**Labo 4: SET**

**Reflectie Chingiz**

Ik vind het bestaan van een SET tool zeker een meerwaarde en ook ethisch verantwoord. Het is tof dat men met de wapens van een hacker in zijn schoenen kan staan en zo de veiligheid van eigen systeem kan testen om te achterhalen welke eventuele vulnerabilities de hacker kan gebruiken en misbruiken.

Als je zelf deze technieken toepast en weet hoe ze werken is het een stuk makkelijker om u daar tegen te wapenen en de betrokken personen (uw personeel) in te lichten hoe ze moeten handelen om de attackers geen kans te geven om in uw systeem binnen te dringen.

Daarom vind ik het ook absoluut noodzakelijk om regelmatig workshops te geven aan uw personeel en nieuwe medewerkers een cursus te geven nog voor ze toegang krijgen tot het netwerk.

Tot op heden blijft de mens de zwakste schakkel in de beveiliging en men kan nooit teveel aanleren om uw data secure te houden.

Men kan zelfs verdergaan en deze tools op een slimme manier gebruiken om de hacker, in geval van een aanval met nepdata te voorzien om hem zo te kunnen ontmaskeren.

Daarnaast is het heel interessant om uw eigen systeem vanuit een ander kijkpunt te bestuderen. Als defensive network engineer moet je aan honderden mogelijke vulnerabilities denken en proberen om alle backdoor dicht te doen, maar een hacker hoeft maar 1 backdoor te vinden om uw systeem te pwnen. Bovendien kan je het systeem technisch niet beveiligen tegen inbraken die gebeuren met gestolen authenticatie gegevens van legitieme gebruikers, en mensen denken soms dat ze heel proactief en veiilig handelen, maar dat is lang niet altijd het geval.