Opdracht NPE

CyberSecurity & Virtualisation - 2022-2023

Het doel van deze opdracht is om enerzijds de configuratie van een virtuele omgeving te automatiseren, en anderzijds te experimenteren met het Metasploit framework. Voor dit project werk je in een groep van 2 studenten, en je mag zelf kiezen met wie je samenwerkt.

> **Belangrijk:** Het resultaat van deze opdracht telt mee voor 25% van het eindcijfer voor dit opleidingsonderdeel. Spendeer dus voldoende tijd aan deze opdracht en wacht niet tot het laatste moment om hieraan te beginnen!
>
> Bovendien wordt er geen tweede examenkans georganiseerd. Wanneer een student in de eerste examenkans niet geslaagd was, blijft de beoordeling voor deze evaluatievorm of de afwezigheid voor deze evaluatievorm geldig voor de tweede examenkans.

Voor deze opdracht ga je in eerste instantie op zoek naar een kwetsbaarheid binnen een softwarepakket dat je kan installeren op een **Debian** VM. Hierbij dien je op zoek te gaan naar een code in de publieke CVE databank. De kwetsbaarheid zal je nadien proberen aan te vallen via het Metasploit Framework. Voor deze opdracht is het **niet toegelaten** om gebruik te maken van een Metasploitable VM, je dient dus zelf vanaf scratch een kwetsbare VM aan te maken.

1. Ontwerp en automatisatie virtuele omgeving

Eenmaal je een kwetsbaarheid (*EN: Vulnerability*) en bijhorende code gevonden hebt, ontwerp je een eenvoudige Proof of Concept omgeving binnen VirtualBox, die je zoveel mogelijk probeert te automatiseren. Voor de automatisatie maak je gebruik van `VBoxManage` voor het aanmaken en de configuratie van de virtuele machines, en `bash` scripts voor het installeren van de nodige software op de kwetsbare Debian VM. De aanval zelf via het Metasploit framework (zie deel 2 van deze opdracht) hoef je niet te automatiseren.

Je omgeving moet minstens bestaan uit volgende VMs:

- Eén VM met Debian (met of zonder GUI, kies zelf wat best past), en
- Eén VM met Kali Linux.

Voor beide VMs maak je gebruik van een VDI die je kan downloaden van osboxes.org (https://www.osboxes.org/kali-linux/). De VDIs hoef je niet in te dienen (wij kunnen deze immers zelf downloaden), maar geef in de deployment handleiding (zie verder) wel duidelijk aan welke virtuele disks je gebruikt hebt voor de omgeving. Voor de (kwetsbare) Debian VM hoef je

uiteraard niet de meest recente versie te gebruiken, want de kans bestaat immers dat de kwetsbaarheid dan reeds gepatched is.

Uiteindelijk moeten wij in staat zijn om, na downloaden van de virtuele disks, jouw omgeving volledig na te bootsen aan de hand van de scripts die je gemaakt hebt.

2. Aanval VM vanaf Kali met behulp van het Metasploit Framework

Het tweede deel van de opdracht bestaat uit het aanvallen van de gekozen kwetsbaarheid vanaf je Kali VM. Op de Kali VM is het Metasploit framework reeds geïnstalleerd.

- Alvorens verder te gaan zal je jouw keuze moeten voorleggen aan jouw lector! Selecteer geen triviale dienst, of een dienst die reeds aan bod kwam in de labo's (bv: telnet verkeer kan je eenvoudig sniffen omdat alles plaintext verstuurd wordt).
- Maak gebruik van het Metasploit framework op de Kali VM.
- Zoek uit hoe je de netwerkdienst kan aanvallen, en test dit uit.

Alvorens je te verdiepen in het Metasploit framework, moet je de kwetsbaarheid die je wil aanvallen eerst voorleggen aan jouw lector ter goedkeuring. Gebruik hiervoor het online formulier:

https://forms.microsoft.com/Pages/ResponsePage.aspx?id=DjH3XBoJxUus1ybHIdTMzdLA8hsRkT5BgJ5-6ixc1YxURjFWQlI3NEtFSENDOTFPU0RESlhVNDg5VS4u

> **Belangrijk:** Per groep moet je dit formulier maar één keer invullen, en de deadline hiervoor is **vrijdag 21/04/2023 - 16:00**. Studenten die dit formulier niet indienen krijgen automatisch een score 0 voor dit onderdeel.

3. Indienen resultaat

Voor deze opdracht zal je drie zaken moeten indienen:

- De scripts die je geschreven hebt voor stap 1 (automatiseren VM omgeving).
- Een beknopte deployment handleiding, in PDF, waarin je (in bullet points) omschrijft welke stappen wij moeten uitvoeren om jouw omgeving uit te rollen in VirtualBox met behulp van de scripts.
- Een korte demo-video, waarin je het resultaat van beide stappen kort demonstreert.

In de demo-video toon je enerzijds dat je via jouw script de virtuele omgeving automatisch kan uitrollen, anderzijds demonstreer je kort een aanval op de geselecteerde netwerkdienst vanaf je Kali VM.

De demo-video maak en deel je via Panopto, gebruik hiervoor bij voorkeur de Desktop App (en dus niet de browser-versie).

De maximale lengte van deze video is **10 minuten** (voor beide delen samen). Merk op dat je in de Panopto client eenvoudig een opname kan pauzeren, en dus meerdere opnames samen kan voegen tot 1 video. Je hoeft dus niet alles in 1 keer te filmen: je kan eerst een opname maken van het eerste deel, de opname pauzeren, en later een tweede opname toevoegen voor het tweede deel.

Voorzie voor de demo van het eerste deel (automatisatie via script) 3-4 minuten, de resterende 6-7 minuten kan je gebruiken voor demonstreren van de aanval.

Geef kort uitleg (via microfoon) bij wat je toont, en deel bij voorkeur ook je webcam via Panopto.

Het resultaat dien je in via Chamilo - onderdeel Opdrachten:

- De scripts en de deployment handleiding dien je in als één ZIP-bestand.
- In de commentaar van je inzending kan je de link naar de Panopto video toevoegen.

Deel de Panopto video met alle lectoren die betrokken zijn bij dit onderdeel:

- Thomas Clauwaert - thomas.clauwaert@hogent.be
- Pieter-Jan Maenhaut - pieterjan.maenhaut@hogent.be
- Joeri Van Herreweghe - joeri.vanherreweghe@hogent.be

> **Belangrijk:** Deadline voor indienen van het script en de video is 21/05/2023 23:59. Dit is een strikte deadline, indienen na de deadline is niet toegelaten en zal resulteren in een score 0 voor het onderdeel NPE.