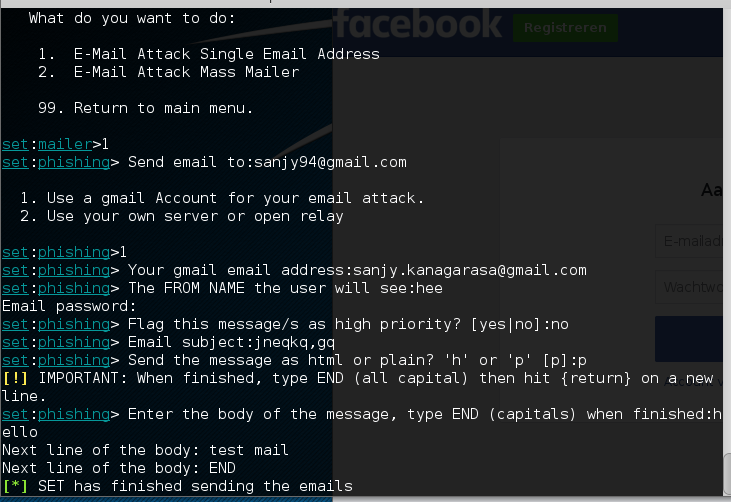
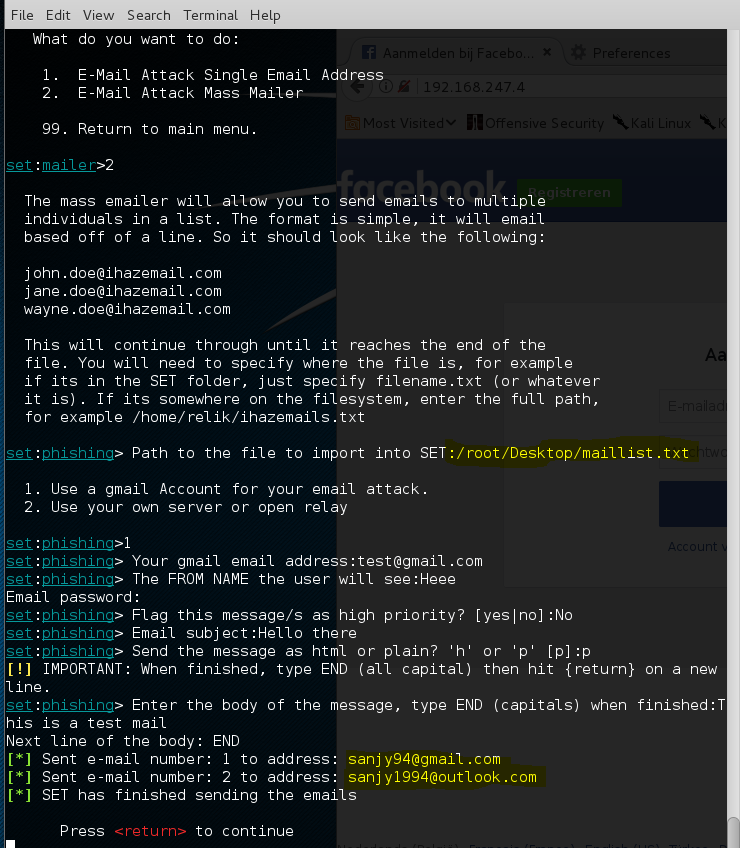
**Labo 4: SET**

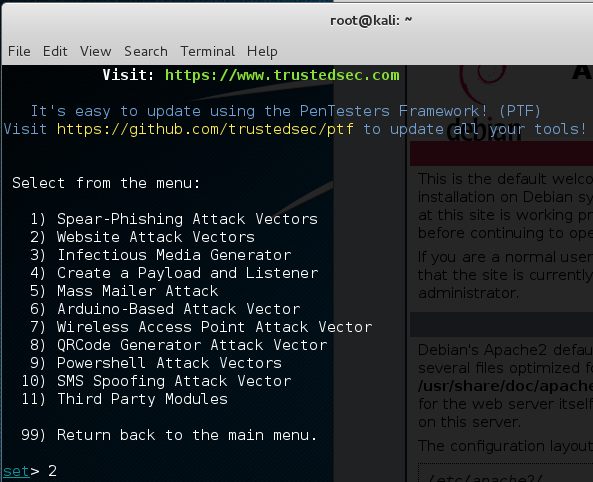
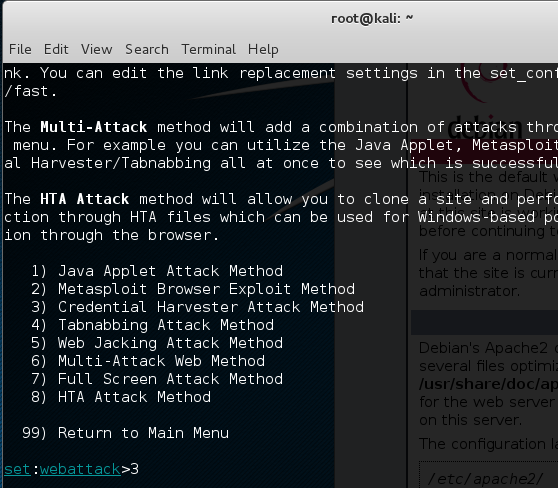
**Single mail Attack**

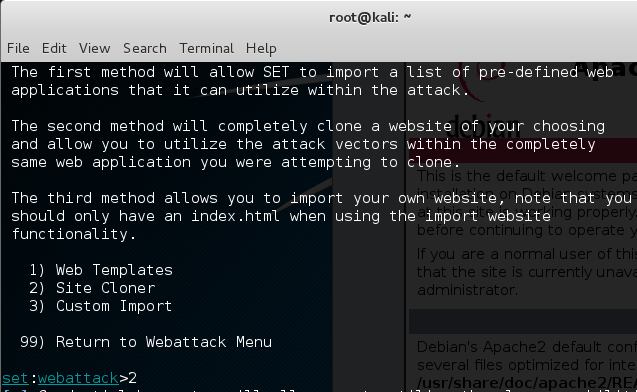


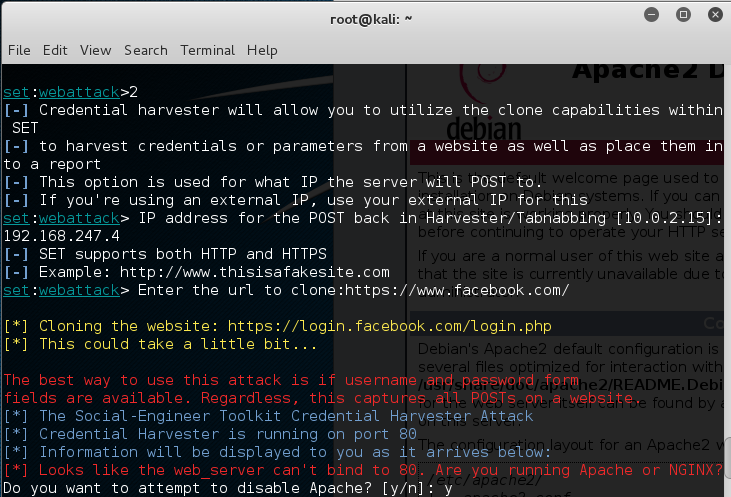
**Mass mail Attack**

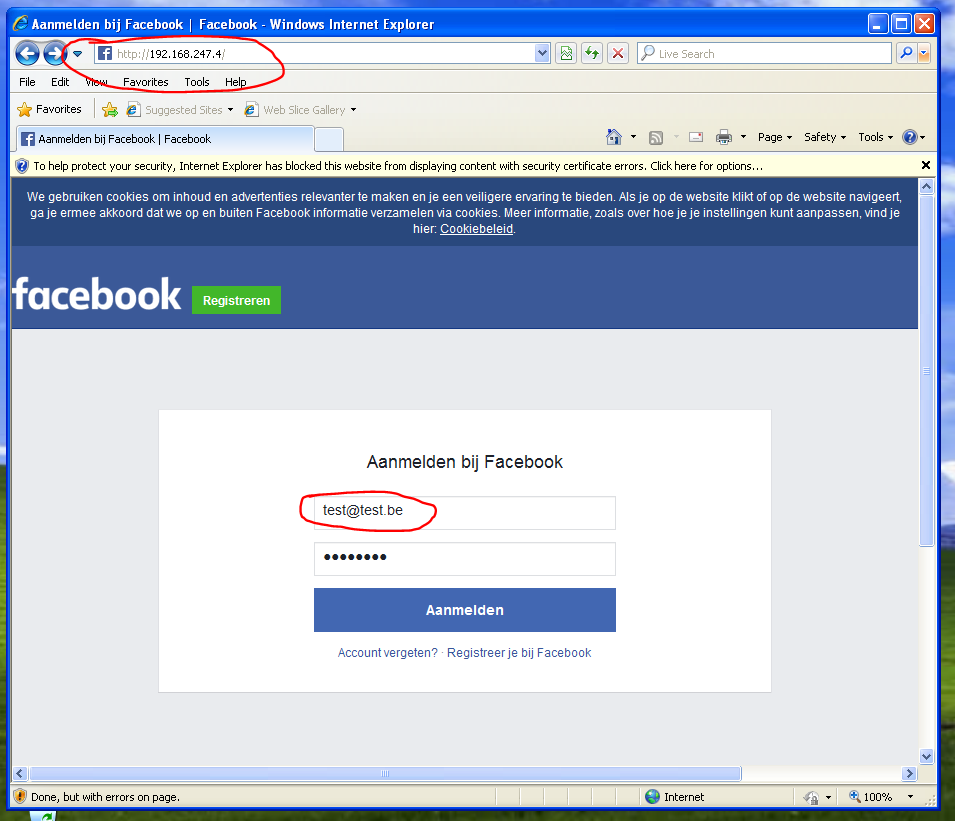


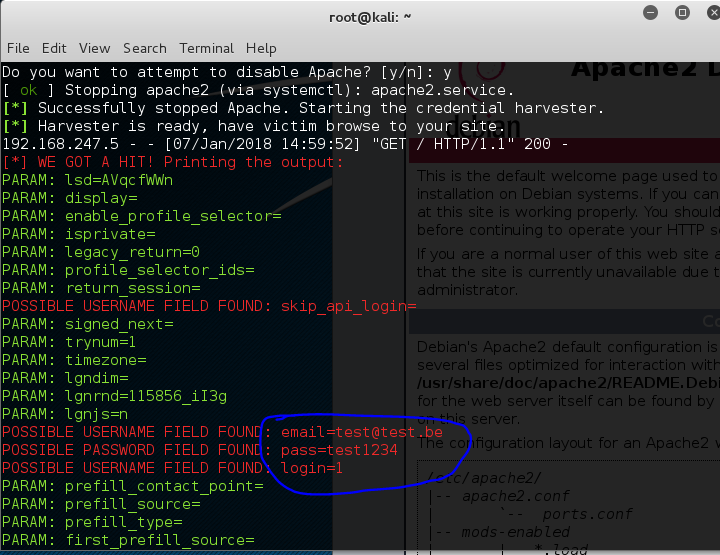
**Web Attack Vector**











**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 veilig handelen, maar dat is lang niet altijd het geval.

**Reflectie Sanjy:**

De Social Engineering Toolkit (SET) vond ik een krachtige belangrijke tool in de information security wereld. SET is niet zo moeilijk te begrijpen en is redelijk eenvoudig in gebruik. Het is vooral ontwikkeld voor pentesten rond social Engineering maar dit is een open socuce tool dus iedereen kunnen gebruiken inclusief hackers.

In dit labo heb ik de mailing attacks en web attack vector aanvallen geprobeerd. Er stond twee soort mail attack. Single en mass mail attacks. Mass mail attack vond ik meeste interessant. Er zijn niet zo grote verschil tussen die twee. Bij mass mail attack, kunt je een file refereren met een lijst van email-adressen en met je mail naar alle email adres var de lijst door gemaild. In de body van je mail, je kunt alles insteken wat je wilt. Voorbeeld een pdf met keylogger, als iemand die pdf open klikt dan wordt alles terug doorgestuurd naar je machine inclusief password enz.

De web attack vector aanval is nog ene interessante onderdeel van SET. Ik heb binnen vijf minuten (met paar enters) hele facebook login pagina gekloond en gedraaid op port 80 met apache server. Als je nu surft naar ip van kali (waar SET draait) van uit zelfde netwerk dan krijg je zelfde pagina als facebook login page. Als iemand nu username en password invult, die allemaal kunt je als plane tekst lezen. Hackers kunnen een fake domein met twee nullen kopen en daar die facebook site kunnen hosten, dan hacker hebt je username en password van je facebook account.

Enerzijds SET is handig voor pentesten en ons eigen systeem checken en beveiligen. Maar als iemand wilt vals spellen dan moet niet zo veel it kennis hebben dit tool gebruiken en misbruiken.