Web application security assessment

Reflectie

Bachelor in de Elektronica-ICT
Cloud & Cybersecurity

Bert Moelans

Academiejaar 2020-2021

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

Inhoudstafel

1 INLEIDING

Voor de eerste keer in mijn opleiding Cloud & Cybersecurity van Thomas More liep ik stage bij een IT-bedrijf. Dit bedrijf was nFuse, gelegen in de Corda Campus in Hasselt. Tijdens deze stage heb ik een PenTest gemaakt en daarbij verschillende fases doorlopen. Daarnaast heb ik gewerkt aan mijn communicatie en presentatie vaardigheden.

In dit document zal dus besproken worden hoe ik deze stage heb ervaren en hoe ik zelf heb gefunctioneerd binnen het bedrijf. Daarbij heb ik ook aan verschillende competenties gewerkt die mij als IT'er nu en in de toekomst van pas zullen komen.

Het eerste deel is een reflectie op inhoudelijk niveau. Hierin wordt uitgelegd wat mijn stage juist inhield en wat dit project nFuse heeft bijgebracht.

In het tweede deel focus ik mij op een persoonlijke reflectie en zal ik mijn beleving van de stage toelichten. Hier worden mijn competenties uitgebreid besproken en geef ik een voorbeeld waarbij ik een persoonlijke groei heb meegemaakt.

2 INHOUDELIJKE REFLECTIE

Mijn stageopdracht was een penetratietest uitvoeren op een kopie van de nFuse-website in een afgesloten omgeving. In het begin heb ik een plan van aanpak opgesteld waarin duidelijk werd dat ik een PenTest zou uitvoeren in verschillende fases.

PenTest fases

De eerste fase was de fase waarin ik alle informatie verzamelde over de site, dit door middel van verschillende tools. Ik gebruikte tools zoals Nmap voor het netwerk te verkennen, maar ook Dirbuster om mappen en bestanden te vinden op de website. Bij het opstellen van de topologie van de site bestudeerde ik “best practices” die ik vond op het internet. Dit zijn manieren waarop netwerken in het beste geval aangesloten kunnen worden.

De tweede fase was de effectieve hacking-fase. Hierin overliep ik de gevonden kwetsbaarheden en zocht ik een manier om deze te gebruiken en zodanig de site te hacken. Dit is ook de fase waarbij ik een CVSS score aan belangrijke kwetsbaarheden gaf. CVSS staat voor “Common Vulnerability Scoring System” en is een manier om kwetsbaarheden een score te geven op 10 over hoe gevaarlijk dat het kan zijn.

De derde fase was het opstellen van een mitigatieplan om deze kwetsbaarheden onschadelijk te maken. Ik legde hier uit hoe je je het best kan wapenen tegen tools zoals nmap en Dirbuster. Daarnaast toonde ik aan dat het updaten van versies enorm belangrijk is. Hoe ouder de versie van bepaalde software, hoe meer kwetsbaarheden het kan bevatten.

De vierde fase was dit mitigatieplan uitvoeren. Deze fase werd afgehandeld door nFuse. Zij gingen aan de slag met mijn handleiding over het beveiligen van de website. Deze handleiding had ik gemaakt in de derde fase.

Daarna kon ik een analyse doen van de beveiligde omgeving in fase 5. Daarbij kwam ik tot de conclusie dat de kwetsbaarheden grotendeels werden opgelost door mijn mitigatieplan.

Wat levert het op voor nFuse?

nFuse heeft door deze PenTest een kijk gekregen op welke tools allemaal gebruikt kunnen worden en op welke vlakken de website kwetsbaarheden vertoont. Hiermee kunnen ze rekening houden bij de toekomstige beveiliging van hun website. Het is vooral belangrijk om deze altijd up-to-date te houden.

Einde van het project?

Ik voerde dit project uit op een vast moment in de tijd. Een bedrijf moet zich echter altijd bewust zijn van de mogelijke gevaren. Deze gevaren kan vinden door regelmatig een PenTest uit te voeren op je eigen infrastructuur. Zo krijg je een goed overzicht van hoe jouw bedrijf is gewapend tegen hackers. Je kan ook zo ver gaan als je wil met een PenTest. Ik heb veel kwetsbaarheden gevonden, maar er zijn altijd manieren om deze te gebruiken bij het hacken, ook al heb ik die niet allemaal gevonden.

Stageopdracht in gebruik genomen?

De PenTest zelf is niet in gebruik genomen, omdat dit ging over een kopie van de nFuse website. De inhoud en methodologie van de PenTest daarentegen zouden wel gebruikt kunnen worden in het later beveiligen van andere websites en omgevingen.

Mijn advies voor nFuse

In de toekomst zou er nog gekeken kunnen worden naar de andere niet onderzochte kwetsbaarheden zoals XSS-aanvallen en SQL-injecties. Deze vond ik met de Owasp ZAP tool, maar heb ik door tijdsgebrek niet volledig kunnen analyseren. Daarnaast zouden ze een maandelijkse PenTest kunnen uitvoeren op de nFuse website. Een andere tip is om de Owasp Top 10 goed te blijven bekijken. Dit is een lijst met kwetsbaarheden voor web applicaties die het meeste impact kunnen hebben op jouw site. De kwetsbaarheid die bovenaan staat is degene die momenteel de meest zware gevolgen kan hebben.

3 PERSOONLIJKE REFLECTIE

Wat heb ik geleerd?

Deze stage bij nFuse was een zeer interessante en leerrijke stage. Ik heb hier niet enkel leren PenTesten, maar ook mijn presentatietechnieken zijn bijgeslepen. Zo gaf ik elke vrijdag een presentatie over wat ik die week had gedaan voor alle medewerkers van nFuse. Ze gaven mij dan feedback waarmee ik dan aan de slag ging voor de volgende keer. Op het einde van de stage hebben ze mij dus ook feedback gegeven over mijn eindpresentatie en dat geeft me een goed gevoel. Ik weet nu dat deze ook is nagekeken door nFuse. Daarnaast waren er ook dagelijks twee “daily standup meetings” waarin verteld werd door elke werknemer wat hij gedaan had en wat de volgende plannen waren.

Waarin ben ik gegroeid?

Ik vind van mezelf dat ik enorm gegroeid ben in het zelfstandig te werk gaan en research doen naar zaken die me onbekend waren. Het grootste deel van de stage deed ik onderzoek naar kwetsbaarheden en hacking mogelijkheden via Google. Hierdoor heb ik enorm veel bijgeleerd en leren werken met zaken die ik voordien niet kende. In de IT is het belangrijk om zelf opzoekwerk te kunnen doen omdat de digitale wereld tegenwoordig altijd verandert. Daardoor ben ik hiermee meer vertrouwd geraakt.

Probleem aanpakken

De eerste presentatie die ik gaf voor nFuse viel niet echt in de smaak. Er werd niet dezelfde lay-out gebruikt, ik kwam zenuwachtig over en mijn foto’s op de dia’s waren veel te groot. Ik ben dus met deze feedback aan de slag gegaan en filmpjes gekeken van TED Talks. Dit is een organisatie die inspirerende mensen aan het woord laat om hun expertise en kennis te delen. Ik leerde hierdoor verschillende presentatietechnieken. De volgende presentatie deed ik zelfs rechtstaand. Dit was iets ongezien en werd meteen als positief ervaren. Ze vonden dat ik elke week interessantere en betere presentaties gaf met meer rust. Dit is een voorbeeld waarin ik enorm ben gegroeid dankzij de mogelijkheid om dit wekelijks te doen.

ITF competenties

Tijdens mijn stage ben ik in aanraking gekomen met verschillende competenties. In de eerste fase van mijn PenTest heb ik dus vooral leren **analyseren**. Ik verzamelde zoveel mogelijk informatie over de website die ik zou hacken. De competentie **realiseren** heb ik voornamelijk leren gebruiken door alles wat ik deed te documenteren. Als ethical hacker is het belangrijk om dit te doen. Je houdt best altijd een log of historiek bij van welke zaken je hebt gedaan zodat je kan aantonen dat je niets verkeerd hebt gedaan als de website zou crashen. Daarnaast heb ik ook bij alle fases realisaties gedaan. Dit gaat van het vinden van informatie (zoals kwetsbaarheden, versienummers van software, …) over de website tot het opstellen van een phishing mail met een link naar een valse website. Daarnaast heb ik ook de competentie **communiceren** bijgeschaafd. In het begin probeerde ik begrippen uit te leggen zonder ze echt goed te begrijpen. Ik heb geleerd om dit niet te doen en eerlijk toe te geven er nog niet zo veel van te kennen.

Projectmatig werken kwam ook aan bod, omdat ik werkte in verschillende fases. Hier was het belangrijk om in te schatten wanneer ik naar een volgende fase kon doorgaan. Uiteindelijk heb ik alle fases kunnen doorlopen dus ben ik hierin geslaagd. De laatste competentie die ik wil bespreken is **professioneel handelen**. Ik heb geleerd zelfstandig maar ook efficiënt te werken met doorzettingsvermogen. In de tweede fase heb ik moeite gehad met hacken. Dit verliep zeker niet van een leien dakje. Toch heb ik doorgezet en deze fase kunnen afronden.

Slotwoord

Mijn stagementoren Rutger en Arif hebben me beide bij de stage ondersteund en altijd gekeken naar mijn noden. Ik was nog niet zo vertrouwd met PenTesting van webapplicaties, maar dat hebben ze in rekening genomen en ze hebben me hierin goed begeleid. Ik merkte al snel dat er heel veel IT kennis en expertise te vinden was bij de werknemers. Mijn stagementoren wisten op al mijn vragen te antwoorden op een begrijpbare manier. Dit is een heel belangrijke eigenschap van een IT'er, vind ik zelf.