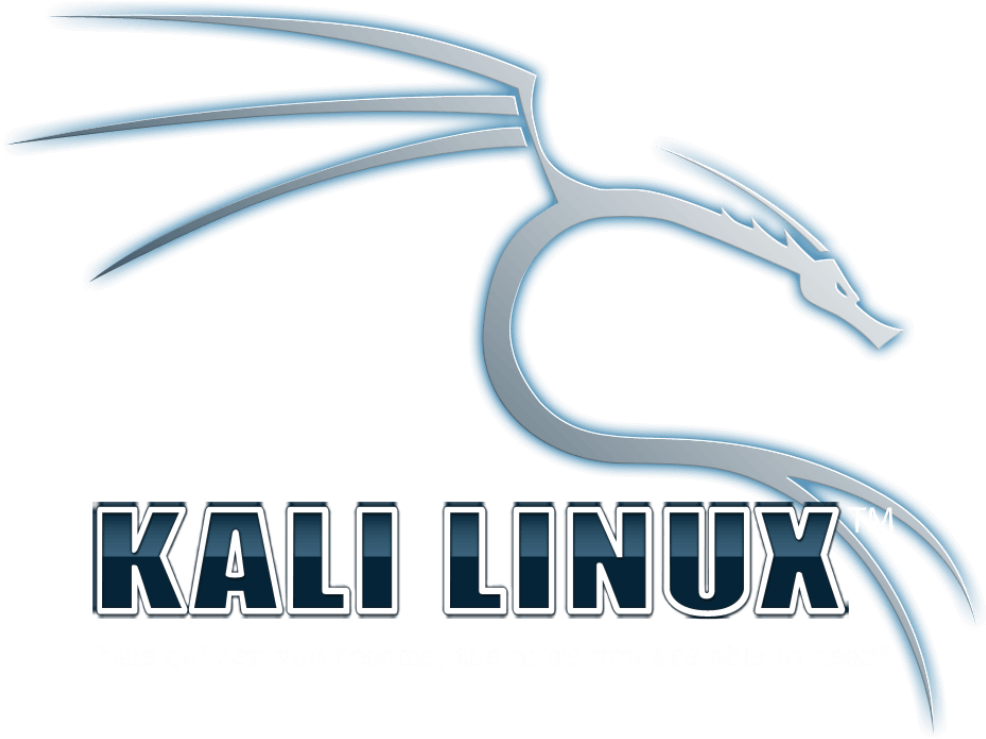
3 FEBRUARI 2020



PENTEST HANDLEIDING

Versiebeheer

Datum	Versie	Auteur	Aanpassingen
16/10/2019	0.1 Concept	Sander Meijering	Document aangemaakt en hoofdstukken bijgewerkt.
21/10/2019	0.2 Concept	Sander Meijering	Target Discovery & Enumeratie
07/11/2019	0.3 Concept	Sander Meijering	Methodiek aangepast.
25/11/2019	0.4 Concept	Sander Meijering	Web Application
16/12/2019	0.5 Concept	Sander Meijering	Alle hoofdstukken.
06/01/2020	0.6 Concept	Sander Meijering	Alle hoofdstukken.
23/01/2020	0.7 Concept	Sander Meijering	Alle hoofdstukken.
03/02/2020	1.0 Final	Sander Meijering	Alle hoofdstukken.

To-Do list

1. Social Engineering tools en technieken verifiëren bij een SE-opdracht.
2. Verificatie van wachtwoord kraken tools en technieken.
3. Verificatie van exploitatie tools en technieken.
4. Verificatie Na-exploitatie tools en technieken. (Linux)
5. Toevoegen Na-exploitatie tools en technieken. (Windows)
6. Verificatie Webapplicatie tools en technieken.
7. Netwerk pentest volledig onderzoeken. (Zowel draadloos als lokaal netwerk)
8. DOS (stress-testing) tools en technieken.
9. Buffer overflow tools en technieken.
10. Responder (Poisoner)

Inleiding

Dit document is een handleiding voor de beginfases van het pentestproces en kan gebruikt worden als hulpmiddel bij latere fases van het pentestproces. Dit document moet gezien worden als handvat voor het pentestproces en **niet** als een verplichte handleiding. Document dient als hulpmiddel en ter verificatie.

De handleiding heeft voornamelijk betrekking op het extern testen van systemen, zoals OSINT (Informatie verzamelen) en het scannen van open poorten tot het openbare web. Daarnaast zijn er veel websites die betrekking hebben op Nederlandse bedrijven, waaronder Nederlandse vacature websites en de kamer van koophandel.

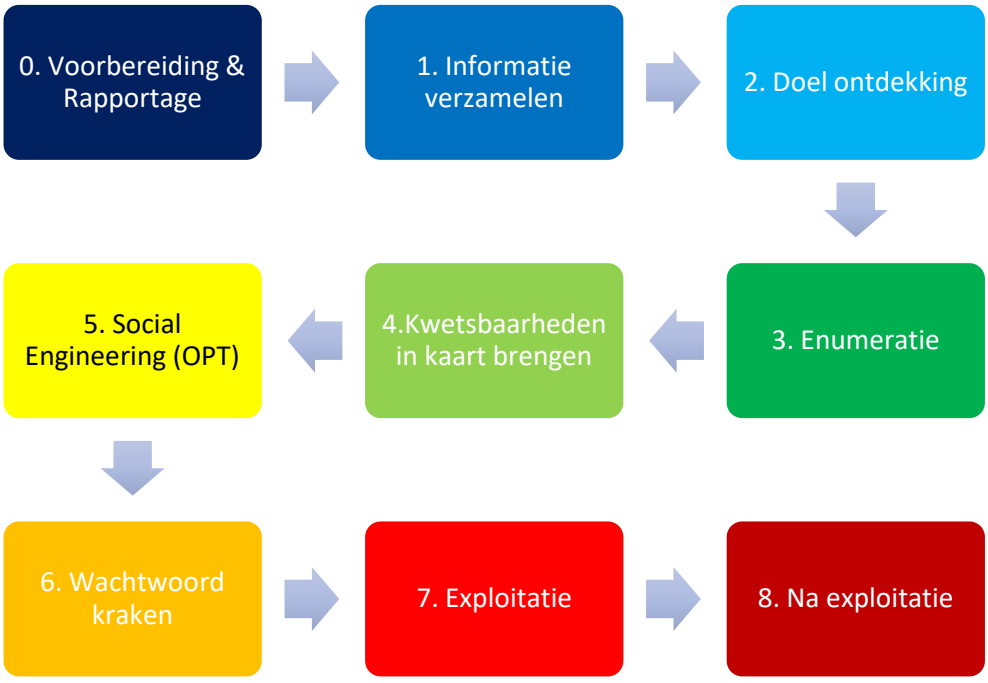
De tools die in deze handleiding terug te vinden zijn, kunnen voornamelijk teruggevonden worden in het besturingssysteem: Kali Linux. Aan het eind van dit document staat een lijst van tools, die zelf geïnstalleerd moeten worden.

Dit document is volledig ter beschikking gezet naar de buiten wereld. Het document blijft bijgewerkt worden en kan teruggevonden worden op de volgende GitHub repository: https://github.com/sanderie10/PentestHandleiding. Voor vragen, discussies en inbreng, neem contact op via email: sander.meijering@hotmail.com

Pentestmethodiek

De auteur heeft onderzoek gedaan naar verschillende pentestmethodieken/ technische handleidingen, waaronder: PTES, OSSTMM, ISSAF, PTF en OWASP OTG.

Onderstaand methodiek is gebaseerd op ervaring van de auteur en onderzoek naar voorgaand genoemde methodieken/ technische handleidingen.



OPT = Optioneel

Elke fase is opgedeeld in verschillende technieken met bijhorende tools en/of websites. De command prompt tools hebben een basis configuratie waarbij alleen de rode tekst gewijzigd moet worden.

Inhoud

Termen en overige informatie

Penetratietester, tester of team	De persoon (personen) die de penetratietest voor entiteit uitvoert. Ze kunnen een internet of externe hulpbron zijn.
Penetratietest, Pentest	Handmatige controle waarbij men zo diep mogelijk wil binnendringen in een systeem om zwakke plekken te vinden en de gevolgen hiervan te kennen. Men gebruikt de zwakke plekken om nog wat dieper in het systeem te komen.
Vulnerability scan	Handmatige controle waarbij men zwakke plekken in een systeem opspoort. Men bepaalt vooraf hoe men dat doet. Bij een vulnerability assessment probeert men alle zwakke plekken te vinden in een klein gebied.

Richtlijnen

ISO/IEC 27001(2) (Informatiebeveiliging)
NEN 7510 (Informatiebeveiliging – zorgsector)

Certificaten

Certified Professional **(OSCP)**	Offensive Security
Certified Expert **(OSCE)**	Offensive Security
Webapplicatie Expert **(OSWE)**	Offensive Security
Licensed Penetration Tester **(LPT)**	EC-Council
Certified Ethical Hacker **(CEH)**	EC-Counsil
Certified Penetration Tester **(CPT)**	IACRB
Certified Expert Penetration Tester **(CEPT)**	IACRB
Certified Mobile and Web Application Penetration Tester **(CMWAPT)**	IACRB
Certified Red Team Operations Professional **(CRTOP)**	IACRB
Pentest+	CompTIA
Penetration Tester **(GPEN)**	GIAC
Exploit Researcher and Advanced Penetration Tester **(GXPN)**	GIAC

0. Voorbereiding

0.1. Bedrijf

Het doel van deze fase is om in overleg met het doelbedrijf de scope van het project te zetten en een testplan te maken.

Soort pentest
Keuze uit:

- White-Box
    - Het testteam heeft volledige carte blanche toegang tot het testnetwerk en is voorzien van netwerkdiagrammen, hardware, besturingssysteem en applicatiegegevens. Dit staat niet gelijk aan echt blinde test, maar kan het proces veel versnellen en leidt tot nauwkeuriger resultaat.
- Black-Box
    - Voorkennis van een bedrijfsnetwerk is niet bekend. Het testteam krijgt alleen IP-adressen en domeinnamen toegekend. Een Black-Box test komt het meest overeen met een externe aanval door een kwaadwillende hacker.
- Grey-Box
    - Het testteam zou worden voorzien van de juiste rechten op gebruikersniveau en een gebruikersaccount en toegang tot het internetnetwerk door versoepeling van specifiek beveiligingsbeleid op het netwerk (Beveiliging op poortniveau).

Doel van pentest
Identificeren van risico's die een negatieve impact hebben op de organisatie. Enkel kwetsbaarheden vinden (Vulnerability Assessment). Het controleren op niet-gepatchte systemen en de mogelijkheid voor detectie en reactie op verschillende vectoren van de pentest.

Communicatie
Op welke manier wordt er gecommuniceerd met de klant of derde partij. Contactpersoon voor noodgevallen. Statusbijeenkomsten: bespreken van planningen, voortgang en problemen.

Scoping van het doel
Welke interne IP-adressen, externe IP-adressen, netwerk bereiken en domeinnamen moet worden getest. Valideer of de opgegeven doeleinden daadwerkelijk in bezit zijn van het bedrijf. Bij het pentesten van software/hardware dat gehost wordt door derde partijen (Clouddiensten, ISP, MSSPs), moeten er eerste goedkeuring van deze bedrijven gevraagd worden. Waar staat de hardware? Andere landen betekent andere wetten.

Tijdschatting
Begin- en einddatum van de pentest en op welke tijden wordt er getest. Binnen/buiten werktijden, Weekend/ doordeweeks. Het maken van een planning/tijdlijn (GANTT-Grafiek).

Beveiliging
Is er een Firewall, IDS/IPS of Load Balancer aanwezig? Is er een incident response team aanwezig en op welke tijden. Incident-responsemogelijkheden worden ook getest. Volwassenheidsniveau van de beveiliging bepalen.

Na exploitatie
Wat wordt er gedaan, wanneer er exploitatie gelukt is. Zover doorgaan als mogelijk of zoeken naar andere mogelijkheden voor exploitatie.

Uitsluitingen (Social-Engineering, Denial of Service)
Mag er Social Engineering gedaan worden en hoe groot is deze scope. Alle werknemers of alleen een gericht aantal personen? (CEO, Risico Manager, Systeem Manager, Data-eigenaren, Security Officer, ISP) Mogen er DoS-aanvallen plaatsvinden? Zo ja wat is hiervan de scope? Welke machines mogen hoe dan ook niet buiten dienst komen te liggen? Welke machines zijn vrijstellingen van de test? Overige uitsluitingen?

Documentatie
PGP-technieken voor encryptie van documenten en bestanden. Wat voor documenten/ producten worden verwacht. TLP (Trafic Light Protocol), voor wie zijn de documenten zichtbaar?

Betaalvoorwaarden
Op welke manier wordt er betaalt? Helft vooraf, helft achteraf. Doorgaans betaald (handig voor lange pentest).

Handtekening
Ondertekenen van goedkeuring voor het pentesten van zowel het doelbedrijf als derde partijen. Ondertekenen van geheimhoudingsverklaringen. Geheimhoudingsverklaring kan volledig, beperkt of geen zijn:

- **Volledig:** Alle informatie met betrekking tot deze taak kan niet worden verspreid/ gebruikt voor onderzoek, training, marketing etc.
- **Beperkt:** Bepaald informatie kan worden gebruikt in marketing/ training en onderzoek scenario's nadat de overeenkomst is gesorteerd van de klant.
- **Geen:** Alle informatie is vrij verspreid en niet onder enige beperking.

0.2. Pentest team
Dit is ter voorbereiding voor de leden van het pentest team.

Aanmaken logboek
Het maken van een logboek, waarin minimaal de volgende delen genoemd worden per actie. Datum, Tijd, Locatie, IP-adres, Fase, Actie, Commando, Tool/Website en Resultaat.

Aanmaken onderzoekomgeving
Het gebruik maken van virtuele omgevingen zoals: Oracle VirtualBox of VMware Workstaiton. Gebruik maken van aparte computer of VPS. Ook nagedacht wat voor OS geïnstalleerd wordt op deze machines. (Vaak Kali Linux)

VPN, Proxy, Tor gebruik (Black-Box of Grey-Box)
Het aanschaffen van een VPN om zo met verschillende IP-adressen te kunnen testen. Of het gebruik maken van Proxies en/of Tor.

Installatie/ Setup van bruikbare tools
Installatie en/of setup van tools die nog niet geïnstalleerd of geconfigureerd zijn op het operating system. Logtools: Faraday en Dradis.

Installatie FireFox Add-ons
Installeer de volgende add-ons op Mozilla FireFox: FireShot (Web-pagina screenshotter), LocaProxy Toolbar (Proxy beheerdeer), Wappalyzer (Website technologie).

API-Keys aanvragen

Veel tools kunnen gebruik maken van API-Keys om de tools te optimaliseren. Maak vooraf accounts op onderstaande websites en schrijf de API-key ergens op. Deze API-keys kunnen gebruikt worden bij tools zoals: Maltego en SpiderFoot.

Have I Been Pwned	https://haveibeenpwned.com/API/Key (3.50 per maand)
De Hashed	https://dehashed.com/api (3 cent per API)
Shodan	https://account.shodan.io/
Censys	https://censys.io/account/api
Hunter	https://hunter.io/api_keys
VirusTotal	https://www.virustotal.com/gui/sign-in
Ipinfo	https://ipinfo.io/account
Spyce	https://spyse.com/account/user#c-domain__anchor--2
We Leak Info	Domain Seized
BuiltWith	https://api.builtwith.com/
Pastebin.com	https://pastebin.com/api

1. Informatie verzamelen

In deze fase wordt er zoveel mogelijk informatie verzameld over het bedrijf/organisatie. De informatie kan worden gebruikt bij het binnendringen van het doelwit. Hoe meer informatie er in deze fase wordt verzameld, hoe meer aanvalsvectoren er in de toekomst gebruikt kunnen worden.

Er zijn twee vormen van informatie verzamelen: actief en passief. Passief verzamelen van informatie is het binnen halen van data zonder dat het doelbedrijf weet dat die onderzocht wordt. Er wordt op geen enkel manier netwerkverkeer verstuurd naar het doelbedrijf dat niet vergeleken kan worden met normaal internetverkeer en -gedrag. Bij actief verzamelen van informatie wordt er juist netwerkverkeer verstuurd naar het doelbedrijf om zoveel mogelijk informatie te verzamelen. Het nadeel van actief is dat het opgevangen kan worden door beveiliging systemen en daardoor het IP-adres kan blokkeren.

1.1. Website/Domein

Eerst wordt er gekeken of het bedrijf een website in bezit heeft. Van deze website wordt zoveel mogelijk informatie verzameld en onderzocht.

Whois, ARIN & DNS-informatie (Passief)

Via de whois-informatie kan er naar voren komen wie de website host. Via DNS-informatie kan er onder andere naar voren komen op welk IP-adres de website draait en in welk IP-bereik zich bevindt. DNS-informatie is opgedeeld in verschillende records, waaronder:

1. SOA = Geeft de server aan die bevoegd is voor het domein.
2. MX = Lijst met de server voor e-mail uitwisselaars van een host of domein.
3. NS = Lijst met de naamserver van een host of domein.
4. A = Een adresrecord waarmee een computernaam kan worden vertaald naar een IP-adres.
5. PTR = Toont de domeinnaam van een host, host geïdentificeerd door zijn IP-adres. (IP-adres)
6. SRV = Service-locatierecord.
7. HINFO = Hostinformatierecord met CPU-type en besturingssysteem.
8. TXT = Algemeen tekstrecord.
9. CNAME = Laat aliassen en bijnamen zien.
10. RP = Verantwoordelijke persoon voor het domein.
11. SPF = Welke servers namen de domeinnaam e-mail mogen verzenden.
12. DMARC = Wordt gebruikt spoofing van e-mail te detecteren en tegen te gaan.
13. ARIN = ARIN & RIPE Database check (IP-adres).

Tools/websites:

1. *Website:* http://whois.domaintools.com/
    a. Haalt het domein whois-record op en vertelt op welk IP-adres de website wordt gehost on of er meerdere websites op hetzelfde IP-adressen worden gehost.
1. *Website:* https://mxtoolbox.com/SuperTool.aspx
    a. Kan alle DNS-informatie ophalen van zowel websites als IP-adressen.
2. *dnsrecon -d* example.com *-agbkz*
    a. Haalt alle mogelijke DNS-informatie op.

Technologie (Passief/ Actief)
Via de technologie informatie kan er naar voren komen op welke services de website draait en welke CMS/ plug-ins gebruikt worden.

Tools/websites:

1. *Website:* https://builtwith.com/
2. *Website:* https://w3techs.com/sites
3. *Browser-extensie:* https://www.wappalyzer.com/download
4. *whatweb -v* example.com

Bovenstaande tools/websites geven allemaal een lijst van technologie dat gebruikt wordt op de website. De websites en browser extensie zijn passief, maar de tool whatweb kan actief gebruikt worden.

Web Application Firewall (WAF) & Load Balancer
Een WAF is een firewall voor HTTP-applicaties. Een WAF kan aanvallen zoals XSS en SQL-injecties tegenhouden en het IP blokkeren. Een WAF kan door wafw00f gedetecteerd worden. Daarnaast is een load balancer een techniek om het netwerkverkeer te verspreiden over verschillende computers. Een load balancer kan door lbd gedetecteerd worden.

- *wafw00f* https://example.com
- *lbd* example.com

Bestanden & Metadata (Passief)
Bestanden op websites zijn ook erg nuttig om mee te nemen in het onderzoek. Vanuit deze bestanden kan er vaak metadata gehaald worden.

Tools/websites:

1. *Metagoofil -d* example.com *-t pdf,dox,xls,ppt,odp,ods,docx,xlsx,pptx -o /Desktop/Files -f Report.html*
    a. Metagoofil zoekt via Google naar bestanden en extract direct de metadata ervan af.
2. *FOCA (GUI)*
    a. FOCA zoekt op verschillende zoekmachines naar bestanden en extract direct de metadata ervan af.
3. *Website:* https://www.google.com/search?q=site:example.com+ext:pdf+|+ext:docx
    a. Google Hacking techniek.

Om metadata van de bestanden eruit te filteren, kunnen er verschillende tools gebruikt worden m.b.t het filetype:

1. *pdfinfo* Bestand.pdf (Kan alleen pdf)
2. *exiftool* Bestand.jpg (Kan meerdere extensies)
3. *Website:* https://www.get-metadata.com/ (Let op privacy)
4. *Website:* http://metapicz.com/#landing (Let op privacy)

Wayback Machine (Passief)
Via archive.org kunnen er oude screenshots die zijn gemaakt van de website terug worden gevonden.

Website: https://archive.org/web/

Website analyse (Passief)
De volgende tools kunnen automatisch geanalyseerd worden door verschillende websites. Deze websites kijken naar security headers en bijvoorbeeld het gebruik van HTTPS

Websites:

1. *Website:* https://securityheaders.com/ (Security headers)
2. *Website:* https://urlscan.io/ (Domein & IP)
3. *Website:* https://internet.nl/ (IPv6, DNSSEC, HTTPS & Security headers)

Securityheaders en internet geven een rapport met alle resultaten en bijhorende cijfer, hoe goed de website is beveiligd op de gevonden punten. Urlscan geeft andere informatie weer zoals redirects etc.

Sub domeinen (Passief/ Actief)
Sub domeinen zijn vaak verborgen in de website en kunnen vaak belangrijke informatie bevatten of de scope verbreden.

Websites:

1. *Website:* https://spyse.com/search/subdomain
2. *Website:* https://dnsdumpster.com/
3. *Website:* https://mxtoolbox.com/SuperTool.aspx?action=axfr:example.com
4. *amass enum -d* example.com

Bovenstaand websites kijken in databases of er sub domeinen bekend zijn van een bepaald domein. Amass haalt gegevens op van zoveel mogelijke websites en toont alle gevonden sub domeinen.

1. *dnsmap* example.com -w wordlist.txt (Brute Force)

dnsmap maakt gebruikt van brute force en verspreid daardoor meer netwerk verkeer dan normaal. Hierdoor valt dnsmap onder actief.

Directories (Actief)
Veel directories zijn net als sub-domeinen verborgen en kunnen dan ook cruciale informatie bevatten.

Tools/websites:

1. *dirb* example.com
    a. Maakt gebruik van ingebouwde wordlist en brute forced de opgegeven website.
2. *dirbuster*
    a. GUI-versie van dirb
3. *skipfish -YO* http://example.com
    a. Is een spider die alle mogelijke directories verzameld.

1.2. Bedrijf & werknemers

Na dat er technische informatie is binnengehaald over de website die het bedrijf in bezit heeft, wordt er overgegaan naar informatie over de werknemers en het bedrijf zelf.

Zoekmachines – Bedrijf (Passief)
Via Zoekmachines kan er genoeg informatie gevonden worden over het doelbedrijf. Daarnaast kan er veel informatie via nieuwsartikelen en de website zelf opgehaald worden.

Veel gebruikte zoekmachines:

- Google (cache: filetype: allintitle: allinurl: site: related:)
- dogpile

De volgende punten zijn relevant om mee te nemen:

- Bedrijfsdata (Locaties, Contactgegevens, KvK, Organogram)
- Relaties (Zakenpartners, Klanten, Concurrenten)
- Marketing, Liefdadigheidsacties
- Vacatures (LinkedIn, Jobbird.com, Werk.nl, Vacant.nl)
- Nieuws (Gerechtszaken)
- Professionele licenties (ISO/IEC 27001, NIST 800-115)
- How-To documenten (Op de website zelf)

Social Media (Passief)
Via Social Media kan er zowel informatie binnen gehaald worden over het bedrijf als over de werknemers van het bedrijf.

De volgende social mediawebsites worden het meest gebruikt:

1. *Website:* https://www.facebook.com/
2. *Website:* https://twitter.com/
3. *Website:* https://www.instagram.com
4. *Website:* https://www.youtube.com/
5. *Website:* https://nl.pinterest.com/
6. *Website:* https://www.linkedin.com

Bovenstaande websites maken gebruik van profielen. Via deze profielen kan er informatie binnen gehaald worden over het bedrijf of werknemer.

Foto's gepost op Social media kunnen ook metadata bevatten en onderzocht worden door de volgende tools/websites:

1. *Website:* https://www.get-metadata.com/
2. *Website:* http://metapicz.com/#landing
3. *exiftool Bestand.jpg*

De twee websites en tool kunnen de gebruikte camera, GPS-locatie en datum vinden van de foto's.

Email (Passief)
Het verzamelen van e-mailadressen van werknemers kan bruikbaar zijn voor het eventueel versturen van phishing mails. Daarnaast kunnen deze e-mails ook onderzocht worden op datelekken.

Tools/websites:

1. *theHarvester* -d example.com -l 500 -b all
    a. Zoekt via verschillende zoekmachines naar emailadressen van het opgegeven domein.
2. python *SimplyEmail*.py -all -e example.com
    a. Zoekt via verschillende websites naar emailadressen van het opgegeven domein.
3. *Website:* https://hunter.io/
    a. Zoekt ook via zoekmachines naar emailadressen van het opgegeven domein.
4. *Website:* https://haveibeenpwned.com/
    a. Bekijkt of het opgegeven emailadres in een datalek voorkomt.
5. *Website:* https://dehashed.com/
    a. Bekijkt of het opgegeven emailadres in een datalek voorkomt.
6. Website: https://intelx.io/
    a. Bekijkt of het opgegeven emailadres in een datalek voorkomt en kan ook het wachtwoord opzoeken.

Email headers
Bij het ontvangen van e-mails van werknemers van het bedrijf kunnen de headers van deze e-mails onderzocht worden. Uit de emailheaders kan het origineel IP-adres gehaald worden vanaf welk netwerk de email is verzonden.

1. *Website:* https://mxtoolbox.com/EmailHeaders.aspx
    a. Analyseert de volledige bron van de email en geeft alle data op een gestructureerde en leesbare wijze neer.

Telefoon/adressen (Passief)
Doormiddel van het telefoonboek kunnen er telefoonnummers en adressen verzameld worden via het opgeven van naam + achternaam.

Websites:

1. *Website:* https://www.telefoonboek.nl/
2. *Website:* https://www.detelefoongids.nl/personen/6-1/

All-In-One (Passief)
Er zijn ook tools die doormiddel van een GUI verschillende OSINT-informatie kunnen vinden voor de pentester. Het handige aan deze tools is dat ze mooi een grafische weergave van veel informatie kunnen weergeven. Daarnaast is het handig om te gebruiken als check-up/verificatie van voorgaande informatie. Door optimaal gebruik te maken van deze tools, is het best zoveel mogelijk API's toe te voegen, die in hoofdstuk 0 zijn beschreven.

SpiderFoot
SpiderFoot is een GUI die gebruikt kan worden om zoveel mogelijke informatie op te halen over IP-adressen, Domeinnamen, Emailadressen, namen en nog meer. SpiderFoot maakt gebruik van OSINT-tools waaronder; Shodan en HaveIBeenPwned.

1. python *sf*.py

Maltego
Maltego is een GUI, die voornamelijk gericht is op het vinden van relaties tussen bijvoorbeeld bedrijven, personen en websites. Maltego maakt ook gebruik van OSINT-tools en kan doormiddel van API's geoptimaliseerd worden.

1.3. IP-adres

IP-informatie (Passief)

Informatie over het IP-adres is ook relevant om mee te nemen, aangezien er met deze informatie gevalideerd kan worden of de IP-adressen daadwerkelijk van het doelbedrijf zijn.

Websites:

1. *Website:* https://ipinfo.io/
    a. Geeft zowel informatie als GEO-locatie van het IP-adres.
2. *Website:* https://mxtoolbox.com/SuperTool.aspx?action=arin:192.168.178.1
    a. Toont de informatie van de ARIN/RIPE database.
3. *Website:* https://check-host.net/ip-info
    a. Vergelijkt GEO-locatie van 3 websites: DB-IP, IP2Location en MaxMind GeoLite2

Reverse IP Lookup (Passief)

Bij een reverse IP lookup wordt er gekeken naar welke websites allemaal op hetzelfde IP-adres draaien. Onderstaand websites geven een lijst van domeinnamen.

Websites:

1. *Website:* https://hackertarget.com/reverse-ip-lookup/
2. *Website:* https://hostingchecker.com/tools/reverse-ip-lookup/
3. *Website:* https://mxtoolbox.com/SuperTool.aspx?action=ptr:192.168.178.1
4. Website: https://viewdns.info/reverseip/

Open Poorten (Passief)

Voordat er gescand wordt, is het altijd handig om naar de volgende drie websites te kijken. Deze websites geven bij het invullen van een IP-adres een overzicht van open poorten en bijhorende services maar ook van poorten die vroeger open stonden met bijhorende services.

Websites:

1. *Website:* https://www.shodan.io/
2. *Website:* https://censys.io/ipv4
3. *Website:* https://www.zoomeye.org/

2. Doel ontdekking

In de tweede fase van de methodiek wordt er onderzoek gedaan naar welke systemen in de scope bereikbaar zijn (Host Alive?) en op welke manier.

2.1. Host Alive?

Eerst wordt er gekeken of het IP-adres bereikt kan worden. Bij het versturen van ICMP-pakketjes naar het doelsysteem, moet er ook gebruik gemaakt worden van Wireshark om te kijken wat de response van het doelsysteem is op het verstuurde pakketje.

1. *hping3 -1* 192.168.178.1 (ICMP)
2. *fping -g* 192.168.178.0/24 (ICMP)

Soms kan het zo zijn dat het doelsysteem ICMP-pakketjes blokkeert en waardoor het lijkt alsof het systeem offline is. Doormiddel van een simpele nmap scan op port 443, die bijna nooit geblokkeerd is kan er gekeken worden of het systeem een response geeft op TCP-niveau.

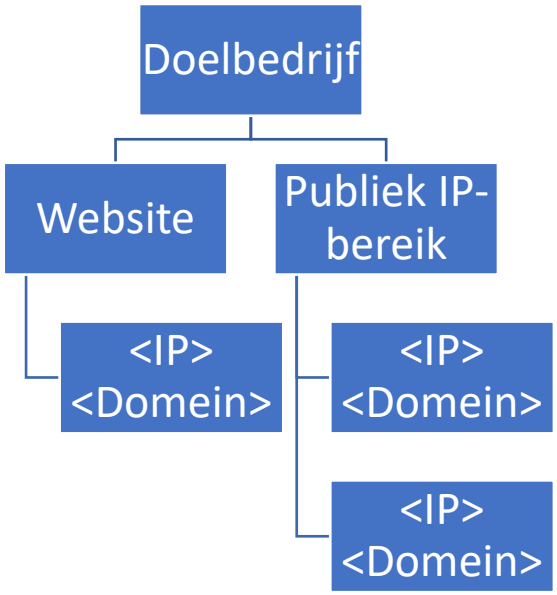
1. *nmap -Pn -p* 443 192.168.178.1 (TCP)
2. nmap -sn 192.168.178.1 (Scant 443, 80 en ICMP)

2.2. Tracing

Doormiddel van tracing kan er achterhaald worden welke knooppunten (nodes) + IP-adressen, het verstuurde pakket langs gaat voordat het wordt afgeleverd op het bestemmingspunt. Firewalls kunnen bepaalde protocollen blokkeren en daardoor kan er ook een omweg gemaakt worden aan de hand van andere protocollen.

1. *traceroute* 192.168.178.1 (UDP 33434)
2. *traceroute -I* 192.168.178.1 (ICMP)
3. *tcptraceroute* 192.168.178.1 443 (TCP)

Nadat er gekeken is welke systemen online staan, kan het doelnetwerk in kaart worden gebracht.



3. Enumeratie

In de 3e fase: enumeratie wordt er gekeken welke poorten open staan en welke services hierop draaien. Vervolgens wordt er zoveel mogelijk informatie opgehaald over de gevonden services. Na deze fase kan er ook gekozen worden om over te gaan op een webapplicatie assessment.

3.1. Poort scan

Alle poorten vallen onder standaard benamingen, dit hoeft niet te zeggen dat verschillende services niet op verschillende poorten kunnen draaien.

- *Poorten onder 1024*
  - Well-Known Ports, worden gebruikt door systeemprocessen die veelgebruikte typen netwerkservices bieden.
- *Poorten tussen 1024 – 29151*
  - Registered Ports, toegewezen voor specifieke service op aanvraag van een verzoekende entiteit.
- *Poorten tussen 49152 – 65535*
  - Dynamic/Private Ports, worden gebruikt voor privé of aangepaste services, voor tijdelijke doeleinden en voor automatische toewijzing van tijdelijke poorten.

Lijst met alle TCP en UDP poort nummers:

- https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
- https://www.speedguide.net/ports.php

Veel voorkomende open poorten, gebaseerd op Google resultaten:

TCP								UDP	
17	111	220	636	1194	5060	8083		53	500
20	113	389	843	1337	5432	8088		67	514
21	115	420	853	1433	5800	8443		68	546
22	119	443	990	1720	5900	8888		69	547
23	135	445	993	1723	6001	10000		88	631
25	137	465	995	2000	6346	30005		111	1434
53	138	514	1024	2300	7547	32768		123	1701
69	139	546	1025	3306	7676			135	4500
79	143	547	1026	3389	8000			137	8200
80	179	548	1027	3689	8080			161	8211
81	194	554	1080	4343	8081			162	28960
110	199	587	1137	4567	8082			445	

TCP-poortscan

1. Veilige scan (20 meest voorkomende poorten)
   a. *nmap -T2 -Pn -vvv --top-ports 20* 192.168.178.1
2. Agressieve scan (1000 meest voorkomende poorten)
   a. *nmap -T4 -Pn -vvv* 192.168.178.1

UDP-poortscan

1. Veilige scan (20 meest voorkomende poorten)
    a. *nmap -sU -T2 -Pn -vvv --top-ports 20* 192.168.178.1
3. Agressieve scan (1000 meest voorkomende poorten)
    b. *nmap -sU -T4 -Pn -vvv* 192.168.178.1

NMAP-responses:

- Open = Applicatie accepteert actief TCP/UDP-verbindingen.
- Closed = Poort is toegankelijk maar er is geen applicatie die ernaar luistert.
- Filtered = Kan niet bepaald worden of de poort open of closed is, omdat pakketfiltering voorkomt dat de pakketjes de poort bereiken. Dit kan gebeuren door: Netwerk firewall, Host firewall of Router regels.

3.2. OS-Fingerprinting

Bij genoeg open poorten kan er achterhaald worden welk OS er op het systeem draait.

Actief

Bij nmap is minimaal één open port en één closed port nodig. Nmap probeert de volgende aspecten te bemachtigen: Leverancier (Vendor), Operating System, Operating System generatie/versie en Apparaat type.

1. *nmap -vvv -Pn -O* 192.168.178.1

Xprobe2 stuurt probes naar het doelsysteem en probeert dan het OS van het systeem te raden.

1. *xprobe2 -vvv -M 11* 192.168.178.1

3.3. Serviceonderzoek

Bij het achterhalen van de open poorten kan er gekeken worden naar welke versie er op een service draait.

Nmap

Doormiddel van Nmap kan er per open poort bekeken worden welke versie van de service erop draait.

1. *nmap -Pn -vvv -sV -p* 443 192.168.178.1

Telnet & Netcat

Telnet maakt een connectie met de service en geeft daarop een antwoord. Werkt onder andere op de services: FTP, SSH, Telnet, SMTP, HTTP.

1. *telnet* 192.168.178.1 80
2. *nc -v* 192.168.178.1 80

Klik een paar keer op enter en/of escape en er komt vanzelf een response.

Service exclusieve tools

Service	Poort	Tool
Microsoft-ds (Samba)	445/TCP	smbclient //WORKGROUP -I 192.168.178.1
		smbmap -u root -p password -H 192.168.178.1
		rpcclient -U "" -N 192.168.178.1
		enum4linux -U -o 192.168.178.1
SNMP	161/UDP	snmp-check 192.168.178.1 -c public
		snmpwalk -c public 192.168.178.1 -v 1
		snmpenum 192.168.178.1 public
		onesixtyone 192.168.178.1 public
FTP	21/TCP	ftpmap -s 192.168.178.1
		ftp 192.168.178.1
SSH	22/TCP	ssh root@192.168.178.1 -p22
Telnet	23/TCP	telnet 192.168.178.1 23
SMTP	25/TCP	smtp-user-enum -M VRFY -u root -t 192.168.178.1
		ismtp -h 192.168.178.1:25
IPSEC (IKE)	500/4500 UDP	Ike-scan 192.168.178.1 -M -A
Netbios-ns	137/TCP	nbtscan -v 192.168.178.0/24
		nbtscan-unixwiz -f 192.168.178.0-100

Gedetailleerde scanners

Via Metasploit Framework en Nmap kunnen er scripts gebruikt worden om nog meer informatie uit services te verzamelen.

Metasploit Framework: https://www.offensive-security.com/metasploit-unleashed/auxiliary-module-reference/

- *Msfconsole > search {Service}*

Nmap scripting engine: https://nmap.org/nsedoc/scripts/

- *nmap -sC* 192.168.178.1
- *nmap --script=*script 192.168.178.1

4. Kwetsbaarheden in kaart brengen

Kwetsbaarheden in kaart brengen komt in andere methodieken voor als vulnerability mapping. In deze fase wordt er via twee manieren gekeken naar kwetsbaarheden. De eerste manier is aan de hand van automatische tools en de tweede manier door handmatig te kijken naar de gevonden versie van een service met bijhorende kwetsbaarheden.

4.1. Automatisch

De volgende tools scannen een IP-adres of range en analyseren dan of er kwetsbaarheden te vinden zijn op de aangegeven systemen. Daarnaast zijn de volgende 4 tools de meest gebruikte vulnerability scanners voor pentesters. De meeste tools hebben een gratis trial versie en OpenVAS is geheel gratis.

- **OpenVAS** – Greenbone
  - Volledig gratis.
- **Nessus** – Tenable.com
  - Nessus Essentials: Gratis maar maximaal 16 IP-adressen en beperkte functies.
  - Nessus Professional Gratis voor 7 dagen of 1 jaar voor 2.825,94.
- **NexPose** – Rapid7.com
  - Community edition: Gratis voor 30 dagen.
  - Nexpose licentie: *1 jaar voor 3125,-*
- **Qualys**– Qualys.com
  - Community edition: Gratis maar beperkte functies.
  - Qualys Cloud Platform: Gratis voor 30 dagen of *per maand: 500,-*

4.2. Handmatig

Naast het automatisch scannen van kwetsbaarheden door tools kan er ook gekeken worden naar de versienummers die in de voorgaande fases zijn gevonden. Deze versienummers kunnen bekeken worden aan de hand van kwetsbaarheid databases. Hier eerst volgen drie belangrijke kwetsbaarheid termen.

Common Vulnerability Scoring System (CVSS)
Industrie standard voor de beoordeling van de ernst van computersysteem beveiliging kwetsbaarheden. CVSS probeert ernstscores toe te wijzen aan kwetsbaarheden. Scores worden berekend op basis van een formule die afhankelijk is van verschillende statistieken die het gemak van exploiting en de impact van exploiting benaderen. Scores variëren van 0 tot 10.

Common Vulnerabilities and Exposure (CVE)
Databank met informatie over kwetsbaarheden in computersystemen en netwerken. Een vergelijkbaar project is dat van OSVDB. https://cve.mitre.org/

Common Weakness Enumeration (CWE)
Een categoriesysteem voor zwakheden en kwetsbaarheden van software. https://cwe.mitre.org/

Kwetsbaarheid databases:

- National Vulnerability Database (NVD)
  - Database van de Amerikaanse overheid
  - https://nvd.nist.gov/
- CVE Security Vulnerability database
  - Database met informatie over kwetsbaarheden
  - https://www.cvedetails.com/
- Xforce ibmcloud
  - Database met informatie over kwetsbaarheden.
  - https://exchange.xforce.ibmcloud.com/
- Packetstormsecurity
  - Data met informatie over kwetsbaarheden en exploits.
  - https://packetstormsecurity.com/

Risico matrix

Bij het in kaart brengen van kwetsbaarheden kan de pentester vervolgens berekenen wat het technische risico van de kwetsbaarheid is voor het bedrijf. Daarnaast kan de pentester een aanbeveling geven over wat het mogelijke bedrijfsrisico kan zijn van de kwetsbaarheid. Uiteindelijk bepaalt het bedrijf zelf wat het bedrijfsrisico is.

	Laag bedrijfsrisico	**Gemiddeld bedrijfsrisico**	**Hoog bedrijfsrisico**
Laag technisch risico			
Gemiddeld technisch risico			
Hoog technisch risico			

Het technisch risico kan ook een cijfer toegekend krijgen aan de hand van CVSS-scores. De nieuwste versie van CVSS is 3.1 en kan berekend worden aan de hand van een rekenmachine: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Na deze fase stopt het vulnerability assessment en kan de tester kiezen om in het systeem proberen in te breken en dus over te gaan naar een penetratietest.

5. Social Engineering (OPT)

Deze fase is optioneel, omdat het vrij diep kan ingaan op de privacy van de werknemers.

Social Engineering is voornamelijk gericht op de werknemers van het bedrijf en is een verdieping van de informatie dat al verzameld is over het bedrijf in de informatie verzamelen fase. Aan de hand van deze fase kan het beveiligingsbewustzijn van de werknemers getest worden. Daarnaast is deze fase enkel gericht op het versturen van phishing mails met neppe inlogportalen of malwarematige bestanden.

Tools

- *python dnstwist.py* example.com
  - Kijkt naar soortgelijke domeinnamen van een domein of die geregistreerd zijn.
- *evilginx2*
  - Man-in-the-middle attack framework voor capturing wachtwoord en bypass 2-factor-authentication.
- *httrack* www.example.com/pagina
  - Tool om volledig de website te kunnen kopiëren.
- *python hiddenEye.py*
  - Kiezen uit verschillende inlogportalen van websites. Vervolgens maakt de tool aan de hand van Ngrok, Serveo, Localxpose of Localtunnel een website met een neppe inlogportaal. Handige tip: redirect naar de link waar de inloggegevens incorrect zijn.
- *settoolkit (*Social Engineer Toolkit (SET))
  - Toolkit met daarin de keuze uit:
    - Spear-phishing
    - Malwarematige Media generator
    - QRCode generator
    - Website aanval
    - Massa mailer aanval

Creëren van malware matig bestand
Bestand met jpg, pdf of png aanmaken dat een malwarematig bestand is.

E-mail spoofing
Aan de hand van een website kan de email verzender gespoofed worden en het eruit laten zien dat de email door iemand anders is verstuurd. Beveiliging dat de ervoor zorgt dat dit soort email naar de spam box gaat: SPF, DKIM en DMARC

- https://emkei.cz/
  - Verstuurd een email vanaf elk mogelijk emailadres.

Wegwerp e-mails
Volgende twee websites kunnen gebruikt worden voor e-mails die niet langdurig gebruikt hoeven te worden.

- *Website:* https://www.guerrillamail.com/
- *Website:* http://www.fakemailgenerator.com/

6. Wachtwoord kraken

In deze fase, wordt er geprobeerd in te breken via het kraken van een wachtwoord. Voordat er begonnen wordt met het starten van wachtwoord kraken, wordt er eerst in kaart gebracht op welke systemen en waar overal ingelogd kan worden. Dit kan verschillen van website inlogportalen of services zoals SSH. Daarnaast zijn documenten omtrent het wachtwoord beleid van het bedrijf cruciaal in deze fase.

Test beveiligingsmechanisme
Check op:

- Na hoeveel pogingen IP of gebruiker geblokkeerd?
- Hoe snel mogen er pogingen gedaan worden?
- Hoelang geblokkeerd? (Minuten, Uren, Dagen, Weken, Maanden)
- Hoe worden accounts ontgrendeld? (Beheerder, Automatisch)

Gebruikersnaam enumeratie
Bij het invullen van verschillende gebruikersnamen:

- Check op verschillende HTTP-responses.
- Check URL op verschillende foutcodes.

Wachtwoord beleid
Waar moet een wachtwoord uit bestaan? Tekenset, kleine letters, hoofdletters, cijfers, speciale symbolen. Wat mag er niet in het wachtwoord: Namen, leeftijd, geboortedatum, gebruikersnamen. Hoe vaak kan een gebruiker een wachtwoord hergebruiken.

Wachtwoord functies
Test functies rond wachtwoorden zoals: Wachtwoord aanpassen/vergeten. Let op wachtwoord tips. Verschil tussen inlog pagina's op verschillende apparaten zoals: Mobiel, Tablet, Desktop.

CAPTCHA-Bypass

Inlog verificatie vragen
Vragen makkelijk te beantwoorden doormiddel van Social Media. Vragen zoals eerste school, vriend, huisdier.

Lijsten met wachtwoorden

1. https://wiki.skullsecurity.org/Passwords
2. https://github.com/danielmiessler/SecLists/tree/master/Passwords/Common-Credentials
3. https://cirt.net/passwords
4. https://github.com/govolution/betterdefaultpasslist
5. /usr/share/wordlists (Kali Linux)

Veel gebruikte gebruikersnamen en wachtwoorden.

Gebruikersnaam		**Wachtwoord**	
root	info	admin	qwerty
test	administrator	password	Pass123
admin	system	passwd	guest
user	super	username	123456789
guest	username	test	123456

Tools om woordenlijsten mee te maken.

crunch 2 6 01234abcdef# -o woordenlijst.txt

- Minimale lengte van (2)
- Maximale lengte van (6)
- Maak gebruik van de letters en cijfers: (01234abcdef#)
- De woordenlijst krijgt de naam: woordenlijst.txt

cewl -d 2 -m 5 -w woordenlijst.txt https://example.com

- Scan tot een diepte van (2)
- Minimale lengte van (5)
- De woordenlijst krijgt de naam: woordenlijst.txt
- Zoekt woorden van de website: example.com

python3 cupp.py -i -w woordenlijst.txt

- -i = Interactieve manier om wachtwoorden te genereren.
- -w = woordenlijst krijgt de naam: woordenlijs.txt

Tools voor brute-force attacks

hydra -l root *-P* woordenlijst.txt *-t* ssh://192.168.178.1

- -l = Gebruiker: root
- -P = woordenlijst: woordenlijst.txt
- -t = server

xHydra is de GUI versie van THC Hydra.

Veel voorkomende protocollen die Hydra kan brute forcen:

FTP	Mysql	SMB	Telnet	SSH	
FTPS	Mssql	SMTP	VNC	RDP	
HTTP	Pop3	SNMP	IMAP	HTTPS	

Protocol exclusieve brute forcers

PPTP	1723/TCP	Thc-pptp-bruter
IKE	500/TCP	IKECrack

7. Exploitatie

Bij het in kaart brengen van kwetsbaarheden kan er nu gekeken worden of deze geëxploiteerd kunnen worden. Eerst moet er gekeken worden of er exploits beschikbaar zijn voor de gevonden kwetsbaarheden en daarna wordt er gezocht naar een framework die ze kan uitvoeren.

7.1 Zoeken naar exploits

Databases met exploits:

- https://www.exploit-db.com/
- http://mvfjfugdwgc5uwho.onion/ (Zeroday.today)
- https://packetstormsecurity.com/

Tools om exploits te zoeken op Kali Linux:

- *searchsploit* Wordpress
  - Zoekt exploits aan de hand van exploit-db.com
- *python pompem.py -s* Wordpress
  - Zoekt via verschillende databases naar exploits

7.2 Uitvoeren exploits

De volgende tools hebben hun eigen database aan exploits, die vervolgens heel simpel uitgevoerd kunnen worden.

- **Metasploit Framework** – Rapid7
- **Armitage** (GUI voor Metasploit Framework)
- **AutoSploit**, Automated mass exploiter aan de hand van Shodan.io API & Metasploit.

Metasploit

Commando's om te gebruiken:

msfconsole	Start Metasploit console
exit	Stopt Metasploit console
connect <IP-Adres> <Port>	Hetzelfde als Telnet of Netcat
search <Woord>	Zoekt bij modules naar Woord
search name:mysql	Zoekt naar alle modules van mysql
use …/…/../Module	Gebruikt een bepaalde auxiliary of exploit
back	Gaat terug naar de vorige optie
show options	Laat alle opties zien.
show targets	Laat alle targets zien.
show payloads	Laat alle payloads zien.
set/ unset	Pas options aan zoals: RHOST, LHOST, RPORT, THREADS, PAYLOAD
check	Checkt of systeem kwetsbaar is.
exploit	Voert de exploit uit.

8. Na-Exploitatie

Na-exploitatie vindt plaats na het succesvol binnen dringen van een systeem. Hierbij kan het zo zijn dat de tester zich bevindt in een “restricted” shell en weinig rechten heeft. Bij privilege escalatie is het de uiteindelijke bedoeling dat de tester root rechten krijgt. Ten slotte kan de toegang behouden worden aan de hand van een backdoor om zo op een later moment terug te komen in het systeem.

8.1 Interne enumeratie

Voordat er begonnen wordt met privilege escalatie wordt er eerst gekeken welke informatie allemaal verkregen kan worden. Doordat besturingssystemen veel veranderen is er onderscheid gemaakt tussen Linux en Windows, omdat deze twee het meest voorkomen.

Linux

- https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List
    - Lijst met commando’s en bestanden die handig zijn voor na-exploitatie.
- https://gtfobins.github.io/
    - Lijst met commands voor het bypassen van lokale beveiliging restricties.

Bruikbare commando’s:

sudo -l	Toont alle toegestane commando’s voor de gebruiker.
uname -a	Toont alle systeem informatie.
whoami	Toont welke gebruiker je op dit moment bent.
id	Toont huidige gebruiker, groep
pwd	Toont in welke directory de gebruiker zich bevindt.
ls -la	Toont alle informatie van de bestanden en mappen in de directory.
ps aux	Toont alle processen
last -a	Toont laatste gebruiker dat heeft ingelogd
lsb_release -d	Toont huidige versie van de distro

Bruikbare bestanden:

/etc/resolv.conf	Name servers (DNS)
/etc/motd	Message of the day
/etc/issue	Huidige versie van de distro
/etc/passwd	Alle gebruikers
/etc/shadow	Hash van wachtwoorden van gebruikers
/etc/sudoers	Informatie over administratierechten.
/home/user/.bash_history	Gebruikersinvoer

Windows

- https://medium.com/@int0x33/day-26-the-complete-list-of-windows-post-exploitation-commands-no-powershell-999b5433b61e & https://0xsecurity.com/blog_files/Windows-Post-Exploitation.pdf
    - Twee websites met commando’s en bestanden die handig zijn voor na-exploitatie.
- https://lolbas-project.github.io/
    - Lijst met executables die handig zijn voor na-exploitatie.

8.2 Privilege escalatie

Algemeen

Tools:

- *BeRoot*

Windows

Wachtwoorden staan opgeslagen in het SAM-bestand dat te vinden is in &SystemRoot%/system32/config/SAM. De wachtwoorden zijn opgeslagen in een hashindeling: LM of NTLM. SYSKEY-functie zit er tegenwoordig ook in.

Dump de SAM-File:

- *gsecdump* (Wachtwoorden van SAM/AD of login sessies)
- *creddump* (cachedump, lsadump, pwdump) + (LM and NT hashes, Cached domain passwords, LSA secrets)
- *samdump2* (Syskey + hashes van Windows 2000/NT/XP/VISTA SAM.)
- *mimikatz* (Plaintexts passwords, hash, PIN code, Kerberos tickets)

Tools:

- *windows Exploit Suggester*
- *windows-privesc-check*
- *powersploit* (PowerShell)
- *tempracer*
- *jaws* (Windows Enum script)
- *empire* (Powershell Windows + Python Linux)
- *chntpw* (Reset Windows password)

Linux

Tools:

- *yodo*
- *unix-privesc-checker*
- *auto-root-exploit*
- *roothelper* (Meerdere scripts)
- *linenum*

Applicatie

- *keefarce* (Haalt wachtwoorden uit KeePass database)
- *chromepass* (Google Chrome wachtwoorden)

Hash krakers:
Bij het binnenhalen van /etc/shadow kan er door de volgende tools het wachtwoord omgerekend worden.

- *hashcat* (Hash-Cracker)
- *john* <bestand met hashed string> (Wachtwoord hash kraker)
- *johnny* (John Gui)
- *hate_crack*
- *cain and abel* (Wachtwoord recovery Windows)
- https://hashkiller.co.uk/Cracker (MD5 + NTLM + SHA1 + MySQL5 + SHA256 + SHA512)

Hash identifier:

- *hash-identifier*
- *findmyhash*

Hash voorbeelden

BASE64	dGVzdDEyMzQ1Njc4OTA=
MD5	8743b52063cd84097a65d1633f5c74f5
SHA1	b89eaac7e61417341b710b727768294d0e6a277b
SHA-256	127e6fbfe24a750e72930c220a8e138275656b8e5d8f48a98c3c92df2caba935
SHA-512	82a9dda829eb7f8ffe9fbe49e45d47d2dad9664fbb7adf72492e3c81ebd3e29134d9bc 12212bf83c6840f10e8246b9db54a4859b7ccd0123d86e5872c1e5082f
NTLM	b4b9b02e6f09a9bd760f388b67351e2b

Rainbow Table Crack:
Een rainbow table is een eenvoudige tabel met allerlei mogelijke wachtwoorden en de hashes van deze wachtwoorden. Het wordt gebruikt om wachtwoorden te kraken. Deze techniek is vele malen sneller dan brute force-techniek, waarbij de hashes van de wachtwoorden nog moeten worden berekend.

- *Website:* https://freerainbowtables.com/
- *Website:* https://ophcrack.sourceforge.io/tables.php
- *Website:* http://project-rainbowcrack.com/table.htm
- *ophcrack* (LM-wachtwoorden)
- *rcrack* (Rainbowcrack)

8.3 Toegang behouden

Tools

EggShell	QuasarRat	ahMyth
EvilOSX	TheFatRat	Backdoor-factory
Parat	Veil	Weevely
Pupy	WMIImplant	

Webapplicatie

De pentester kan beginnen met deze fase na de enumeratie fase en er een webapplicatie is gedetecteerd. Informatie uit voorafgaande fases: informatie verzamelen en enumeratie kan gebruikt worden in een webapplicatie test. Voordat er begonnen wordt met het testen van de webapplicatie moet eerst alle webpagina's en directories in kaart gebracht worden. Hierin zijn standaard webpagina's ook van belang, zoals:

- /Robots.txt
- /Login

Bij het analyseren van HTTP-requests maak gebruik van webproxies, zoals: Burpsuite en Webscarab.

HTTP Headers

Doormiddel van element inspecteren of door een proxy kan de header uitgelezen worden.

Headervelden

- Content-length = Geeft de lengte van de inhoud aan.
- Location = indien de server de webbrowser naar een andere pagina doorverwijst wordt hierbij het benodigde pad gevoegd.
- Server = Omvat een beknopte beschrijving van de serversoftware
- User-Agent = Geeft informatie over de aanvrager. Dit is meestal een webbrowser.
- Date = De datum en het tijdstip waarop het document verzonden is.
- Host = Omdat het pakket naar IP-adres wordt gestuurd weet de server niet op welk domein men aan het surfen is. In HTTP 1.1 is het verplicht om met deze header het domein mee te delen.

HTTP-response

- 100+ = Mededelend
- 200+ = Goed gevolg
- 300+ = Omleiding
- 400+ = Aanvraagfout (Fout door de client)
- 500+ = Serverfout (Fout door de server)
- 600+ = Proxyfout

https://nl.wikipedia.org/wiki/Lijst_van_HTTP-statuscodes

Web Application Framework & Content Management Systems

Handmatig:

HTTP Headers	X-Powered-By: …
	X-Generator: …
Cookies	GET /cake HTTP /1.1
	GET / HTTP/1.1
HTML Source Code	Belangrijke codes: head tags en meta tags
	<meta name="generator" content="…."/>
	<body id="…"
	DNN Platform
Specifieke bestanden en mappen	https://github.com/fuzzdb-project/fuzzdb/tree/master/discovery/predictable-filepaths (FuzzDB)

Technieken

Authenticatie bypass	Direct Page Request (Forced browsing)	
	Parameter modification	
	Session ID prediction	
Authorisatie testen	Directory traversal/ File include	
	Local File Inclusion	/preview.php?file=example.html
	Remote file Inclusion	
Session management testen	Cookie analyze	Cookie verzameling, Cookie reverse Engineering, Cookie manipulatie
	Cross-Site-Request-Forgery	
Input validation testing	Reflected XSS (Cross-Site Scripting)	
	Stored XSS (Cross-Site Scripting)	
	HPP (HTTP Parameter Poluttion)	
	SQL-Injection	/page.php?id=5
	Command Injection	

Proxy:

- Burp Suite (Proxy, Intruder, Repeater)
- WebScarab (Proxy & Fuzzer)
- OWASP ZAP (Automated scan: identificeert aanvallen, Manual Explore)
- Paros (Snelle proxy om Requests en Response te filteren.)

Exploiting

OWASP Checklist: https://www.owasp.org/index.php/Testing_Checklist

- SQLMap (SQL-Injection) – sqlmap -u 'https://example.com/page.php?id=5' --random-agent
- SQLNinja (Microsoft SQL Server)
- LFISuite (Local File Inclusion)
- Kadimus (Local File Inclusion)
- Commix (Command Injection)
- XSSER (XSS)
- recon-ng (Metasploit achtig)
- wfuzz (Brute force webpages op verschillende aanvallen)

CMS exclusief tools:

- Wpscan – WordPress scanner
- Joomscan – Joomla scanner
- Drupwn – Drupal scanner
- Wordpress Exploit Framework. https://github.com/rastating/wordpress-exploit-framework

Kwetsbaarheid scanner

Betaald	Gratis
Netsparker (5000 p/j)	*./w3af_console*
Acunetix (7000 p/j)	*nikto -host* https://example.com
Probely (70 p/m	*wapiti -u* https://example.com

Browser hacking

- BeEF

SSL:

- Sslscan (SSL-scan)
- Sslyze (SSL-scan)
- https://www.ssllabs.com/ssltest/

Reverse Shell cheat sheet
Bij een website waarbij het mogelijk is om een reverse shell te uploaden, gebruik de volgende cheatsheet: http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

- Weevely3
- B374k
- Miyachung
- Wso-2.8-web-shell

Netwerk pentest

Lijst van tools

Intercepter-NG	Multifunctioneel network toolkit.
Netsniff-NG	Multifunctioneel network toolkit.
Dsniff	Passief monitor netwerk voor interessante data.
filesnarf	Zelfde als Dsniff
mailsnarf	Zelfde als Dsniff
msgnarf	Zelfde als Dsniff
urlsnarf	Zelfde als Dsniff
webspy	Zelfde als Dsniff
Arpspoof	Netwerk interceptie
dnsspoof	Netwerk interceptie
macof	Netwerk interceptie
Wireshark	Analyze network traffic, sniffer, Intercepter
TcpDump	Netwerk sniffer
Kismet	Wireless network detector, sniffer and IDS.
Dsniff	Netwerk sniffer
Ettercap	MITM
BetterCAP	MITM
Morpheus	MITM
Aircrack-NG	MITM
Reaver	Audit security of Wifi (WPA/WPA2)
Wifite	Draadloos netwerk tool
Wifiphisher	Draadloos netwerk tool
Airsnort	Draadloos netwerk tool
BdAddr	Draadloos netwerk tool
Bluesnarfer	Draadloos netwerk tool
Btscanner	Draadloos netwerk tool
FakeAP	Draadloos netwerk tool
GFI LANguard	Kwetsbaarheid tool
WifiTAP	Wifi Tool
GPSdrive	GPS tool
MACchanger	Netwerk tool
Ngrep	Network sniffing
Ntop	Network sniffing
Phoss	Network sniffing
SinFP	Network sniffing
SMB Sniffer	Network sniffing
Sslstrip	HTTPS naar HTTP
Sslstrip2	HTTPS naar HTTP
Ssldump	HTTPS naar HTTP

DoS (Stress test)

Het doelbedrijf kan akkoord gaan met het uitvoeren van (D)DoS-aanvallen. De tester kijkt hierbij of het mogelijk is om een systeem of website offline te krijgen.

Stress test

Is een testvorm waarbij de stabiliteit van een geheel wordt getest. Hierbij wordt getest met een zwaardere belasting dan gebruikelijk, vaak tot het punt dat het systeem het begeeft. Het doel hiervan is te onderzoeken wat er gebeurt en waar de grens ligt.

Software: Een test waarbij getest wordt op zaken als robuustheid, beschikbaarheid en foutafhandeling bij zware belasting. Het doel van deze tests is na te gaan of de software niet crasht als gevolg van bijvoorbeeld te weinig RAM-geheugen en/of opslagcapaciteit, ongebruikelijke aantallen gelijktijdige gebruikers of DoS-aanvallen.

DoS (Denial of Service)

Een situatie waarin een computersysteem onbedoeld niet beschikbaar is voor de door de gebruiker verwachte dienstverlening

DDoS (Distributed Denial Of Service)

Pogingen om een computer, computernetwerk of dienst niet of moelijker bereikbaar te maken voor de bedoelde klanten. Het verschil met een DoS is dat bij DDoS meerdere computers tegelijk de aanval op hun doelwit uitvoeren.

Er zijn twee algemeen vormen van DoS-aanvallen: crashaanvallen en de flood aanvallen. Er zijn verschillende soorten van DoS-aanvallen, maar ook verschillende vormen van aanvallen.

Vijf basisvormen:

1. Verbruik van computer gerelateerde middelen, zoals bandbreedte of schrijfruimte.
2. Verstoring van configuratie-informatie.
3. Verstoring van de staat van het apparaat, zoals het ongevraagd resetten.
4. Verstoring van netwerkcomponenten.
5. Obstructie van communicatiemiddelen tussen de beoogde gebruikers en het doelwit, zodat ze niet meer adequaat kunnen communiceren.

Tools

- HOIC (High Orbit Ion Cannon) – Verstuurd HTTP POST en GET requests.
- LOIC (Low Orbit Ion Cannon) – Verstuurd TCP of UDP-pakketjes.
- Memcrashed
- SlowLoris – Verstuurd HTTP requests.
- T50, Stress testing op 15 verschillende protocollen (Waaronder: ICMP, TCP, UDP).
- UFONet, Mogelijkheid op DDoS https://ufonet.03c8.net/

Tools list

In onderstaande tabellen staan de tools/websites die in deze handleiding voorkomen met bijhorende GitHub repository.

(Na exploitatie en netwerk pentest tools zijn niet meegenomen)

Websites

http://whois.domaintools.com/
https://mxtoolbox.com/SuperTool.aspx
https://builtwith.com/
https://w3techs.com/sites
https://www.wappalyzer.com/download
https://www.google.com/
https://www.get-metadata.com/
http://metapicz.com/#landing
https://archive.org/web/
https://securityheaders.com/
https://urlscan.io/
https://internet.nl/
https://spyse.com/search/subdomain
https://dnsdumpster.com/
https://www.dogpile.com/
https://hunter.io/
https://haveibeenpwned.com/
https://dehashed.com/
https://intelx.io/
https://www.telefoonboek.nl/
https://www.detelefoongids.nl/personen/6-1/
https://ipinfo.io/
https://check-host.net/ip-info
https://hackertarget.com/reverse-ip-lookup/
https://hostingchecker.com/tools/reverse-ip-lookup/
https://viewdns.info/reverseip/
https://www.shodan.io/
https://censys.io/ipv4
https://www.zoomeye.org/
https://nvd.nist.gov/
https://www.cvedetails.com/
https://exchange.xforce.ibmcloud.com/
https://packetstormsecurity.com/
https://emkei.cz/
https://www.guerrillamail.com/
http://www.fakemailgenerator.com/
https://www.exploit-db.com/
http://mvfjfugdwgc5uwho.onion/ (Zeroday.today)
https://packetstormsecurity.com/
https://www.ssllabs.com/ssltest/
http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
https://ufonet.03c8.net/

Tools

dnsrecon	Kali Linux
wafw00f	Kali Linux
Metagoofil	Kali Linux
FOCA	https://github.com/ElevenPaths/FOCA
Pdfinfo	Kali Linux
exiftool	Kali Linux
amass	Kali Linux
dnsmap	Kali Linux
Dirb	Kali Linux
Dirbuster	Kali Linux
skipfish	Kali Linux
TheHarvester	Kali Linux
SimplyEmail	https://github.com/SimplySecurity/SimplyEmail
SpiderFoot	https://github.com/smicallef/spiderfoot
Maltego	Kali Linux
Nmap	Kali Linux
Xprobe2	Kali Linux
telnet	Kali Linux
nc	Kali Linux
Metasploit Framework	Kali Linux
Smbclient	Kali Linux
Smbmap	Kali Linux
Rpcclient	Kali Linux
Enum4linux	Kali Linux
Snmp-check	Kali Linux
Snmpenum	https://github.com/ajohnston9/snmpenum
Onesixtyone	https://github.com/trailofbits/onesixtyone
Ftpmap	https://github.com/ovpn-to/ftpmap
ftp	Kali Linux
Ssh	Kali Linux
Smtp-user-enum	Kali Linux
ismtp	Kali Linux
Ike-scan	Kali Linux
Ikeforce	https://github.com/SpiderLabs/ikeforce
Nbtscan	Kali Linux
Nbtscan-unixwiz	Kali Linux
OpenVAS	Kali Linux
Nessus	https://www.tenable.com/products/nessus
NexPose	https://www.rapid7.com/products/nexpose/
Qualys	https://www.qualys.com/
dnstwist	https://github.com/elceef/dnstwist
Evilginx2	https://github.com/kgretzky/evilginx2
httrack	Kali Linux
hiddeneye	https://github.com/DarkSecDevelopers/HiddenEye
settoolkit	Kali Linux
crunch	Kali Linux

Cewl	Kali Linux
Cupp.py	https://github.com/Mebus/cupp
Hydra	Kali Linux
xhydra	Kali Linux
Thc-pptp-bruter	Kali Linux
IKECrack	Kali Linux
Searchsploit	Kali Linux
Pompem	https://github.com/rfunix/Pompem
Armitage	Kali Linux
Autosploit	https://github.com/NullArray/AutoSploit
Burp Suite	Kali Linux
WebScarab	Kali Linux
OWASP ZAP	Kali Linux
Paros	Kali Linux
SQLMap	Kali Linux
SQLNinja	Kali Linux
LFISuite	https://github.com/D35m0nd142/LFISuite
Kadimus	https://github.com/P0cL4bs/Kadimus
Commix	https://github.com/commixproject/commix
XSSER	Kali Linux
Recon-ng	Kali Linux
Wfuzz	Kali Linux
wpscan	Kali Linux
Joomscan	Kali Linux
Drupwn	https://github.com/immunIT/drupwn
Wordpress exploit framework	https://github.com/rastating/wordpress-exploit-framework
Netsparker	https://www.netsparker.com/
Acunetix	https://www.acunetix.com/
Probely	https://probely.com/
BeEf	Kali Linux
sslscan	Kali Linux
sslyze	Kali Linux
Weevely3	https://github.com/epinna/weevely3
HOIC	https://github.com/FelixWieland/HOIC
LOIC	https://github.com/NewEraCracker/LOIC
Memcrashed	https://github.com/649/Memcrashed-DDoS-Exploit
SlowLoris	https://github.com/gkbrk/slowloris
T50	Kali Linux

Bronnen

Methodieken:

http://www.pentest-standard.org/index.php/Main_Page (PTES)
https://www.isecom.org/OSSTMM.3.pdf (OSSTM)
http://www.oissg.org/issaf/ (ISSAF)
https://www.owasp.org/images/1/19/OTGv4.pdf (OTG)
http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html (PTF)
https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf (PCI DSS)

Tool lijsten:

https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/
https://github.com/jesusprubio/awesome-nodejs-pentest
https://github.com/enaqx/awesome-pentest/blob/master/README.md
https://github.com/sbilly/awesome-security/blob/master/README.md
https://github.com/wtsxDev/Penetration-Testing
https://www.yeahhub.com/windows-linux-privilege-escalation-tools-2019/
https://github.com/pentestmonkey?tab=repositories

Pentest/ Cybersecurity forums:

https://www.reddit.com/r/hacking/ (963K)
https://www.reddit.com/r/privacy/ (662K)
https://www.reddit.com/r/netsec/ (352K)
https://www.reddit.com/r/HowToHack/ (210K)
https://www.reddit.com/r/security/ (137K)
https://www.reddit.com/r/cybersecurity/ (111K)
https://www.reddit.com/r/AskNetsec/ (104K)
https://www.reddit.com/r/ReverseEngineering/ (91K)
https://raidforums.com/
https://hackforums.net/

Testomgevingen: (gemarkeerde enkel gebruikt.)

https://lab.pentestit.ru/pentestlabs/8	Website
https://www.hackthebox.eu/	Website
https://ctf.hacker101.com/	Website
http://www.gh0st.net/wiki/index.php?title=Main_Page	Website
https://www.root-me.org/?lang=en	Website
https://www.hackthissite.org/	Website
http://underthewire.tech/	Website
http://overthewire.org/wargames/	Website
https://pentesterlab.com/	Website
https://attackdefense.com/	Website
https://www.vulnhub.com/	Virtualbox
Metasploitable	Virtualbox
Webgoat/ WebWolf	Virtualbox