Praktikrapport

Koncern it - Københavns Kommune

Navn: Dara Parvizi
Praktikforløb: 22 august - 28 oktober
Vejleder: James Hindsgavl Brink
Skole : Københavns Erhvervsakademi - KEA

Forord

Denne rapport er udarbejdet og skrevet i forbindelse med mit 10 ugers praktikforløb hos KIT som står for Københavns IT Koncern i københavns kommune. Denne Rapport ville klargøre og beskrive hvilke arbejdsopgaver jeg fik for mit praktikforløb, samt hvilke kompetencer og viden jeg fik opnået hos KIT. Denne rapport ville ikke gå i detaljer om virksomheden da der er blev aftalt mellem virksomheden og jeg at der kun tilladt at udarbejde en generel beskrivelse af mit praktikforløb.

Indholdsfortegnelse

Indledning

På 3.semester er det obligatorisk at IT-sikkerhed studerende at være i 10 ugers praktikforløb. Som IT-sikkerhed studerende var det min tur til arbejde hos i en virksomhed samt vise mine evner og færdigheder. Desuden jeg ville få en forståelse af at hvordan en It-sikkerhed afdeling i en virksomhed ville fungerer og er struktureret i den virkelige verden.
Efter masser en ansøgninger, blev jeg indkaldt til en samtale hos københavns kommune da søgte en it-sikkerhed praktikant. Alle it-sikkerhed studerende på 2.semester i en af timerne i klassen blev informeret om at Københavns kommune søger en praktikant. Til første indkaldte samtale gik alt fint som forventet. Der blev snakket om hvad jeg kunne tænkte mig og hvad de kunne tænke sig tænkte at jeg ville lave og i hvilke arbejdsopgaver jeg skulle arbejde med. Efter en uge fik et opkald at jeg har fået praktikpladsen. Praktikforløbet var fra d. 22 august til d.28 oktober.
Jeg skulle være tilstede i IT koncern bygning hvilket er tæt på Fuglebakken st. i 10 uger .På 4.sal var IT koncern afdeling som er en afdeling hvor de arbejder med it-sikkerhed. Jeg skulle se sammen med såkaldte monitorering-holdet. Dette hold var indholdet af 6 mennesker eksklusiv mig. Alle medlemmerne havde erfaring med IT-sikkerhed og havde arbejdet hos Koncern IT længe. Jeg var hos dem 9 uger og den sidste en uger var jeg hos netværk-holdet som lå på 2-sal. i den periode var jeg sammen med medarbejdere på netværk-holdet som vi fik lavet forskellige arbejdsopgaver opgaver.

I denne rapport ville jeg beskrive hvilke arbejdsopgaver jeg arbejdet med i mit praktikforløb hos Koncern IT. Derefter ville jeg beskrive om hvordan jeg har udviklet mig både fagligt og personligt. Til sidst ville jeg konkludere på mit praktikforløb. Jeg har skrevet “Praktiklog” ,som beskriver mine daglige arbejdsrutiner hos Koncern IT, under mit praktikrapport. Der er inkluderet en virksomheds udtalelse fra mit hold i denne rapport som jeg har fået feedback angående mit arbejdsindsats hos dem.

Virksomhedsbeskrivelse:

It-koncern en it-organisation med ca. 4500 medarbejder som er en enhed under Økonomiforvandling i københavns kommune. De leverer stabil, sikker og effektiv it og digitale løsninger til virksomhedsområder, ansatte, patienter og borgere. Desuden er deres formål at forvaltningerne er i stand til at tage sikre systemer i brug og benytte dem på en sikker måde. På It-koncern er der risikovurderinger, sikkerhedsgodkendelser, tilsyn, logning, monitorering og overvågning i KIT.

Læringsmålene for Praktikken:

I praktikken startede jeg med at blive præsenteret for KIT med arbejderne og få en forståelse af arbejdsgangen vha. min kontaktperson. Derefter blev jeg kort introduceret til de værktøjer der bliver benyttet til logging, monitorering og overvågning på monitorigening holdet. Samt blev jeg introduceret til andre platforme til at kommunikere med andre medarbejder som er relateret til arbejdsopgaver. Disse værktøjer som benyttes på monitoreringen holdet er:

Darktrace:
et overvågning værktøj som bliver brugt til at overvåge alle endpoint og alle deres assets. I dette værktøj har man en web-interface som man kan sætte regler og alarmer for at mitigering for alle assets, opbygge sikkerhed og analyse trafik på bestemte enheder. Draktrace kan ses som en avanceret Security onion som jeg fik brugt på 1.semester.

Logpoint:
Et værktøj som hjælper med at indsamle log fra alle assets. Dette værktøj kan sætte regler og alarmer op og lave rapport for specifikke handlinger som indtastede forkerte adgangskode, oprette af bruger og flere andre ting. Desuden er man i stand til at søge manuelt hvor Logpoint har en web-interface som har en søgbar som

medarbejder kan bruge til at søge noget specifik for analysere og undersøge en trafik eller incident.

Trend micro:
For at beskytte alle enheder fra Virus, malware, sårbar indhentet filer har KIT benyttet sig af Trend micro. Dette værktøj er dedikeret til at kigge på enheder. Det kigger ikke på netværkstrafik, men det ser på hvad endpoint har indhentet, kigger på hashet af det bestemte fil. Samt kan Trend micro kigge på de forskellige handlinger en bestemt endpoint har udført. Det kan f.eks være at hvilke programmer der bliver kørt på det bestemte endpoint.

Nessus:
Nessus er et værktøj der bliver brugt at scanne netværket for se om der sårbarheder på assets og unødvendige åbnet porten.

Cycognito:
De første 4 er til interne monitorering og logging på virksomhed. Det sidste værktøj som hedder Cycognito er en virksomhed som har samarbejde med KIT. Deres arbejdsopgave er at scanne de eksterne assets bl.a. KITs hjemme og give dem anbefalinger og rapporter angående en specifike sårbarhed som eksisterer på en assets. Rapportering foregår på Cycognito hvor man har en bruger og men kan få en overblik over rapporterne.

Til kommunikation i Koncern IT bliver det brugt:

Outlook:
Det bliver brugt til at svare på mail og til at planlægge møder.

Microsoft team
Dette bliver brugt til at holde samtale og holde virtuelle møder.

Edoc:
Denne platform bliver brugt til gemme sine filer som pdf og word dokumenter.

ServiceNow:
Platformen som bliver brugt til at oprette forskellige sager som omhandler arbejdsopgaver.
Da jeg var en uge hos netværks holdet fik jeg ikke brugte nogle værktøjet. Jeg og en medarbejder fra netværks holdet fik lavet en pentesting active directory lab som var 4 bærebare, en switch og en wifi.

Forklaring af arbejdsopgaver hos monitoring holdet:

Først og fremmest fik jeg oplært at hvordan jeg skulle bruge værktøjer og kommunikation platform hos dem. Derudover blev jeg meldt til Darktrace kursus for at have en bedre forståelse af dette værktøj. Jeg fik forskellige arbejdsopgaver som var:

Analyse forskellige alarmer i Darktrace:
Dette var en daglig arbejdsopgaver hvor jeg skulle analyse forskellige alarmer for at se om farlige dette alarm kunne være. Det har selvfølgelige nogle falsk positive alarmer også. Jeg skulle undersøge trafikken og Titlen på alarmerne. Darktrace var et brugervenlig værktøj som for være hver eventuelle udførte incident ville der være en titel. Derfor blev jeg bedt om at undersøge hvad det angreb eller incident gik ud på og hvor farlig det kunne være.

Kigge på logs på et bestemte endpoint eller trafik i Logpoint:
Det var også en daglig arbejdsopgave gik ud på at undersøge og kigge på log på et bestemte endpoint og analyser om der er sket en mystiske handling.

Analyse endpoint med Trend micro:
De første to blev jeg mere involveret i end at analyse endpoint. Jeg fik analyseret et barbær som brugeren fik informeret os dette bærbar har mærkelige opførsel de sidste par gange. Derudover fik holdet og jeg analyseret bærbarret .

Finde fortrolige filer (SMB) på port 445:

Denne arbejdsopgaven gik ud på vi skulle gå ind på forskellige shared folder på forskellige enheder hvis de havde port 445 åbnet. Dette kunne lad sig gøres ved hjælpe af Kali linux. Først og fremmest skulle vi se om hvem har disse port åbnet og efterfølgende kigge på deres filer og se om vi kan finde fortrolige data i deres filer.

Skrive python script og analyse brugbar python script:
Jeg fik en arbejdsopgave som omhandlede at skrive en python script for at printe smb træet for folder og subfolders for specifik shared folder på netværket. Udover det fik jeg analyseret forskellige python script som jeg skulle diskutere og vurdere om disse scripts kunne bruges til at implementere i virksomheden.

Analyse pentesters opførsel og analyse benyttet bærbar fra pentester:
Der kom forbi nogle “whitehat” pentesterer for at lave penetration testing i den interne netværk i KIT. Holdet og jeg fik observerede hvad de fik lavet vha. de monteringen og log værktøjer som jeg har nævnt tidligere. Efter pentesters opgave analyserede vi selve bæbaret, Især hvilke salgs kommandoer de har fik udført på dette bærbær.

Forklaring af arbejdsopgaver hos netværks holdet :

Som jeg nævnte tidligere vi fik lavet en Active directory lab og da jeg havde en uge hos dem fik vi lavet opsætning af vores lab og derudover forstår de grundlæggende viden om active directory og til sidste udføre forskellige angreb vha. undersøgelse de forskellige angreb der kan udføres. Efter angrebet ville vi lave mitigering på active directory så det ikke være muligt at gentage de forskellige udførelser af angreb.

Konklusion:

På mit 10 ugers praktikforløb hos KIT fik jeg klart udviklet mig selv både fagligt og personlig. Jeg fik arbejdet med forskellige tools og jeg kan få en bedre forskellige hvordan man arbejder i den virkelige verden samt at en forståelse af hvordan et hold

arbejder sammen. Jeg er blevet mere struktureret og præcis til de opgaver jeg har arbejder med. Det allervigtigste ting som jeg fik lært og jeg ville gerne nævne er at man skal meget undersøge og blive sikker på det IT besluninger man træffer.

Monitorering holdet havde en stor indflydelse på mine faglig kompentencer. De skubbede og prægede mig i den rigtige retning . De var flinke og hjalp mig både fagligt og personligt. Selvom jeg var i tvivl om forskellige opgaver og hvordan de laves efter de fik havde forklaret mig det, kunne jeg altid henvende mig til dem stille spørgsmål igen. Som en nysgerrig person, har jeg ikke holdt mig tilbage for at stille spørgsmål. På den måde ville jeg være sikker på hvordan jeg skal løse mine opgaver på bedst mulig måde. De første 2-3 uger brugte jeg mere min tid på at stille spørgsmål og tilpasse mig på virksomheden.

Refleksion over læringsmål og blev de opnået?

Min tid hos KIT har været en yderst lærerig oplevelse af slagsen. Jeg kan konstatere at jeg tilfreds med mit praktikforløb og derudover har jeg udviklet mig og udvidet min viden om It-sikkerhed. Der er selvfølgelig plads mere til udvikle sig både fagligt og personligt. Jeg fik lært at benytte flere værktøjer og jeg har mestret dem som bliver brugt hos KIT. Udover oplæring af værktøjer fik jeg en bedre forståelse af netværk og forskellige protokoller som jeg ikke var bekendt med. Desuden fik jeg indblik i hvordan en pentester ville penteste en virksomhed . Hos netværks holdet fik jeg lært de grundlæggende viden af Active Directory og opsætning af den. Derudover fik jeg lært forskellige angreb og hvordan man kan lave mitigering. Der var selvfølgelig nogle udfordringer og der stadig plads til forbedring og udvide min viden angående med Active directory, sårbarheder og forskellige angrebsmetoder. Hele mit praktikforløb var godt, hvor jeg fik udvikling, erfaring og masse bekendtskaber inden for arbejdslivet.

Virksomheds Udtalelse

Praktiklog