Voorstel Eindproject:
Cyber Attack Simulator

Probleemstelling

Het opzetten en uitvoeren van realistische cybersecurity-oefeningen is vandaag vaak een moeizaam proces. Het handmatig aanmaken van testomgevingen en aanvalsscenario's kost veel tijd, vraagt technische kennis en leidt vaak tot inconsistente resultaten.
In veel omgevingen gebeurt security testing daardoor te weinig of zonder herhaalbaarheid, wat de kwaliteit van detectie- en responsprocedures beperkt.

Om dit aan te pakken, is er nood aan een geautomatiseerde, reproduceerbare en schaalbare oplossing die testomgevingen kan opzetten, aanvallen kan simuleren en resultaten kan verzamelen zonder manuele tussenkomst.

De belangrijkste behoeften zijn:

1. Automatisch opzetten en beheren van virtuele machines en netwerkomgevingen.
2. Scriptmatig uitvoeren van verschillende aanvalsscenario's met oplopende moeilijkheid.
3. Verzamelen en centraliseren van logs en detectiegegevens.
4. Ondersteuning voor parallelle uitvoering om tijd te besparen.
5. Duidelijke en reproduceerbare rapportage van testresultaten.

Doelstelling

Het doel van dit project is om een PowerShell-gebaseerde Cyber Attack Simulator te ontwikkelen die het volledige testproces automatiseert: van de creatie van virtuele machines tot de uitvoering van aanvallen en de rapportage van resultaten.
De simulator ondersteunt meerdere moeilijkheidsniveaus en maakt het mogelijk om verschillende scenario's tegelijk te draaien. Zo kunnen securityteams of studenten efficiënt en gecontroleerd oefenen op detectie en respons, zonder risico voor echte systemen.

Minimal Viable Product (MVP)

Het MVP bestaat uit een werkend PowerShell-framework met de volgende functies:

1. **VM-automatisering**
    - Automatisch opzetten en configureren van virtuele machines via Hyper-V of een ander platform.
2. **Basale aanvalsscenario's**
    - Ten minste drie gescripte aanvallen, zoals een brute-force login, een eenvoudige privilege escalation en een netwerk-scan.
3. **Levelstructuur**
    - Een systeem om moeilijkheidsniveaus te definiëren waarbij elk hoger level extra aanvallen of complexiteit toevoegt.
4. **Logging en verzameling**
    - Logs per scenario worden centraal opgeslagen in gestructureerde bestanden (CSV of JSON).
5. **Parallelle uitvoering**
    - Meerdere scenario's of VM-sets kunnen tegelijk draaien via Start-Job of Runspaces.
6. **Configuratie via parameters**
    - De gebruiker kan instellingen aanpassen zoals aantal VM's, type aanvallen of moeilijkheidsniveau.
7. **Validaties en foutafhandeling**
    - Het systeem controleert afhankelijkheden, middelen en invoer. Fouten worden opgevangen en hersteld waar mogelijk.
8. **Interactiviteit**
    - Indien configuratie ontbreekt, kan de gebruiker input geven via prompts.
9. **Rapportage**
    - Een overzichtsrapport (CSV of eenvoudige HTML) toont de resultaten en detecties per run.
10. **Testing met Pester**
    - Kernfuncties zoals VM-aanmaak, scenario-executie en logging worden getest met PowerShell Pester.

Extra Functionaliteiten

Om het project verder te verdiepen en beter te laten scoren:

1. Geavanceerde aanvalssimulaties zoals lateral movement, ransomware-simulaties of phishing-emulatie.
2. Integratie met SIEM-systemen (Splunk, Azure Sentinel) voor realtime loganalyse.
3. Professionele rapportage in HTML of PDF, met grafieken en detectiepercentages.
4. Eenvoudige GUI of webinterface voor het beheren en starten van simulaties.
5. Cloudondersteuning voor automatische deployment in Azure of AWS.
6. Scenario-bibliotheek met versiebeheer.
7. Educatieve modus die uitleg geeft over de gebruikte aanvalstechnieken en mitigaties.

Argumentatie volgens rubric

Analyse

Het project vertrekt vanuit een realistische nood in cybersecurity: het gebrek aan schaalbare en herhaalbare testmogelijkheden. De bestaande werkwijze (handmatig testen) wordt geanalyseerd en omgezet in een geautomatiseerde aanpak. Dit toont inzicht in de context en probleemstelling, zoals de rubric vereist.

Design

Het ontwerp combineert PowerShell met virtualisatie (Hyper-V/VMware) en modulaire scenario's.
De structuur is bewust opgesplitst in provisioning, scenario-executie en logging, wat uitbreidbaarheid en onderhoud bevordert.
De keuze voor PowerShell als kerntechnologie is logisch: het biedt directe integratie met Windows en API's, en ondersteunt automatisering van meerdere lagen.

Kennisverwerving

Het project vereist technische verdieping in PowerShell, netwerkbeheer, aanvalstechnieken en loganalyse.
Integraties met externe frameworks (zoals MITRE ATT&CK) en SIEM-oplossingen tonen een sterke leercurve, wat perfect aansluit bij de rubricvereisten voor kennisontwikkeling.

Usability

De simulator is ontworpen met gebruiksgemak in gedachten: een eenvoudige CLI en optionele GUI maken het toegankelijk voor zowel studenten als professionals.
Door configuratie via parameters en templates kan de tool flexibel worden ingezet in verschillende omgevingen.

Robustheid

De tool bevat foutafhandeling, resource-checks en logging die zorgen voor stabiliteit.
Bij fouten wordt feedback gegeven en worden herstelpogingen uitgevoerd.
Dit garandeert betrouwbaarheid en fouttolerantie, belangrijke punten in de rubric.

Uitbreidbaarheid

De modulaire structuur laat toe om nieuwe scenario's en aanvalstypen toe te voegen zonder de kern aan te passen.
Gebruik van parameterbestanden en plug-ins maakt uitbreiding eenvoudig en schaalbaar.

Best Practices en Structuur

De code volgt PowerShell best practices: duidelijke functies, consistente naamgeving en commentaar.
Door de scheiding tussen provisioning, aanval en rapportage blijft de code onderhoudbaar en transparant.

Testing

Met Pester worden de belangrijkste onderdelen getest, zoals VM-aanmaak en logging.
CI/CD-integratie (zoals GitHub Actions) kan later gebruikt worden voor automatische regressietests.
Zo wordt de kwaliteit van de code gewaarborgd.

Eindresultaat

Het eindproduct is een schaalbare en reproduceerbare Cyber Attack Simulator in PowerShell die realistische aanvallen uitvoert, detecties test en resultaten overzichtelijk rapporteert.
De simulator is modulair, stabiel en gebruiksvriendelijk, en vormt een bruikbaar hulpmiddel voor zowel onderwijs als professionele securitytraining.