AP HOGESCHOOL ANTWERPEN

AP.BE

Security Project

Cloud documentatie

Opleiding: 2ITCSC1

Academiejaar:2023-2024

Kamil Banaszek

Jonas Janssens

Bram Van Goethem

Jan Guldentops

Inhoudsopgave

1 Inleiding

Voor het cybersecurityproject zijn wij toegewezen aan de Cloud-groep. In het begin was het niet duidelijk wat er precies van ons verwacht werd. Er was gezegd dat wij de cloudomgeving zouden monitoren met een SIEM. Hierdoor gingen we ervan uit dat we een VM op de infrastructuur zouden hebben, maar dit bleek niet het geval te zijn. We moesten onze monitoring integreren in de SIEM van groep 3 (implementatie van een SIEM). Uiteindelijk is ook de lokale AD hieraan toegevoegd, waarop wij ons hebben gefocust.

Met "cloudomgeving" wordt de O365-omgeving bedoeld. Hiervoor zouden we een tenant krijgen, waarvan we de logs kunnen ophalen. We zouden controleren of bepaalde beveiligingsvoorwaarden zijn geïmplementeerd.

We vonden de eerste weken persoonlijk erg traag. De communicatie binnen het team verliep nog niet soepel en de onduidelijkheden rond de opdracht vormden een groot probleem. Het duurde even voordat we als groep goed op gang kwamen.

2 Kickoff

Bij de Kickoff zijn we direct begonnen met onderzoeken welke soorten cloudomgevingen bedrijven en gemeentes gebruiken. Hier kregen we niet veel resultaten op terug. Alleen Azure AD (Entra ID) kwam steeds terug.

3 Begin research

In het begin van ons onderzoek begonnen we met het onderzoeken van welke cloudoplossingen gemeentes gebruiken. Onze lector zei dat we ons moesten focussen op het Microsoft 365-gedeelte. Vervolgens begonnen we met brainstormen over hoe we dit zouden aanpakken. Wat we ontdekten, is dat Security Onion werkt met Elasticsearch, wat een integratie heeft voor Office 365. Zonder een werkende Security Onion moesten we wachten tot alles van de infrastructuur gereed was en tot Security Onion beschikbaar was.

Het SIEM-team twijfelde in het begin over de keuze voor een definitieve SIEM. Hun eerste keuze was Wazuh, en de andere was Security Onion. Ze gingen aan de slag met Security Onion, maar kwamen al snel problemen tegen.

Ons team kwam vrij snel uit op Azure CLI. Azure CLI is een command-line tool waarmee je Azure-resources rechtstreeks vanuit de opdrachtregel kunt beheren. Het is ontworpen om ontwikkelaars en IT-professionals te helpen efficiënt met Azure-services te werken en taken te automatiseren. In het begin leek dit een goede tool om mee te beginnen, maar we hadden nog geen tenant en de informatie over EntraID was nog beperkt.

EntraID zelf is de cloudgebaseerde identiteits- en toegangsbeheerservice van Microsoft. Het dient als ruggengraat voor authenticatie en autorisatie voor Azure-cloudservices en de Microsoft 365-suite (voorheen Office 365) van toepassingen, evenals voor duizenden andere cloudgebaseerde en on-premises toepassingen.

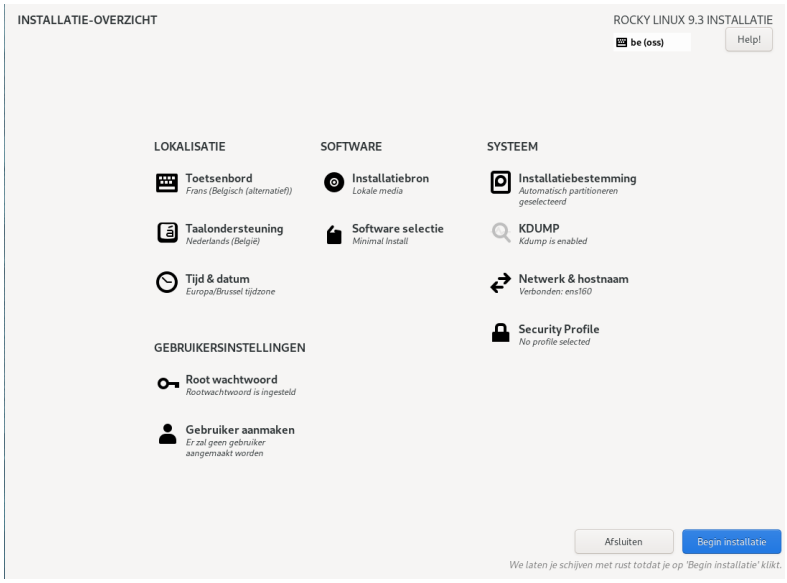
4 Rocky9

Een belangrijke eis van het project was het gebruik van een Rocky-machine in plaats van Debian of Ubuntu. Dit bleek soms een uitdaging, vooral bij het gebruik van tools zoals BloodHound en bij het installeren van Security Onion. Desondanks diende dit als een solide startpunt.

We zijn begonnen met het maken van een Rocky OVA voor onze groep zodat we gemakkelijk testomgevingen konden opzetten.

4.1 Instalatie

De installatie van Rocky zelf is zeer eenvoudig met gui voor de minimal install.



Dankzij de eenvoudige installatie en het gebruik van het OVF Tool had onze groep snel een OVA die we gedurende het project konden gebruiken. Uiteindelijk zijn we overgestapt naar de infrastructuur die was opgezet door groep 1.

5 Wazuh

Voor het vak Project Analysis hebben we de blueprint opgesteld voor het Claritas-project. Hierbij werd aangegeven dat we Wazuh zouden gebruiken voor monitoring, wat als startpunt diende terwijl we wachten op de tenant.

Wazuh is een open-source beveiligingsmonitoringplatform dat organisaties helpt bij het detecteren van bedreigingen, reageren op incidenten en beheren van

nalevingsvereisten. Het biedt uitgebreide functies voor het monitoren van beveiligingsgebeurtenissen en het analyseren van logbestanden om potentiële risico's te identificeren en te mitigeren. Het is een relatief eenvoudig SIEM dat met behulp van de ELK-stack zijn logs genereert en analyseert. Deze SIEM is zeer lichtgewicht en integreerbaar met verschillende andere technologieën. Het is echter belangrijk op te merken dat Wazuh een beperkte schaalbaarheid heeft en dat het soms lastig kan zijn om de juiste regels te creëren. Als een host-based SIEM richt Wazuh zich op het bewaken en analyseren van de individuele hosts/endpoints binnen een netwerk.

5.1 Instalatie

Wazuh-installatiescript en execute

```
[root@localhost ~]# curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh && sudo bash ./wazuh-i
nstall.sh -a -i
```

De output toont de toegangscertificaten voor:

Wazuh webinterface met het IP-adres van de machine.
Bij het openen van het Wazuh-dashboard voor de eerste keer kan je browser een waarschuwingsbericht tonen waarin staat dat het certificaat niet is uitgegeven door een vertrouwde autoriteit. Dit is normaal. Je kunt het certificaat accepteren als uitzondering of het systeem configureren om een certificaat van een vertrouwde autoriteit te gebruiken.

De wachtwoorden voor alle Wazuh-indexer- en Wazuh-API-gebruikers zijn te vinden in het bestand wazuh-passwords.txt.

```
[root@localhost ~]# sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

5.2 Alternatief

Als anternatief kan men de ova gebruiken van wazuh

https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html

5.3 Gebruik

Omdat de SIEM-groep heeft besloten om Security Onion te gebruiken, Hierdoor zijn we gestopt met Wazuh. Dit besluit is genomen vanwege verschillende factoren die Security Onion tot een betere keuze maken voor het project.

Netwerkmonitoring: Security Onion biedt uitgebreide netwerkmonitoring met tools zoals Suricata en Zeek, die diepgaande netwerkverkeersanalyse mogelijk maken.

Volledig platform: Het is een alles-in-één platform voor inbraakdetectie, logbeheer en forensische analyse, wat handig is voor organisaties die een complete beveiligingsoplossing zoeken.

Visualisatie: Het gebruik van Elasticsearch, Logstash en Kibana in Security Onion biedt krachtige visualisatiemogelijkheden voor beveiligingsdata.

Gebruiksvriendelijkheid: Het biedt een eenvoudige setup en kan worden opgeschaald voor verschillende netwerkgroottes, waardoor het flexibel is voor diverse behoeften.

Kortom, Security Onion is ideaal voor uitgebreide netwerkbeveiliging en visualisatie, terwijl Wazuh beter is voor endpoint monitoring en SIEM-functionaliteiten.

6 Security onion

Security Onion is een open-source Linux-distributie die wordt gebruikt voor netwerkbeveiligingsmonitoring, threat hunting en logbeheer. Het integreert

verschillende krachtige tools zoals Suricata, Zeek, Logstash, Elasticsearch en Kibana om organisaties te helpen bij het bewaken en beveiligen van hun netwerkactiviteiten. Het systeem biedt gebruiksvriendelijke interfaces voor waarschuwingen, dashboards en het vastleggen van pakketten, en kan worden ingezet in zowel kleine als grote netwerkomgevingen.
Lokaal hebben we security onion niet opgezet. De hardware requirements waren hoog met

- 16 GB RAM minimum
- 200 GB Opslag minimum
- 4 CPU kernen minimum

6.1 Instalatie

1. Start Installation:
   Select "Yes" to start the installation process.
   Choose Installation Type:
   Select "Install Security Onion."
   Choose "Standalone" installation.
2. Select Setup Type:
   Choose "Standard" setup.
3. Agreement and FQDN:
   Accept the license agreement.
   Set a Fully Qualified Domain Name (FQDN) for your system.
4. Network Configuration:
   Select a network interface card (NIC) for management.
   Configure a static IP address, subnet mask, and gateway.
   Set DNS servers and DNS suffix.
5. Internet Access Configuration:
   Opt for direct internet access.
6. Set Root Credentials:
   Enter and confirm the root email and password.
7. Access Configuration:
   Configure access IP ranges (CIDR notation) to define which IP ranges can access the web interface.
8. Finalize Installation:
   Review your settings and confirm to start the installation process.

9. Reboot System:
   After installation completes, remove the USB and reboot the system.
10. Post-Installation:
    Access the Security Onion web interface by navigating to https://<your- ip> in a web browser.

7 Informatie uit Entra ID verkrijgen.

We zijn begonnen met het maken van een applicatie op een Entra ID-account (Azure Active Directory) dat we hebben ontvangen. Het was niet zo duidelijk hoe alles werkte omdat we geen extra uitleg kregen, maar het is ons gelukt om een applicatie te registreren en de benodigde informatie over onze tenant te verkrijgen. Het registreren van een applicatie in Entra ID is een essentiële stap om ervoor te zorgen dat onze applicatie kan communiceren met Microsoft 365-services. Dit proces omvatte het configureren van de juiste machtigingen en het verkrijgen van de client-id en tenant-id die we nodig hadden voor authenticatie.

7.1 Tools

7.1.1 Azure CLI

Azure CLI is een command-line tool waarmee we Microsoft 365 Entra ID (Azure Active Directory) kunnen beheren. Het biedt een breed scala aan commando's voor het beheren van AD-resources zoals gebruikers, groepen en toepassingen. Azure CLI is platformonafhankelijk en kan worden gebruikt op Windows, macOS en Linux, wat ideaal is voor ons team omdat we bekend zijn met shell-scripting en het Unix/Linux-ecosysteem. Het stelt ons in staat om Entra ID-resources via de opdrachtregel te beheren en herhalende taken te automatiseren met shell-scripts. Dit is vooral handig voor het snel verzamelen van beveiligingsinformatie en andere data uit Azure AD.

7.1.2 Azure PowerShell

Azure PowerShell is een set cmdlets voor het beheren van Microsoft 365 Entra ID (Azure Active Directory) vanuit de PowerShell-omgeving. Het maakt gebruik van een objectgerichte benadering, wat krachtig is voor het beheren van complexe configuraties en het uitvoeren van geavanceerde scriptingtaken. Hoewel we niet bekend zijn met PowerShell, biedt Azure PowerShell een robuuste set van tools die ons in staat stelt om AD-resources efficiënt te beheren. Het biedt integratie met andere Windows-tools en -services, wat het geschikt maakt voor geavanceerde automatisering en configuratiebeheer. Dit maakt het eenvoudiger voor ons om gedetailleerde beveiligingsinformatie uit Azure AD te halen en te integreren met andere systemen.

7.1.3 Microsoft Graph API

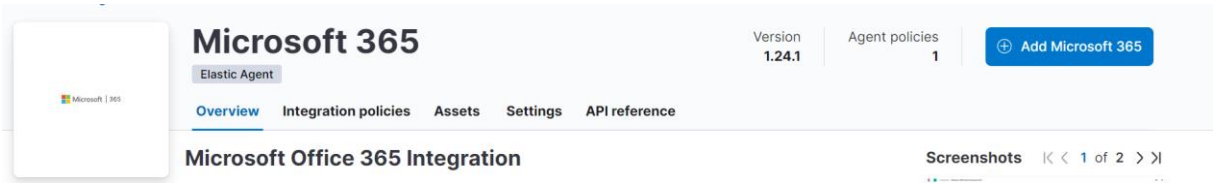
Microsoft Graph API is een RESTful web-API die ons toegang biedt tot een breed scala aan Microsoft Cloud service resources, waaronder Microsoft 365 Entra ID (Azure Active Directory). Het biedt een uniforme manier om te communiceren met verschillende Microsoft-services zoals Microsoft 365. Microsoft Graph API stelt ons in staat om toegang te krijgen tot en beheer te hebben over AD-bronnen via een RESTful API. Dit maakt het mogelijk voor ons om specifieke beveiligingsinformatie uit Azure AD te extraheren en te gebruiken in andere programma's voor verdere verwerking en analyse.

7.1.4 Python Scriptjes

We gebruiken Python om beveiligingsinformatie uit Microsoft 365 Entra ID (Azure Active Directory) te halen en te integreren met elasticsearch. Met Python kunnen we diverse taken uitvoeren, zoals het ophalen van gegevens via de Microsoft Graph API, het verwerken van deze gegevens en het opslaan ervan in Elasticsearch voor verdere analyse.

7.1.5 Elasticsearch integratie & Kibana

Microsoft 365-integratie is al ingebouwd in ons project, en met de eenvoudige configuratie en registratie van een applicatie op Entra ID werkt het prima out of the box. Het doel is niet om de meest complexe software en methoden te gebruiken die er zijn, maar om het zo simpel mogelijk te houden en ervoor te zorgen dat het werkt.



We hebben Kibana gebruikt dat wordt geleverd met Elasticsearch om datavisualisaties te maken zodat we de gegevens kunnen bekijken. Met Kibana kunnen we ook een aangepast dashboard maken waarbij we panels maken met behulp van een lens. Dit betekent dat we gegevens kunnen presenteren in tabel- of grafiekvorm waarbij we gebruik maken van dataviews om de juiste velden te selecteren die we willen tonen in de lens.

7.1.6 Gekozen tools

7.1.6.1 Microsoft Graph API

Daarnaast gebruiken we de Microsoft Graph API om extra gegevens op te halen die niet direct geïntegreerd zijn in onze Elasticsearch.

7.1.6.2 Python Scriptjes

De API kan niet direct communiceren met Elasticsearch. Daarom hebben we besloten om een populaire programmeertaal te gebruiken om ervoor te zorgen dat de informatie correct en naar het juiste programma wordt verzonden.

7.1.6.3 Elasticsearch & Kibana

We hebben gekozen voor Elasticsearch en Kibana om de data te visualiseren. Als we andere technologieën hadden willen gebruiken dan hadden we dubbel werk gedaan van het SIEM team.

7.1.7 Niet gebruikte tools

In het begin hebben we geprobeerd Azure CLI en Azure PowerShell te gebruiken in plaats van Python en de Microsoft Graph API. De algemene werking van beide tools werd niet positief ervaren door ons team. We liepen herhaaldelijk tegen problemen aan en hebben veel tijd verloren door het gebruik ervan met foutmeldingen die we niet konden oplossen en meer. Bovendien was het installeren van extra pakketten om PowerShell-commandos uit te voeren niet eenvoudig omdat we op Rocky Linux 9 werken waar standaard geen PowerShell beschikbaar is.

8 Active directory

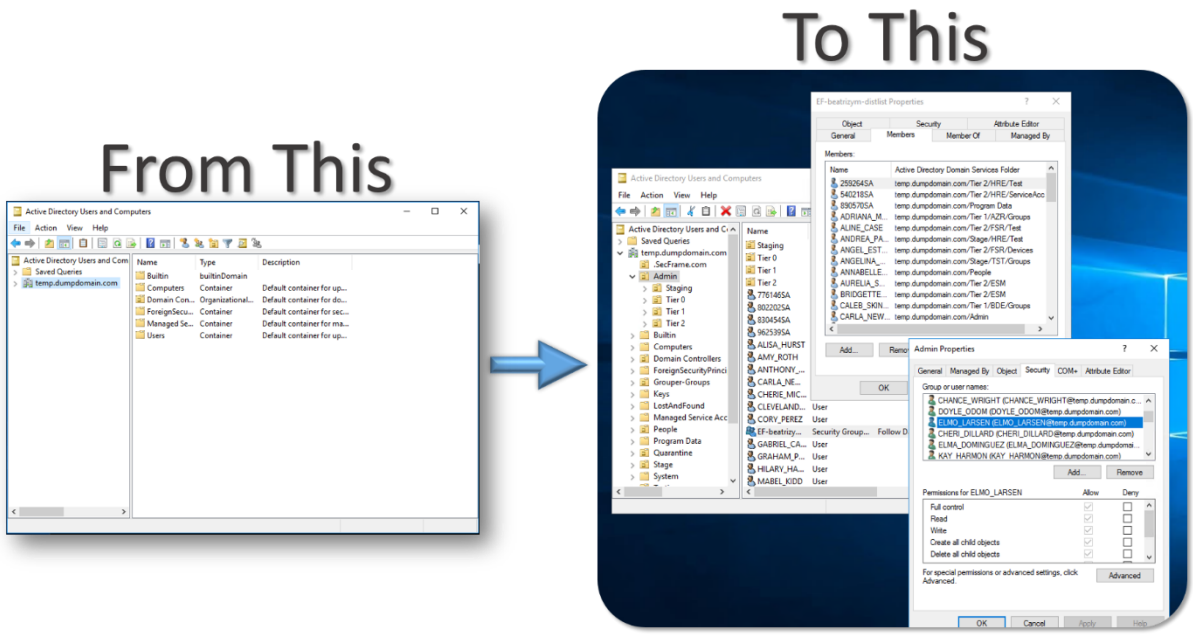
Windows Server Active Directory (AD) is een directoryservice van Microsoft die netwerkbeheer vergemakkelijkt door gebruikers, computers en andere apparaten binnen een netwerk te organiseren en te beheren. Het centrale onderdeel, Active Directory Domain Services (AD DS), slaat gegevens op en beheert communicatie tussen gebruikers en domeinen, wat zorgt voor gecentraliseerd beheer en verbeterde beveiliging.

Active Directory stelt beheerders in staat om netwerkbronnen efficiënt te beheren en biedt gebruikers een vereenvoudigde inlogervaring met een enkele login voor toegang tot alle toegestane bronnen. Het wordt gebruikt voor het beheren van

gebruikers en groepen, het verlenen van netwerktoegang en het afdwingen van beveiligingsinstellingen en configuraties via groepsbeleid, wat de algehele productiviteit en beveiliging binnen een organisatie verbetert.

8.1 BadBlood

BadBlood is een testtool ontworpen om een Active Directory-omgeving te vullen met willekeurige gebruikers, groepen en andere objecten. Dit helpt beheerders en beveiligingsprofessionals om de prestaties en beveiliging van hun Active Directory-infrastructuur te testen en verbeteren door een realistische, maar veilige, simulatie van een echte netwerkomgeving te creëren.



8.1.1 Installatie

Requirements:

Domain Admin and Schema Admin permissions

Active Directory Powershell Installed

On Windows:

“git clone https://github.com/davidprowe/badblood.git””

“./badblood/invoke-badblood.ps1”

8.2 Sharphound

SharpHound is een dataverzameltool die deel uitmaakt van het BloodHound-project. Het verzamelt uitgebreide informatie over een Active Directory-omgeving, waaronder gebruikers, groepen, toestemmingen, sessies en relaties. SharpHound gebruikt verschillende methoden om gegevens te verzamelen, zoals LDAP-query's, SMB-verzoeken en Windows Management Instrumentation (WMI). Deze verzamelde gegevens worden vervolgens geëxporteerd naar een database die door BloodHound kan worden geanalyseerd om inzicht te krijgen in de netwerkstructuur en potentiële beveiligingsrisico's.

8.2.1 Installatie

Voor de instalatie van shatphound moet de windows firewall and virus detection worden uitgezet.

1. Script:
   Download het script van de bloodhound repo of clone the repo
   https://github.com/BloodHoundAD/BloodHound/tree/master/Collectors

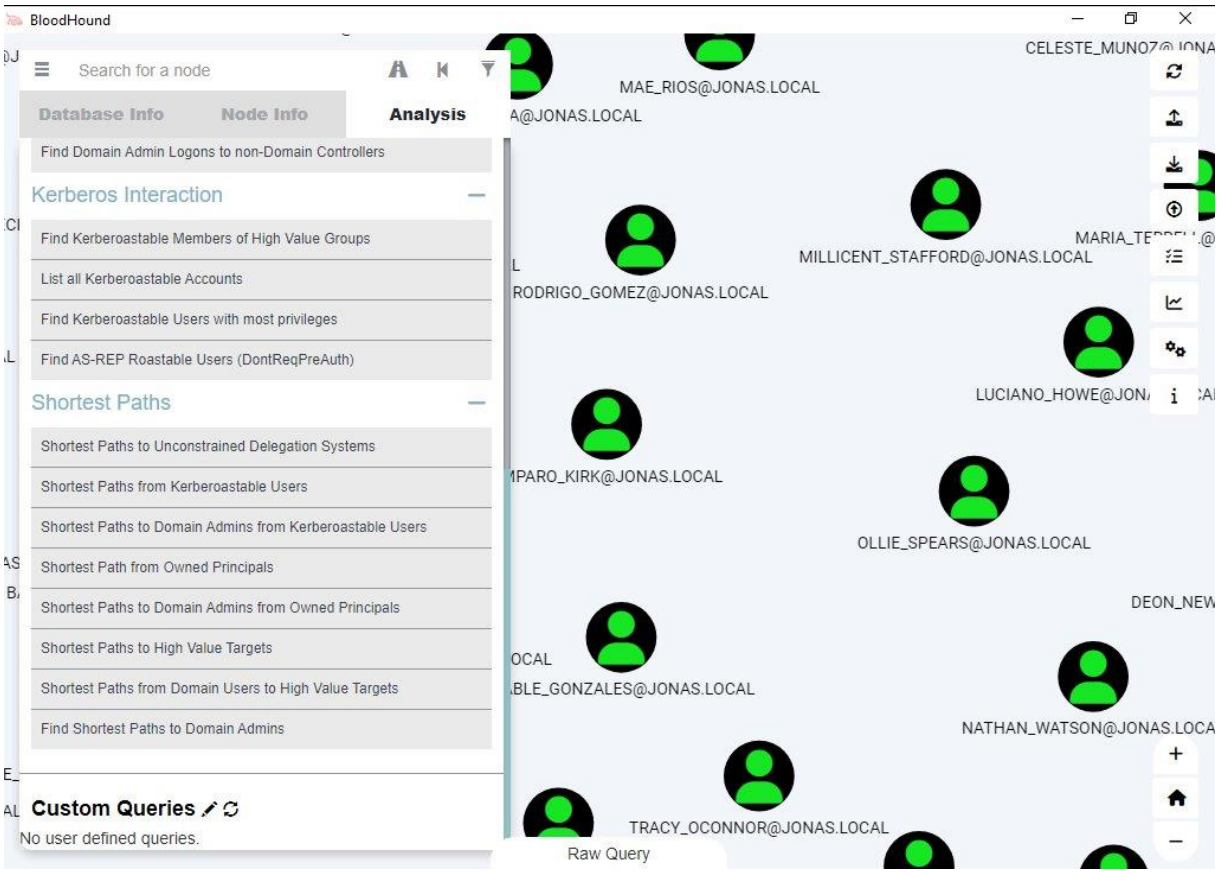
2. Running:
   Run het script vna sharphound.
   “SharpHound.exe”
   Er zijn geen flags voor nodig

   Het script zal een zipfile geven met de data van de Active Directory

20240413172551_computers.json	JSON File	8 KB	No
20240413172551_containers.json	JSON File	2 KB	No
20240413172551_domains.json	JSON File	1 KB	No
20240413172551_gpos.json	JSON File	1 KB	No
20240413172551_groups.json	JSON File	79 KB	No
20240413172551_ous.json	JSON File	28 KB	No
20240413172551_users.json	JSON File	146 KB	No

8.3 Bloodhound

BloodHound is een grafische tool die de door SharpHound verzamelde gegevens gebruikt om de structuur en relaties binnen een Active Directory-omgeving te visualiseren. Het maakt gebruik van grafentheorie om complexe netwerken van gebruikers en toestemmingen inzichtelijk te maken. BloodHound helpt beveiligingsprofessionals om potentiële aanvalspaden te identificeren, zoals privilege-escalatieroutes, die aanvallers zouden kunnen gebruiken om toegang te krijgen tot gevoelige delen van het netwerk. Door deze kwetsbaarheden te identificeren, kunnen organisaties maatregelen nemen om hun beveiliging te verbeteren.



8.3.1 Installatie

De basisinstallatie van BloodHound op een lokale machine is vrij simpel.

1. Clone de repository:

    git clone https://github.com/BloodHoundAD/BloodHound.git

2. In de `example` map staat het `docker-compose.yml` bestand.

3. Start de Docker-compose:

    docker compose up -d

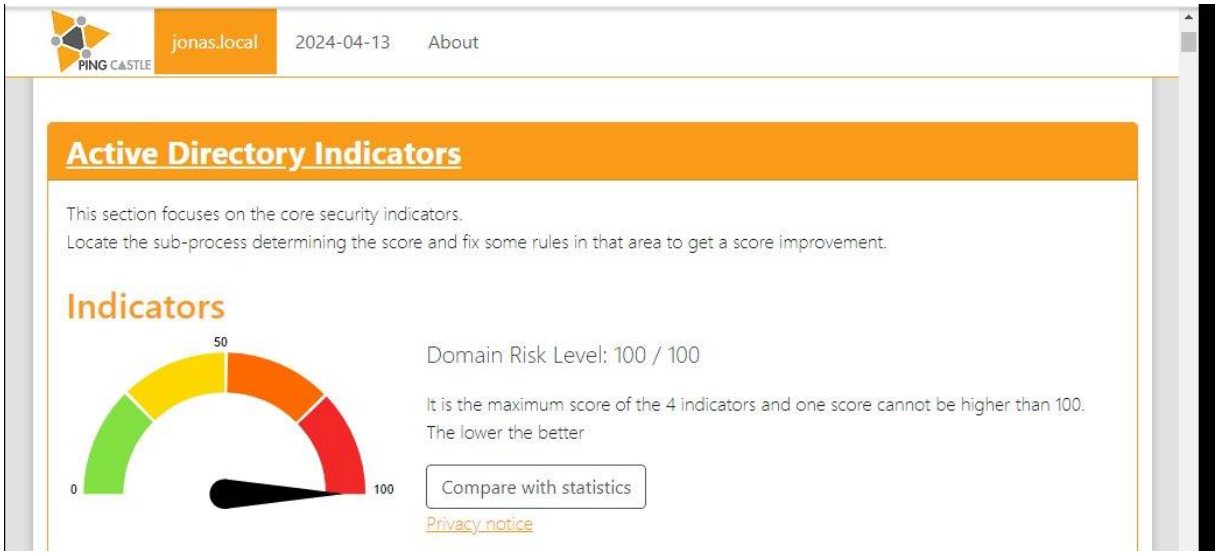
4. Kopieer het gegenereerde wachtwoord. Het BloodHound-dashboard zal beschikbaar zijn op het IP-adres van de machine en poort 8000.

8.3.2 Probleem

Voor het opzetten van BloodHound in onze omgeving moeten er poorten worden aangepast in de .env-bestand. Aangezien we BloodHound niet zoals bedoeld gebruiken, kunnen we geen bestanden uploaden om deze te bekijken.

8.4 Pingcastle

PingCastle is een beveiligingstool die specifiek is ontworpen om de veiligheid van een Active Directory-omgeving te beoordelen. Het voert een uitgebreide scan uit en analyseert verschillende aspecten van de AD-omgeving, zoals configuraties, zwakke punten en naleving van best practices. Na de scan genereert PingCastle een gedetailleerd rapport met scores en aanbevelingen om de beveiliging te verbeteren. Dit rapport biedt inzichten in potentiële risico's en geeft concrete adviezen over hoe deze risico's kunnen worden gemitigeerd, waardoor de algehele veiligheid van de AD-infrastructuur wordt versterkt.



9 Azurehound

AzureHound is een tool die deel uitmaakt van het BloodHound-project, specifiek gericht op het verzamelen en analyseren van gegevens binnen Microsoft Azure-omgevingen. Net als SharpHound voor on-premises Active Directory, verzamelt AzureHound gegevens over gebruikers, groepen, toestemmingen, rollen en relaties in Azure Active Directory (Azure AD).

Gegevensverzameling: AzureHound verzamelt informatie over Azure AD-omgevingen, inclusief details over gebruikersrollen, rechten, en de toewijzing van machtigingen. Het maakt gebruik van de Azure AD Graph API en de Microsoft Graph API om deze gegevens te verkrijgen.
Analyseren van Aanvalspaden: De verzamelde gegevens worden geanalyseerd met BloodHound om potentiële aanvalspaden binnen de Azure-omgeving te identificeren. Dit helpt beveiligingsprofessionals om kwetsbaarheden en misconfiguraties te ontdekken die kunnen leiden tot privilege-escalatie of onbevoegde toegang.
Visualisatie: De gegevens die door AzureHound zijn verzameld, worden gevisualiseerd in BloodHound, waardoor een grafische weergave van de netwerkstructuur en relaties binnen Azure AD wordt gecreëerd. Dit maakt het eenvoudiger om complexe beveiligingsproblemen te begrijpen en aan te pakken.

9.1.1 Installatie

1. Download de zip:
   https://github.com/BloodHoundAD/AzureHound/releases/
2. Execute het scipt met flags:
   “.\azurehound.exe list -u `"$AdminUsername`" -p `"$AdminPassword`" -t `"$TenantId`" -a `"$ClientId`" -s `"$SecretValue`" az-ad -o ` " $ downloadPath\azure-output.json`""

   Dit met de respectievele account, tenant id, en secrets.

10 Scripts

10.1 Python

Het eerste script creëert een index template met hardcoded instellingen en creëert ook een datastream om ervoor te zorgen dat beide met elkaar kunnen werken.

We gebruiken Python-scripts als volgt: Eerst lezen we een configuratiebestand met IDs en geheimen en slaan we deze op in een variabele. Vervolgens zorgt het script ervoor dat we een POST-verzoek sturen om een token op te halen dat actief is. Met behulp van dat token en een URL kunnen we data uit een tenant ID ophalen van een bepaald endpoint dat in de URL staat. Ten slotte halen we de benodigde informatie op en voegen deze toe aan de datastream met behulp van de Elasticsearch-module.

10.2 Powershell

Het powershellscript automatiseert het downloaden, uitpakken en uitvoeren van AzureHound, SharpHound en PingCastle, en schakelt tijdelijk de Real-Time Protection van Windows Defender uit om eventuele interferentie te voorkomen. Na voltooiing wordt Windows Defender weer ingeschakeld.

10.3 Bash

Een script automatiseert het proces van het kopiëren van meerdere bestanden van een externe machine naar een lokale machine, door gebruik te maken van de `scp`-commandoregeltool in combinatie met `sshpass` voor wachtwoordauthenticatie.
Dit script zal de zip file van azurehound en sharphound en de html van pingcastle pullen.

```
#!/bin/bash

USER="Administrator"
PASSWORD="VMWare@AP"
HOST="10.180.10.1"
REMOTE_PATH="/C:/Users/Administrator/Desktop"
LOCAL_PATH="/home/clari-group6"
FILES=("20240512212147_Bloodhound.zip","ad_hc_project.local.html")

for FILE in "${FILES[@]}"; do
        sshpass -p "$PASSWORD" scp "$USER@$HOST:$REMOTE_PATH/$FILE" "$LOCAL_PATH"
done
```

10.4 HTTP

Het HTTP-script wordt gebruikt samen met crontab om het gekopieerde PingCastle-bestand te laten zien op de machine op poort 9080

11 Nog toetevoegen

Color coding voor values die niet veilig zijn. In een dashboard tonen we bv rood als die niet veilig zijn en groen als die wel veilig zijn.
Scriptjes met SSL versturen.

TrevorSpray is een tool voor pentesting en beveiligingsonderzoek, gericht op spray-aanvallen op Active Directory-omgevingen. Een spray-aanval, of password spraying, is een brute force-aanval waarbij een klein aantal veelgebruikte wachtwoorden wordt geprobeerd op veel accounts, in plaats van een account met veel verschillende wachtwoorden. Dit maakt het moeilijker voor beveiligingssystemen om de aanval te detecteren vanwege het lage aantal mislukte inlogpogingen per account.

TrevorSpray automatiseert dit proces door veelgebruikte wachtwoorden tegen alle gebruikersaccounts in een Active Directory-omgeving te testen. Het doel is om zwakke wachtwoorden en kwetsbare accounts op te sporen, zodat beveiligingsprofessionals deze problemen kunnen verhelpen voordat kwaadwillenden er misbruik van maken. Het is een nuttige tool voor het identificeren van beveiligingslekken en het versterken van de wachtwoordbeveiliging binnen een organisatie.

12 Bronnen

https://learn.microsoft.com/en-us/cli/azure/install-azure-cli

https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id

https://rockylinux.org/download

https://documentation.wazuh.com/current/getting-started/index.html

https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html

https://github.com/davidprowe/BadBlood?tab=readme-ov-file

https://bloodhound.readthedocs.io/en/latest/data-collection/sharphound.html

https://learn.microsoft.com/en-us/graph/use-the-api

https://learn.microsoft.com/en-us/entra/fundamentals/how-to-find-tenant

https://learn.microsoft.com/en-us/entra/identity/users/groups-settings-v2-cmdlets

https://learn.microsoft.com/en-us/cli/azure/install-azure-cli

https://learn.microsoft.com/en-us/powershell/azure/install-azure-powershell?view=azps-12.0.0

https://www.pingcastle.com/