monde réel

Pourquoi l'OSCP

- Certification de relativement bon niveau
- La certification la plus connue d'Offensive Security (les créateurs de Kali Linux)
- Pas une cert "bullshit" a la CISSP, CEH
- Introduit pas mal de concepts vu et revu dans le monde réel
- Problème

Exemples

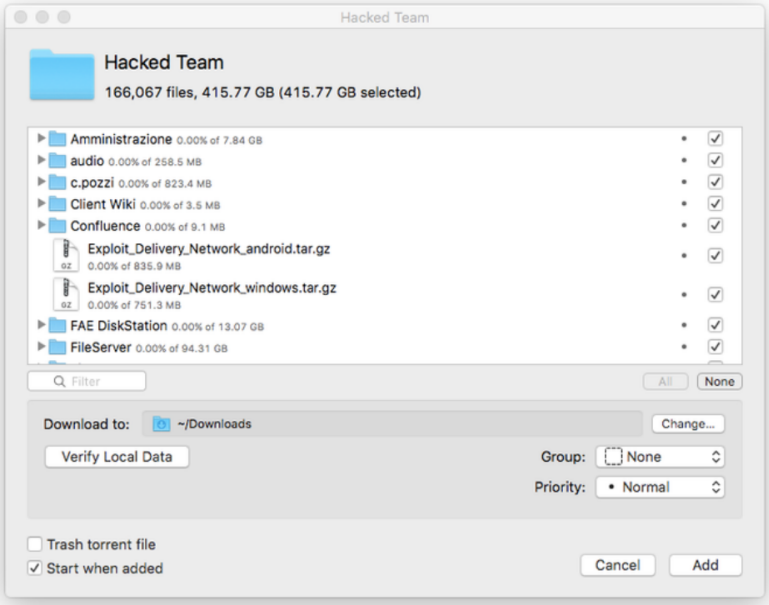
Hacking Team piraté – 400 GB de données dans la nature

@KORBEN — 6 JUILLET 2015

Mise au même rang que Blue Coat, Amesys, Gamma International et Trovicor, la société italienne **Hacking Team** a été classé comme ennemi d'Internet.

Ces derniers vendent à leurs clients une solution de surveillance à distance baptisée Remote Control Systems (RCS) incluant les outils DaVinci et Galileo qui permettent, en autres, de collecter des infos sensibles (emails, historiques d'appels, carnet d'adresses..etc.), les touches tapées au clavier (keylog), de prendre des captures-écran, récupérer l'historique des recherches web, suivre le GPS du téléphone, enregistrer l'audio des appels téléphoniques, activer la caméra du téléphone ou de l'ordinateur, activer le micro de l'ordinateur ou du téléphone pour enregistrer les bruits ambiants ou les conversations...etc etc.

Bref, un beau joujou pour les gouvernements. Seulement, voilà... La société Hacking Team vient de se faire poutrer, se faisant dérober un peu moins de 400 Gb de données sensibles comme des contrats, des factures et de la doc.



Exemples

[BREAKING] Nintendo's Old Files Have Been Stolen; That's Why There's Super Mario 64, Says Report

Tech Times | 05-05

A Nintendo massive breach had happened over the weekend. Over 2TB of old files of the said company have been leaked, according to a report. Interestingly, a day after the said breach, a fan-made port of Super Mario 64 running at 4K resolution on PC was released-- rising the speculations of whether the info came from the said breach.

Exemples

- Bon, vous avez compris l'idée

Objectifs

- Savoir analyser l'infrastructure d'un réseau, trouver les points faibles.

Objectifs

- Savoir analyser l'infrastructure d'un réseau, trouver les points faibles.
- Savoir faire du pentest web afin d'avoir une porte d'entrée plausible sur des serveurs.

Objectifs

- Savoir analyser l'infrastructure d'un réseau, trouver les points faibles.
- Savoir faire du pentest web afin d'avoir une porte d'entrée plausible sur des serveurs.
- Savoir faire de l'énumération afin de pouvoir faire une Elévation de privilèges.

Objectifs

- Savoir analyser l'infrastructure d'un réseau, trouver les points faibles.
- Savoir faire du pentest web afin d'avoir une porte d'entrée plausible sur des serveurs.
- Savoir faire de l'énumération afin de pouvoir faire une Elévation de privilèges.
- Comprendre les configurations des AD et trouver les problèmes potentiels.

Objectifs

- Savoir analyser l'infrastructure d'un réseau, trouver les points faibles.
- Savoir faire du pentest web afin d'avoir une porte d'entrée plausible sur des serveurs.
- Savoir faire de l'énumération afin de pouvoir faire une Elévation de privilèges.
- Comprendre les configurations des AD et trouver les problèmes potentiels.
- Savoir exfiltrer des données sans laisser trop de traces.

Objectifs

- En sécurité on a 3 “principaux” domaines: l’exploit, le pentest et la défense.

Objectifs

- En sécurité on a 3 “principaux” domaines: l’exploit, le pentest et la défense.
- L’exploit c’est trouver des bugs dans des programmes, eg des CVEs.

Objectifs

- En sécurité on a 3 “principaux” domaines: l’exploit, le pentest et la défense.
- L’exploit c’est trouver des bugs dans des programmes, eg des CVEs.
- Le pentest c’est trouver des erreurs d’organisation dans des infras.

Objectifs

- En sécurité on a 3 “principaux” domaines: l’exploit, le pentest et la défense.
- L’exploit c’est trouver des bugs dans des programmes, eg des CVEs.
- Le pentest c’est trouver des erreurs d’organisation dans des infras.
- La défense c’est un peu un fourre tout dans ce cas la, en gros éviter les erreurs d’orgas et/ou de bugs[1] en amont ou sur le tas

[1] https://rust-lang.org/

Objectifs

- En sécurité on a 3 “principaux” domaines: l’exploit, le pentest et la défense.
- L’exploit c’est trouver des bugs dans des programmes, eg des CVEs.
- Le pentest c’est trouver des erreurs d’organisation dans des infras.
- La défense c’est un peu un fourre tout dans ce cas la, en gros éviter les erreurs d’orgas et/ou de bugs[1] en amont ou sur le tas
- Ici on s’intéresse au pentest.

[1] https://rust-lang.org/

Modalités de notation

- Un serveur a infiltrer avec un rapport a rendre pendant les dernières heures de cours.

Matériel nécessaire

- Préférable: Une VM Kali Linux afin d'éviter les temps de compilations des inévitables gentoo-istes.

Matériel nécessaire

- Préférable: Une VM Kali Linux afin d'éviter les temps de compilations des inévitables gentoo-istes.
- Agréable: un OS avec un noyau Linux [2]

[2] Non, WSL1, ça compte pas trop :P. WSL2 ça peut avoir ses bugs.

Matériel nécessaire

- Préférable: Une VM Kali Linux afin d'éviter les temps de compilations des inévitables gentoo-istes.
- Agréable: un OS avec un noyau Linux [2]
- En vrac: `nmap`, `owasp-zap`/`Burp Suite`, `firefox`, `gobuster`/`dirsearch`, `BlueHound`, `sqlmap`,`hashcat` et plus encore.

[2] Non, WSL1, ça compte pas trop :P. WSL2 ça peut avoir ses bugs.

Où trouver les ressources ?

- Le discord du cours, que je vais de ce pas vous donner.

Où trouver les ressources ?

- Le discord du cours, que je vais de ce pas vous donner.
- Le lien du cours pour toutes les slides/ressources qu'on a vu en cours: https://code.govanify.com/govanify/esgi-oscp.

Où trouver les ressources ?

- Le discord du cours, que je vais de ce pas vous donner.
- Le lien du cours pour toutes les slides/ressources qu'on a vu en cours: https://code.govanify.com/govanify/esgi-oscp.
- Les listes awesome ctf/security sur GitHub et lire beaucoup de writeups :D

Plan du cours

- Introduction au Pentest web

Plan du cours

- Introduction au Pentest web
- Introduction a l'exploit binaire/reverse et au reverse engineering[3]

[3] https://code.govanify.com/govanify/esgi-re/

Plan du cours

- Introduction au Pentest web
- Introduction a l'exploit binaire/reverse et au reverse engineering[3]
- Introduction a l'Elevation de privilèges et a la configurations de serveurs + AD

[3] https://code.govanify.com/govanify/esgi-re/

Plan du cours

- Introduction au Pentest web
- Introduction a l'exploit binaire/reverse et au reverse engineering[3]
- Introduction a l'Elevation de privilèges et a la configurations de serveurs + AD
- Beaucoup de pratique :)

[3] https://code.govanify.com/govanify/esgi-re/

Le Pentest web

Le Pentest web

Le