ACTWISE

Internship assignment

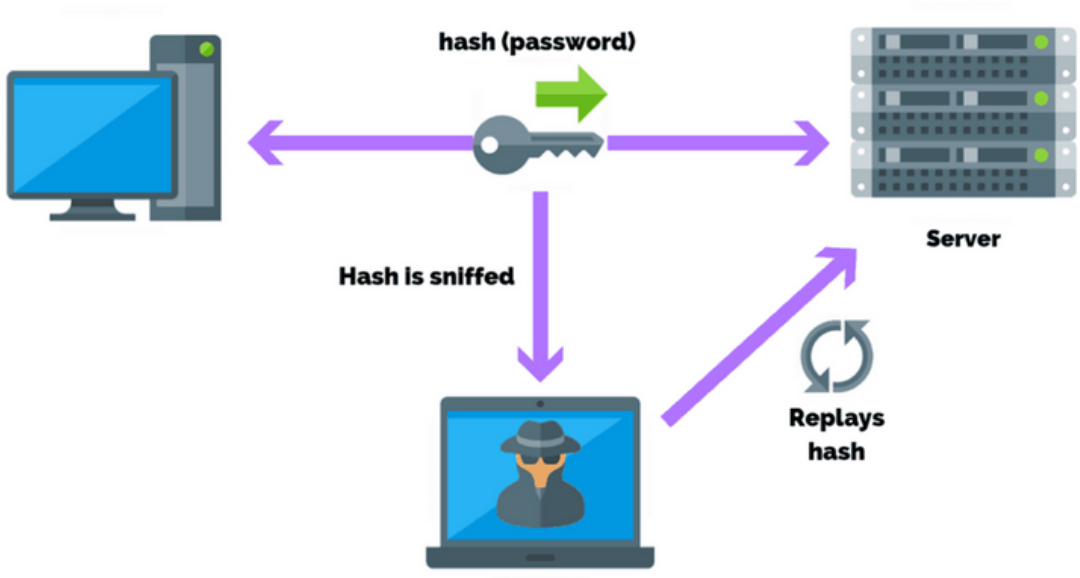
Defend against Cyber Attacks: Pass-the-Hash Attack

Contact
Cindy Van den Hoecke
careers@is4u.be

ActWise NV
Veldkant 33A
2550 Kontich
België

Omschrijving

Pass-the-Hash is een hackingtechniek waarmee aanvallers kunnen inloggen op een server door gebruik te maken van gestolen hashwaarden. Het doel van deze stageopdracht is om de effecten van een Privileged Account Management (PAM) oplossing te onderzoeken tegen dergelijke aanvallen. We willen ook de impact van verschillende configuraties van de PAM-oplossing op de bescherming tegen deze aanvallen in kaart brengen.



Om dit in kaart te kunnen brengen ga je met deze opdracht eerst een onbeveiligde omgeving opzetten die je nadien gaat aanvallen met een Pass-The-Hash aanval.
Nadien installeer je een PAM oplossing waarmee je een omgeving beveiligd. De PAM oplossing die voor deze opdracht gebruikt gaat worden is CyberArk PAM. CyberArk PAM is een vooraanstaande oplossing in de wereld van Privileged Account Management, ontworpen om de beveiliging van organisaties te versterken door het beheer en de bescherming van geprivilegieerde accounts en toegangsrechten. PAM speelt een cruciale rol in het minimaliseren van cyberdreigingen en het beschermen van kritieke systemen en gevoelige gegevens.

Magic Quadrant

Figure 1: Magic Quadrant for Privileged Access Management

Source: Gartner (July 2022)

Oplevering:

Er zal gevraagd worden om volgende deliverables op te leveren:

1. Een onbeveiligde omgeving opzetten met een Active Directory (AD) en enkele test servers.
2. Verschillende Pass-the-Hash aanvallen uitvoeren op de onbeveiligde omgeving om kwetsbaarheden te identificeren.
3. CyberArk PAM implementeren als beveiligingsoplossing voor de omgeving.
4. De PAM-oplossing configureren en optimaliseren voor de beveiligde omgeving.
5. Meerdere Pass-the-Hash aanvallen uitvoeren op de beveiligde omgeving met verschillende PAM-configuraties.
6. Een vergelijking maken tussen de resultaten van de aanvallen en de effecten van diverse PAM-configuraties op de algehele veiligheid van de omgeving.

Mogelijke uitbreidingen:

1. Het opsporen van actieve Pass-The-Hash aanvallen met de PAM oplossing.

Projectmethodologie

ActWise hanteert voor haar projecten agile projectmethodologieën, zoals XP en SCRUM. Het project dat hierboven is beschreven, volgt dezelfde aanpak. Deze methodologieën richten zich op het waarborgen van de kwaliteit van softwareoplossingen. Dit wordt bereikt door het project op te splitsen in kortere iteraties en door middel van intensieve communicatie binnen en buiten het projectteam. De nadruk op intensieve communicatie is een intrinsiek kenmerk van agile, wat resulteert in een diepgaande begeleiding tijdens de stageperiode.