RINGOET ANTHONY

2022

C'EST QUI ? C2 !

QU'EST-CE QUE C2 ?

FRAMEWORK C2

C2 vient de son abréviation de C&C qui veut dire Command and Control, ces Frameworks sont souvent utilisés par les Red Teamer et Pentesters comme de solides outils et ainsi contrôler les machines compromises lors des audits de sécurité.

Il en existe énormément et la liste est non-exhaustive, ils sont souvent utilisés lors de la post-exploitation.

Les Frameworks sont choisis en fonction du niveau de la technique qu'on utilisera pour pivoter entre plusieurs machines selon le réseau, la structure et les sécurités utilisés par l'entreprise.

LISTES DES FRAMEWORK C2

- Cobaltstrike
- Covenant
- Sillent trinity
- Koadic
- Merlin
- Metasploit

FRAMEWORK COBALTSTRIKE

Cobaltstrike est celui qui est plus souvent utilisé sur les plateformes du monde entier, il permet un déploiement de fonctionnalités intéressantes.

- Keylogging
- Upload et Download de fichiers
- Socks Proxy
- Déploiement de VPN
- Escalation de privilège
- L'utilisation de Mimikatz
- Etc...

Il prend en charge les protocoles HTTP, HTTPS, DNS et SMB.
De plus, il est fourni d'une boîte à outils de développement avec son kit d'artefact qui aide lors de la mise en code sur la personnalisation du Shell.

FRAMEWORK COVENANT

Covenant est un Framework qui est utilisé lors des post-exploitations, celui-ci est pris en charge sur plusieurs plateformes ASP.NET ainsi que tous les systèmes d'exploitation, il est également fourni avec une image de Docker qui est déjà préconfigurée pour aider à l'installation.

- Les scripts d'exfiltration
- Indicateurs de suivi
- Compilation dynamique
- Échange de clés chiffrées
- Escalation de privilège latéral
- L'utilisation de Mimikatz
- Etc...

Covenant a été développé en C# et peut être personnalisé directement via une interface web qui permet une gestion aisée pour les multi-utilisateurs.

FRAMEWORK SILLENT TRINITY

Sillent trinity est un Framework de commandes et de contrôles asynchrones, il prend en charge l'aboutissement de nombreuses recherches sur les langages de scripts .NET tiers intégrés pour faire appel dynamiquement aux API.

- Entièrement modulaire
- Compilation dynamique
- Mises à jour et communications en temps réel
- CLI moderne et convivial
- Journalisation étendue
- Etc...

Sillent trinity est développé en python3 et .NET DLR (Dynamic Language Runtime) qui permet de prendre en charge plusieurs langages, permet l'utilisation d'échanges via un canal sécurisé avec une paire de clés publique-privé.

FRAMEWORK KOADIC

Koadic est un Framework de post-exploitation Windows qui utilise Windows Script Host (JScript/VBScript) et prend en charge les versions de Windows ceux-ci vont de Windows 2000 à Windows 11.

- Augmente l'intégrité (UAC Bypass)
- L'utilisation de Zombie
- Dumps les fichiers SAM/SECURITY
- Analyse le réseau (PORT SMB)
- Possibilité de pivoté
- Etc...

Koadic est un Framework créé en python pratique et utile qui est basé sur JavaScript avec un chiffrement XOR, celui-ci s'installe sur les machines cibles à l'aide du MsHTA (Microsoft HTML Application).

FRAMEWORK MERLIN

Merlin est un Framework très utile, celui-ci se chargera de mettre ses capacités à éviter la détection d'antivirus, il utilise une architecture client-serveur et il est fourni avec plusieurs fonctionnalités les plus connues et avancées dans le Red Teaming.

- JWT (Jason Web Token) chiffrer
- Divers Shellcode d'exécution
- Modifier dynamiquement le Hash
- Domain Fronting
- OPAQUE (l'échange de clés d'authentification)
- Etc...

Ce Framework communique sur le (TLS = la couche session), pour maintenir chiffré le contenu du trafics des messages JSON en texte brute entre le client et le serveur, celui-ci présente des obstacles lorsqu'il y a des Proxys.

FRAMEWORK METASPLOIT

Metasploit est un outil pour le développement et l'exécution d'exploits contre une machine distante, il permet de réaliser des audits en sécurité, de tester et développer ses propres exploits. Créé à l'origine en langage de programmation Perl, le Framework Metasploit a été complètement réécrit en langage Ruby

- Exploitation des vulnérabilités
- Banque de Modules (payloads, exploit,...)
- Escalade de privilèges
- Suppression des logs et des traces
- Fuzzing
- Etc...

Celui-ci améliore la sensibilisation à la sécurité, il permet de donner de solides armes aux personnes qui défendent leurs infrastructures tout en gardant une longueur d'avance sur les éventuelles attaques qui pourraient se produire.

MERCI !

https://github.com/tcostam/awesome-command-control

https://www.cobaltstrike.com/

https://www.orangecyberdefense.com/fr/insights/blog/ethical-hacking/focus-sur-le-domain-fronting