MONIN
Database Managed Services

HANDLEIDING

Security Audit

Contactpersoon	Jonas Willems (Monin NV)

T 03/450 67 89
E info@monin-it.be
W www.monin-it.be
BE 0879.917.484

MONIN nv.
Prins Boudewijnlaan 41
2650 Edegem

MONIN

INHOUD

1 INLEIDING

Een security audit is een essentieel onderdeel van het waarborgen van de veiligheid van systemen en netwerken. Deze handleiding neemt u stap voor stap mee door het proces, waarbij verschillende tools worden gebruikt voor OSINT, databreaches-lookup, vulnerability assessments en encryptie-in-transit.

1.1 OSINT (Open Source Intelligence)

Open Source Intelligence (OSINT) is het proces van het vergaren en analyseren van informatie uit publieke bronnen. In deze fase concentreren we ons op het verkrijgen van inzicht in de organisatie vanuit een externe, openbare context. Het doel is om mogelijke kwetsbaarheden bloot te leggen, zoals e-mailadressen, subdomeinen en publieke relaties. Dit draagt bij aan het begrip van hoe een potentiële aanvaller informatie zou kunnen vergaren om een gerichte aanval uit te voeren.

1.2 Databreach Search Engines

Datalekken vormen een aanzienlijk veiligheidsrisico, omdat gelekte informatie vaak wordt misbruikt voor aanvallen zoals phishing of het uitproberen van gestolen inloggegevens. In deze fase onderzoeken we of de organisatie eerder betrokken is geweest bij datalekken en of e-mailadressen of wachtwoorden openbaar beschikbaar zijn. Dit stelt ons in staat om proactief maatregelen te nemen, zoals het wijzigen van wachtwoorden en het implementeren van extra beveiligingslagen, aangezien hackers vaak proberen de beveiliging te omzeilen door toegang te krijgen tot wachtwoorden of hun gehashte versies, die vervolgens kunnen worden ontcijferd.

1.3 Vulnerability Assessment

Een grondige beoordeling van kwetsbaarheden is een onmisbaar onderdeel van een sterke beveiligingsstrategie. In deze fase richten we ons op het systematisch identificeren van zwakke plekken. Hierbij spelen twee essentiële onderdelen een rol: het onderzoeken van de host en het doorlichten van de webserver en applicatie. Beide aspecten zijn van groot belang om een volledig beeld te krijgen van de beveiligingssituatie.

1.4 Network Analysis Tools – Encryption In Transit

Een grondige veiligheidsaudit omvat een nauwkeurige netwerkanalyse voor risico-identificatie en aanvalsdetectie. Deze sectie focust op Netwerkanalysetools, zoals Wireshark en Tcpdump, met nadruk op het controleren van de versleuteling van het internetverkeer.

2 FASE 1: OSINT (OPEN SOURCE INTELLIGENCE)

2.1 theHarvester

theHarvester is echt handig als je de online aanwezigheid van een doeldomein wilt ontdekken. Het geeft je waardevolle inzichten die je kunt gebruiken voor beveiligingsbeoordelingen, OSINT-onderzoek en het opsporen van mogelijke zwakke plekken in de digitale infrastructuur. Door meerdere bronnen te gebruiken, krijg je een schat aan informatie.

URL: https://github.com/laramies/theHarvester

Commando:

```
theHarvester -d example.com -l 500 -b all
```

Parameters:

-d example.com: Specificeert het doeldomein waarvoor informatie moet worden verzameld. Vervang "example.com" door het gewenste domein.

-l 500: Stelt een limiet in voor het aantal resultaten dat moet worden weergegeven. In dit geval zijn maximaal 500 resultaten toegestaan.

-b all: Hiermee wordt aangegeven dat alle beschikbare bronnen moeten worden gebruikt om informatie te verzamelen. Dit omvat zoekmachines, DNS-gegevens, PGP-sleutels, Shodan, en meer. API keys mogelijk.

2.2 SpiderFoot

SpiderFoot automatiseert OSINT-verzameling en -analyse.

Het kan bijvoorbeeld de volgende gegevens verwerken:

- IP-adres
- Domein/subdomein
- Netwerk subnet (CIDR)
- E-mailadres
- Telefoonnummer
- Naam van een persoon

URL: https://github.com/smicallef/spiderfoot

Commando:

```
python3 ./sf.py -l 127.0.0.1:5001
```

Parameters:

-l 127.0.0.1:5001: Specificeert het doel-IP-adres (127.0.0.1) en de poort (5001) voor de spiderfoor webapplicatie (GUI). Hierop kan een scan gestart worden.

2.3 FOCA

FOCA is een krachtige tool die automatisch naar documenten kan zoeken en de metagegevens van deze documenten kan analyseren. Je kunt ook handmatig documenten toevoegen aan de tool, waardoor je de mogelijkheid hebt om zelf gevonden documenten te onderzoeken en relevante metagegevens zoals IP-adressen, namen en computernamen te extraheren. Hiermee biedt FOCA een flexibele aanpak voor het onthullen van verborgen details in verschillende bestandstypen.

URL: https://github.com/ElevenPaths/FOCA

2.4 Maltego

Maltego is een krachtige grafische tool die is ontworpen voor het visualiseren van informatie en het in kaart brengen van relaties tussen verschillende gegevenselementen. Het stelt gebruikers in staat om complexe gegevens te analyseren en te begrijpen door middel van visuele representatie. Je kan de gegevens die je gevonden hebt via theHarvester, FOCA en spiderfoor importeren. De betaalde versie heeft veel meer mogelijkheden.

URL: https://www.maltego.com/

2.5 Photon

Photon is een krachtige OSINT-tool die razendsnelle website-analyse mogelijk maakt. Met indrukwekkende snelheid verzamelt het diverse gegevens, waaronder URLs, inlichtingen, bestanden, geheime sleutels, en meer. De flexibele instellingen stellen gebruikers in staat de webcrawl aan te passen aan hun behoeften

URL: https://github.com/s0md3v/Photon

Commando:

```
python3 photon.py -u example.com
```

Parameters:

-u, --url: Specificeert de doel-URL voor analyse.

3 FASE 2: DATABREACHES LOOKUP

3.1 Have I Been Pwned

Have I Been Pwned is een online service waarmee je kunt controleren of je e-mailadres betrokken is bij bekende datalekken. Hier is hoe je het gebruikt:

1. Bezoek de Website: https://haveibeenpwned.com/
2. Geef een gevonden e-mailadres in.
3. Controleer op Lekken: Klik om te zien of het e-mailadres voorkomt in bekende datalekken.
4. Resultaten: Ontvang gedetailleerde informatie over de betrokken databreaches.

3.2 LeakPeek

LeakPeek is een online dienst waarmee je mogelijke gegevenslekken kunt onderzoeken. Volg deze stappen om gebruik te maken van LeakPeek:

1. Bezoek de Website: https://leakpeek.com/
2. Begin Onderzoek: Op de website kun je direct beginnen met het onderzoeken van mogelijke gegevenslekken.
3. Voer Gegevens In: zoals e-mailadressen of gebruikersnamen, om het onderzoek te starten.
4. Resultaten: Ontvang informatie over eventuele gegevenslekken waarbij de ingevoerde gegevens betrokken kunnen zijn.

3.3 DeHashed

DeHashed is een online dienst waarmee je mogelijke gegevenslekken kunt onderzoeken. Deze is wel betalend. Volg deze stappen om gebruik te maken van DeHashed:

1. Bezoek de Website: https://dehashed.com/
2. Aanmelden: Je moet je aanmelden voor een account op DeHashed. Voer vervolgens gevonden gegevens in om te controleren op gelekte wachtwoorden.
3. Resultaten: Ontvang gedetailleerde informatie over eventuele gelekte wachtwoorden die verband houden met je gevonden gegevens.

3.4 Intelligence X

Intelligence X is een platform waarmee je kunt zoeken naar gegevens van jouw organisatie. Dit platform is zeer prijzig maar geeft toegang tot zeer recente databreaches. Volg deze stappen om Intelligence X te gebruiken:

1. Bezoek de Website: https://intelx.io/
2. Zoekopdracht Uitvoeren: Voer een zoekopdracht in, specifiek gericht op je organisatienaam, domein of andere relevante gegevens.
3. Resultaten: Ontvang gedetailleerde informatie over mogelijke gegevens die beschikbaar zijn op het platform met betrekking tot de organisatie.

4 FASE 3: VULNERABILITY ASSESSMENT

4.1 Host:

4.1.1 NMAP

NMAP is een krachtige tool voor netwerkservices en poortscans. Dit voorbeeldcommando voert een grondige scan uit om alle open poorten en services te identificeren en biedt een uitgangspunt voor verdere beveiligingsmaatregelen.

URL: https://github.com/nmap/nmap

Commando:

```
nmap -p 1-65535 -sV -sT host
```

Parameters:

-p-: Scan alle 65535 poorten.

-sV: Detecteer de versie van services.

-sC: Voer standaardscripts uit voor service-detectie.

-oN scan_resultaat.txt: Sla de resultaten op in een tekstbestand.

4.1.2 THC-HYDRA

thc-hydra is een krachtige tool ontworpen om de sterkte van inloggegevens te testen door middel van brute force-aanvallen op verschillende protocollen.

URL: https://github.com/vanhauser-thc/thc-hydra

Commando:

```
hydra -l username -P password_list.txt ftp://example.com
```

Parameters:

-l [gebruikersnaam]: Specificeert de gebruikersnaam voor de aanval.

-P [wachtwoordlijst.txt]: Specificeert het pad naar de wachtwoordlijst.

[service://doeladres]: Specificeert de service (bijv. ftp, http) en het doeladres, waardoor het verschillende protocollen kan testen.

4.1.3 MONIN'S DB INSPECTOR

Zie gebruikershandleiding Monin's DB. Inspector.

4.1.4 OPENVAS

OpenVAS is een krachtige open-source vulnerability scanner die wordt gebruikt om beveiligingslekken in systemen te identificeren.

URL: https://github.com/greenbone/openvas-scanner

Installatie:

Zorg ervoor dat OpenVAS is geïnstalleerd op je systeem. Afhankelijk van je besturingssysteem kunnen installatie-instructies variëren. Raadpleeg de OpenVAS-documentatie voor gedetailleerde installatiestappen.

- Start OpenVAS op door de juiste opdracht in je terminal in te voeren. Dit kan variëren, maar het kan er ongeveer uitzien als:

```
openvas start
```

- Gebruik de OpenVAS-beheerinterface (vaak toegankelijk via een webbrowser) om een nieuwe scan te configureren.
- Stel de scanparameters in, zoals het doelsysteem, het type scan (bijv. volledige scan) en eventuele specifieke instellingen.
- Start de scan en laat OpenVAS het doelsysteem grondig analyseren op beveiligingslekken.
- Na de scan ontvang je uitgebreide rapporten met informatie over gevonden kwetsbaarheden, risiconiveaus en aanbevolen maatregelen.

4.1.5 NESSUS

Nessus is een toonaangevende vulnerability scanner die wordt ingezet voor gedetailleerde evaluatie van kwetsbaarheden in systemen. Volg onderstaande stappen om Nessus te gebruiken:

URL: https://www.tenable.com/products/nessus

1. Installeer Nessus op je systeem door de installatie-instructies te volgen op de officiële Nessus-website.
2. Start Nessus en ga naar de webinterface die normaal gesproken toegankelijk is via een webbrowser op https://localhost:8834.
3. Maak een Nessus-account aan of log in met bestaande inloggegevens.
4. Creëer een nieuwe scan en configureer de parameters zoals het doelsysteem, het type scan (bijv. vulnerability scan, compliance scan) en andere specifieke instellingen.

5. Start de scan en laat Nessus het doelsysteem grondig analyseren op kwetsbaarheden.
6. Bekijk de uitgebreide scanrapporten die Nessus genereert. Hierin vind je details over gevonden kwetsbaarheden, risiconiveaus en aanbevolen oplossingen.

4.1.6 NEXPOSE

Nexpose is een krachtige vulnerability management-oplossing die geavanceerde scans uitvoert om kwetsbaarheden te identificeren en te classificeren. Hier zijn de stappen om een geavanceerde scan uit te voeren met Nexpose:

URL: https://www.rapid7.com/products/nexpose/

1. Installeer Nexpose volgens de richtlijnen op de officiële Rapid7-website.
2. Open de Nexpose-console via een webbrowser door naar het juiste adres te gaan (meestal https://localhost:3780).
3. Log in op de Nexpose-console met de juiste inloggegevens
4. Configureer de scanparameters, zoals het type scan (bijv. volledige scan, snelle scan) en specifieke instellingen op basis van de behoeften van de organisatie.
5. Start de geavanceerde scan en laat Nexpose kwetsbaarheden identificeren en classificeren op het doelsysteem.
6. Bekijk de gedetailleerde rapporten die Nexpose genereert. Deze rapporten bevatten informatie over de aard van de kwetsbaarheden, de ernst en aanbevolen oplossingen.

4.2 Webserver & Applicatie

4.2.1 WAFW00F

WAFW00F is een tool die is ontworpen om web application firewalls (WAFs) te identificeren en eventuele zwakheden op te merken. Hier volgt een eenvoudig voorbeeld van het uitvoeren van een WAF-check met WAFW00F:

URL: https://github.com/EnableSecurity/wafw00f

Commando:

```
wafw00f -u http://example.com
```

Parameters:

-u http://example.com: Specificeert de doel-URL voor de WAF-check.

4.2.2 OWASP ZAP

OWASP ZAP (Zed Attack Proxy) is een uitgebreide tool voor het testen van beveiliging van webapplicaties. Deze tool wordt gebruikt voor het vinden van vulnerabilities. Hier is hoe je een actieve scan uitvoert met OWASP ZAP:

URL: https://www.zaproxy.org/

1. Installeer OWASP ZAP op je systeem door de installatie-instructies te volgen op de officiële OWASP ZAP-website.
2. Start OWASP ZAP en open de grafische gebruikersinterface (GUI) via de opdrachtregel of het startmenu.
3. Configureer de doel-URL van de webapplicatie die je wilt scannen binnen de OWASP ZAP-interface.
4. Voer een actieve scan uit door de doel-URL te selecteren en de scan te starten vanuit het OWASP ZAP-dashboard.
5. OWASP ZAP zal actief zoeken naar kwetsbaarheden, zoals SQL-injecties, cross-site scripting (XSS) en andere beveiligingslekken. Analyseer de resultaten zorgvuldig.

4.2.3 DIRB

DIRB is een krachtige tool die wordt gebruikt voor het ontdekken van verborgen mappen op een webserver. Hier is hoe je DIRB kunt gebruiken om mogelijke inbreukpunten te identificeren:

URL: https://www.kali.org/tools/dirb/

Commando:

```
dirb http://example.com
```

4.2.4 SQLMAP

SQLMAP is een krachtige tool voor het detecteren van SQL-injecties en het identificeren van kwetsbaarheden in databases. Hier is hoe je SQLMAP kunt gebruiken:

URL: https://sqlmap.org/

Commando:

```
sqlmap -u "http://example.com/index.php?id=1" -dbs
```

Parameters:

-u: **"http://example.com/index.php?id=1":** Specificeert de doel-URL met de parameter die mogelijk kwetsbaar is voor SQL-injectie.

4.2.5 NIKTO

NIKTO is een krachtige tool voor het scannen van bekende kwetsbaarheden en het identificeren van mogelijke beveiligingslekken op web servers. Hier is hoe je NIKTO kunt gebruiken:

URL: https://github.com/sullo/nikto

Commando:

```
nikto -h http://example.com
```

Parameters:

-h http://example.com: Specificeert de doel-URL voor het scannen op kwetsbaarheden.

5 FASE 5: NETWORK ANALYSIS TOOLS

5.1 Tcpdump

Tcpdump is een tool waarmee je netwerkverkeer kunt vastleggen, en in combinatie met Wireshark kun je het vastgelegde verkeer analyseren voor mogelijke beveiligingsproblemen. Hier is hoe je tcpdump kunt gebruiken:

URL: https://www.tcpdump.org/

Commando:

```
tcpdump -i eth0 -n -s 0 -w capture.pcap
```

Parameters:

-i eth0: Specificeert de interface waarop je het netwerkverkeer wilt vastleggen (vervang eth0 door de juiste interface).

-n: Toont IP-adressen in numerieke vorm.

-s 0: Gebruikt de maximale pakketlengte.

-w capture.pcap: Geeft de bestandsnaam op waarin het vastgelegde verkeer wordt opgeslagen.

5.2 Wireshark

Wireshark is een krachtige tool voor het analyseren van netwerkverkeer. Je kan de .pcap file importeren of zelf sniffen. Hier is hoe je vastgelegd verkeer importeert en analyseert met Wireshark:

URL: https://www.wireshark.org/download.html

1. Start Wireshark op je computer.
2. Ga naar "File" in het bovenste menu en kies "Open" om het tcpdump-bestand te importeren.
3. Bekijk de vastgelegde pakketten in de hoofdweergave van Wireshark.
4. Typ in het filtervak ssl of tls en druk op Enter. Hierdoor worden alle pakketten gefilterd die SSL/TLS-versleuteling bevatten.
5. Versleutelde pakketten worden vaak in verschillende kleuren weergegeven in Wireshark. Bijvoorbeeld, HTTPS-verkeer (beveiligde websites) wordt meestal groen weergegeven.
6. Bekijk de details van geselecteerde pakketten en zoek naar SSL/TLS-handshakes. Deze geven aan dat er een versleutelde verbinding tot stand is gebracht.
7. Hoewel de payload zelf versleuteld is, kun je de headers en metagegevens bekijken voor meer informatie over de versleutelde verbinding.

6 FASE 6: DATABASE SCANNERS

6.1 Msdat

Msdat is een tool die wordt gebruikt voor het identificeren van zwakheden in de databaseconfiguratie, vooral gericht op Microsoft SQL Server. Volg deze stappen om een scan uit te voeren:

URL: https://github.com/quentinhardy/msdat

6.2 Odat

Odat is een tool ontworpen voor het ontdekken van mogelijke inbreukpunten in Oracle-databases. Volg deze stappen om een scan uit te voeren:

URL: https://github.com/quentinhardy/odat