1/18/2022

Acker,Luc L.R.A. van den

Fontys hogenschool ICT

Body of knowledge

Cyber Security Semester 4

Contents

[1.2 Set-up of a test Web Shop 3](#_Toc124942818)

[2 Web application and defense 4](#_Toc124942819)

[2.1 Path Traversal, (remote) File inclusion and Command Injection 4](#_Toc124942820)

[2.2 Wat is Path Traversal en hoe werkt het? 4](#_Toc124942821)

[2.3 Wat is (Remote) File Inclusion en hoe werkt het? 5](#_Toc124942822)

[2.4 Wat is Command Injection en hoe werkt het? 6](#_Toc124942823)

[3 Database Attack and Defense 7](#_Toc124942824)

[3.1 SQL Injection 7](#_Toc124942825)

[4 Web Site Attack and Defense 9](#_Toc124942826)

[4.1 Cross-Site Scripting(XSS) 9](#_Toc124942827)

[4.2 Cross-Site Request Forgery(CSRF) 9](#_Toc124942828)

[4.3 Law & Ethics, Responsible Disclosure and GDPR 10](#_Toc124942829)

[4.3.1 Voorbeelden van Cyber Crime 10](#_Toc124942830)

[4.3.2 Responsible disclosure 11](#_Toc124942831)

[5 Identification of Vulnerabilities 12](#_Toc124942832)

[5.1 Network Scanning 12](#_Toc124942833)

[5.2 Footprinting, Reconnaissance and Social Engineering 13](#_Toc124942834)

[5.2.1 Footprinting/Reconnaissance 13](#_Toc124942835)

[5.2.2 Social Engineering 13](#_Toc124942836)

[6 Protect the Network 14](#_Toc124942837)

[6.1 Network Seperation and Segmentation with Firewalls 14](#_Toc124942838)

[6.2 Firewall Rules 15](#_Toc124942839)

[6.3 Secure Network Connections(HTTPS/TLS/SSH) 16](#_Toc124942840)

[HTTPS 16](#_Toc124942841)

[TLS 16](#_Toc124942842)

[SSH 16](#_Toc124942843)

[6.4 VPN Setup 17](#_Toc124942844)

[7 Attack the Network and Defend 18](#_Toc124942845)

[7.1 Network spoofing and Man in The Middle Attacks 18](#_Toc124942846)

[Sniffing 18](#_Toc124942847)

[Spoofing 19](#_Toc124942848)

[19](#_Toc124942849)

[7.2 Network/Host Intrusion Detection and Prevention 19](#_Toc124942850)

[8 Identity & Access Management 20](#_Toc124942851)

[9 Business Continuity & Risk Mitigation 22](#_Toc124942852)

[RTO en RPO 22](#_Toc124942853)

[10 IT System Hardening 23](#_Toc124942854)

[11 Wireless hacking 24](#_Toc124942855)

## 1.2 Set-up of a test Web Shop

Om veilig te kunnen experimenteren met verschillende onderwerpen rondom cyber security, wordt allereerst een veilige omgeving opgezet. Deze omgeving bestaat uit een router, een Kali linux machine en een DVWA(**D**amn **V**ulnerable **W**eb **A**pplication).

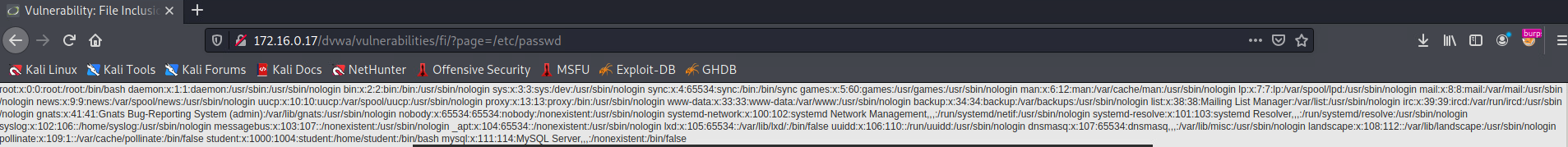
# 2 Web application and defense

### 2.1 Path Traversal, (remote) File inclusion and Command Injection

### 2.2 Wat is Path Traversal en hoe werkt het?

Het doel van een Path Traversal Attack is om toegang te krijgen tot bestanden of directories buiten de web root folder. Door variabelen te manipuleren in file references(bijvoorbeeld “../” toevoegen) is het mogelijk om toegang te krijgen tot bestanden die niet toegankelijk horen te zijn. Wanneer een webapplicatie goed is beveiligd, wordt een Path Traversal Attack natuurlijk lastiger. Met een Path Traversal Attack is het dus mogelijk om toegang te krijgen tot gevoelige bestanden, directories of zelfs source code.

DVWA Path Traversal

Onder het kopje File Inclusion is het mogelijk misbruik te maken van Path Traversal. Wanneer een bestand aangeklikt wordt, verwijst de app naar een nieuwe pagina. De URL van deze pagina is: 172.16.0.17/dvwa/vulnerabilities/fi/?page=file3.php. Door deze URL aan te passen tot 172.16.0.17/dvwa/vulnerabilities/fi/?page=/etc/passwd, wordt data weergegeven die de gebruiker niet hoort te zien(onderstaand screenshot). Gelukkig zijn de wachtwoorden niet zichtbaar, maar de usernames van alle gebruikers zijn wel zichtbaar. Voor een brute force attack is een aanvaller dus al halverwege.

Wanneer het Security Level naar “high” wordt gezet, werkt de bovenstaande URL niet meer. Door misbruik te maken van Uniform Resource Identifiers(URI) is het echter alsnog mogelijk om toegang te krijgen. Een URI is een unieke benaming voor een stuk data. In dit geval is het mogelijk gebruik te maken van de “file” URI. De URL ziet er dan als volgt uit: 172.16.0.17/dvwa/vulnerabilities/fi/?page=file:///etc/passwd.

A screenshot of a computer

Description automatically generated with medium confidenceDoor de URL aan te passen naar 72.16.0.17/dvwa/vulnerabilities/fi/?page=/proc/version is het ook mogelijk om meer informatie te vinden over het Operating System van de slachtoffer(onderstaand screenshot).

### 2.3 Wat is (Remote) File Inclusion en hoe werkt het?

Een File Inclusion kwetsbaarheid geeft een aanvaller de mogelijkheid om een bestand te uploaden naar de server van een website. Meestal wordt hierbij misbruik gemaakt van “dynamic file inclusion” functionaliteiten. Meestal staat er een script in het bestand, wat uitgevoerd wordt op de server. Andere gevolgen kunnen zijn:

* Code execution op de client kant, bijvoorbeeld cross site scripting(XSS).
* Denial of Service (DoS)
* Gevoelige informatie wordt gelekt.

DVWA Remote File Inclusion

Graphical user interface, application

Description automatically generatedHet doel van deze opdracht is het gebruiken van een bestand dat gehost wordt op de machine van de aanvaller. In dit geval is het doel om Google te hosten via de DVWA. Door De URL aan te passen van 172.16.0.17/dvwa/vulnerabilities/fi/?page=include.php naar 172.16.0.17/dvwa/vulnerabilities/fi/?page=http://google.com wordt google weergegeven in de pagina van de DVWA. Zoals in het screenshot hiernaast te zien is, staat de bekende zoekbalk van google bovenaan de pagina weergegeven.

Als de Security Level verhoogd wordt naar “medium” is het niet meer mogelijk om slechts <http://google.com> aan de URL toe te voegen. De website vervangt “http” nu met “https”. Echter wordt enkel exact “http” vervangen door “https”. Het filter herkent bijvoorbeeld “Http” niet meer door de hoofdletter, dus door dit in de URL te zetten in plaats van “http” is google.com nog steeds beschikbaar. De enige aanpassing die gemaakt hoeft te worden is de “h” in “http” vervanger met een hoofdletter, waardoor de URL er als volgt uitziet: 72.16.0.17/dvwa/vulnerabilities/fi/?page=Http://google.com. Het resultaat blijft hetzelfde als in het bovenstaande screenshot.

Om (Remote) File Inclusion tegen te gaan, wordt gebruik gemaakt van validatieprotocollen. Wanneer alle bestanden blind worden geaccepteerd, is het natuurlijk heel simpel om malafide software te uploaden. Daarom is het verstandig om alle bestanden te valideren voordat ze naar de server geüpload worden. Wanneer een gebruiker bijvoorbeeld online een CV moet kunnen uploaden, is het aan te raden om alleen word/PDF bestanden te accepteren.

### 2.4 Wat is Command Injection en hoe werkt het?

Command Injection, ook wel Shell Injection genoemd, is een kwetsbaarheid in een web applicatie, waardoor een aanvaller OS commands kan uitvoeren op de server waar de applicatie op draait. Door een command uit te voeren op de server kan een aanvaller delen van de infrastructuur van de host om zeep helpen.

DVWA Command Injection

Text

Description automatically generatedTijdens deze opdracht wordt geprobeerd om gegevens op te halen door middel van command injection. Waar de DVWA een IP-adres verwacht, wordt er geen validatie uitgevoerd voor de input, waardoor alle karakters ingevoerd kunnen worden. Door eerst een cijfer(1) in te voeren, met daarna een commando, wordt het systeem om de tuin geleid en wordt het meegegeven commando uitgevoerd. Wanneer 1;cat /etc/passwd in wordt gevoerd, gaat het systeem een cat-commando uitgevoerd, en wordt alle data uit de passwd folder weergegeven, zoals in het screenshot hiernaast te zien is.

Als de Security Level verhoogd wordt naar “medium”, worden tekens als “;” of “&&” gefilterd door de DVWA. Het commando hierboven zal dus niet meer werken. In de DVWA is dus een filter toegevoegd, waardoor bepaalde character arrays gefilterd worden. Het nadeel hieraan is echter dat een computer dit letterlijk leest, en alleen de bovenstaande teksten filtert. “&&” is dus geen mogelijkheid, maar “&” is nog prima te gebruiken. Om hetzelfde resultaat te krijgen als in het screenshot hierboven, moet de “;” in het bovenstaande commando vervangen worden door een teken dat niet gefilterd wordt, maar er wel voor zorgt dat de DVWA de weg kwijt is. Het commando komt er dan als volgt uit te zien: 1&cat /etc/passwd. In dit commando wordt de “;” dus vervangen door “&”. Omdat dit niet meegenomen wordt in het filter, kan het commando alsnog uitgevoerd worden.

# 3 Database Attack and Defense

### 3.1 SQL Injection

SQL Injection is een kwetsbaarheid waarbij gebruik wordt gemaakt van SQL-statements. Met deze SQL-statements wordt geprobeerd data opgehaald, opgeslagen, gewijzigd of verwijderd. Indien deze statements niet of niet voldoende gecontroleerd worden, kan er misbruik van gemaakt worden, zoals in het voorbeeld hieronder te zien is.

DVWA SQL Injection

De DVWA biedt een pagina aan waarop een gebruiker een ID in kan voeren, en vervolgens de volledige naam van de bijbehorende gebruiker krijgt, inclusief het bijbehorende ID. De DVWA gebruikt de volgende query om tot dit resultaat te komen: SELECT first\_name, last\_name FROM users WHERE user\_id = ‘$id’;. Vervolgens wordt gekeken of de applicatie kwetsbaar is voor SQL Injection. Door in het invoerveld 3’ OR ‘1’ = ‘1 in te voeren, is het mogelijk om alle gebruikers op te halen, wat betekent dat de applicatie inderdaad kwetsbaar is voor SQL Injection. Vervolgens wordt gekeken of het mogelijk is om erachter te komen welke tabellen bestaan in de database, met behulp van de volgende query:

A picture containing text

Description automatically generated3' UNION SELECT table\_schema,table\_name FROM information\_Schema.tables;#. De “UNION SELECT” in deze query geeft aan dat de gegevens uit twee of meerdere “SELECT” commando’s samengevoegd moeten worden. “table\_schema” geeft aan waar een tabel staat, en “table\_name” geeft de naam van de tabel aan. Deze gegevens worden opgevraagd uit “information\_Schema.tables”. Deze bevat informatie over alle tabellen in de database. Door aan het einde “#” toe te voegen, wordt aangegeven dat er na deze query niks meer uitgevoerd moet worden. Wanneer dit allemaal uitgevoerd wordt, worden de namen en locaties van alle tabellen in de database opgehaald, zoals in het screenshot hierboven te zien is. De locatie van de tabellen staat bij “First name” en de naam van de tabellen staat bij “Surname”.

Text

Description automatically generatedGraphical user interface, text, application, email

Description automatically generatedDoor de Security Level op te krikken naar “medium” is het niet meer mogelijk om simpelweg een SQL-query in te voeren in een tekstbalk, aangezien deze vervangen is door een drop-down. De query zal dus via Burpsuite aangepast moeten worden. Vanuit daar wordt de POST-request onderschept. Op regel 15(zie screenshot hiernaast) is te zien welke parameters meegegeven worden in de query. Door daaraan OR 1=1 toe te voegen, wat altijd waar is, geeft de server alle gebruikers terug. Leuk, maar waarom werkt de OR 1=1 nu wel? Omdat er geen tekstveld is waarop de gebruiker dit soort parameters mee kan geven, lijkt het erop dat de developers er vanuit gaan dat het risico afgedekt is. In het screenshot hiernaast is te zien dat dit echter niet het geval is. Aangezien alleen de security op de web applicatie gewijzigd is, veranderen de risico’s niet. Via Burpsuite zijn alle trucjes van de “low” security nog steeds mogelijk, alleen de plek waar de parameters aangepast worden zijn anders.

# 4 Web Site Attack and Defense

### 4.1 Cross-Site Scripting(XSS)

XSS is een aanvalstype waarbij malafide scripts geïnjecteerd worden in websites die normaal gesproken betrouwbaar horen te zijn. Het script wordt dan bijvoorbeeld op de server van de website geüpload, waardoor het betrouwbaar lijkt te zijn. De browser van een andere gebruiker heeft dus geen idee dat het script niet betrouwbaar is, waardoor toegang tot cookies, sessies of andere gevoelige data verstrekt wordt. Hierdoor is een andere eindgebruiker vaak het slachtoffer van dit soort aanvallen. Het effect van zo’n XSS aanval kan variëren van een licht risico tot een serieus risico, afhankelijk van de gevoeligheid van de betreffende data en de security van de website.

DVWA Cross-Site Scripting

Text

Description automatically generatedHet doel van deze opdracht om een script te uploaden naar de server van de DVWA, om vervolgens dit script uit te laten voeren bij de eindgebruiker. Met dit script wordt de Security Level van de DVWA verhoogd naar “impossible”. De Security Level wordt in een cookie opgeslagen, waardoor het toevoegen van een cookie voldoet om de Security Level te verhogen. Omdat het invoerveld voor Messages een maximale lengte van 50 karakters heeft, moet dit eerst verhoogd worden via de “inspector”(zie screenshot hierboven, maxLenght geeft aan hoeveel karakters er ingevoerd mogen worden). Vervolgens is de maximale lengte groot genoeg om het volgende script in te voeren:

<script>document.cookies = “security=impossible”</script>. Zoals in het screenshot hiernaast te zien is, wordt de Security Level na het uitvoeren van het script automatisch op “impossible” gezet.

### 4.2 Cross-Site Request Forgery(CSRF)

Via CSRF wordt een eindgebruiker met behulp van Social Engineering gedwongen om ongewenste acties uit te voeren op een geauthentiseerde webapplicatie. Social Engineering is een vorm van hacken waarbij de aanvaller zich richt op de zwakste schakel van het systeem, namelijk de mens. Door bijvoorbeeld een link via een email of chatbericht te versturen, misleidt een aanvaller de eindgebruiker om misbruik te maken van normaal gesproken beveiligde data/functionaliteiten. Wanneer de eindgebruiken een normale gebruiker is, kan een succesvolle aanval leiden tot een hoop zorgen bij de eindgebruiker. Een voorbeeld van een CSRF-aanval is bijvoorbeeld een SMS-bericht/email van de ING, waarin aangegeven staat dat de gebruiker via de link in het bericht zijn wachtwoord moet wijzigen. Wanneer de gebruiker op deze link klikt, krijgt de aanvaller toegang tot de bankgegevens van de gebruiker, wat natuurlijk enorme gevolgen kan hebben. Wanneer het slachtoffer een administratief account heeft, kan de schade nog veel groter zijn, en kan bijvoorbeeld een hele webapplicatie gesloopt worden.

## 4.3 Law & Ethics, Responsible Disclosure and GDPR

GDPR(General Data Protection Regulation), of AVG(Algemene Verordening Gegevensbescherming) in het Nederlands, is een wet over het beschermen van persoonsgegevens. De wet is in de hele Europese Unie ingevoerd op 25 mei 2018. De AVG gaat dus over het beschermen van persoonsgegevens van personen in de EU, en geldt voor ondernemingen en instanties over de hele wereld.

### 4.3.1 Voorbeelden van Cyber Crime

Case 1

Graphical user interface, text

Description automatically generated

<https://www.parool.nl/nieuws/abn-en-rabobank-getroffen-door-ddos-aanval~b1f07efe/?referrer=https%3A%2F%2Fwww.google.com%2F>

op 24 mei 2018 zijn ABN en Rabobank getroffen door een DDoS-aanval. DDoS(Distributed Denial-of-Service) houdt in dat een webserver compleet overbelast wordt met internetverkeer, waardoor gebruikers geen toegang meer hebben tot de service, of erg traag wordt. Voor ABN en Rabobank betekent dit dat klanten geen bankzaken kunnen doen, en dus geen betalingen kunnen doen, of simpelweg hun bankrekening beheren. Vaak eisen de aanvallers bij een DDoS-aanval geld in ruil voor het beëindigen van de aanval. Indien dit geld niet betaald wordt, kan het dagen, of zelfs weken duren totdat de server weer normaal beschikbaar is voor gebruikers, wat enorm schadelijk is voor een bedrijf. Enkele dagen later, op 27 mei 2018 werden beide banken wederom getroffen door een DDoS-aanval, maar deze tweede aanval duurde gelukkig maar vier uur.

Cyber misdaden zijn een goed voorbeeld van “high risk, high reward”. Hackers kunnen in korte tijd enorm veel geld verdienen door bijvoorbeeld een DDoS-aanval, maar het risico om gepakt te worden, is ook enorm. Ook is het natuurlijk onethisch om geld te verdienen ten koste van anderen. Ook al zijn cyber-misdaden niet goed te praten, hebben ze toch een meerwaarde. Cyber-aanvallen zorgen ervoor dat cyber-specialisten zich ontwikkelen. Wanneer duidelijk is dat een systeem op ieder moment aangevallen kan worden, zorg je er wel voor dat dit zo moeilijk mogelijk gemaakt wordt.

### 4.3.2 Responsible disclosure

Bij deze verklaar ik dat ik gevonden kwetsbaarheden of data direct meld bij de eigenaar hiervan. Daarnaast zal ik mijn kennis op het gebied van Cyber Security nooit inzetten op een illegale manier, of op een manier waar anderen problemen van kunnen ondervinden.

# 5 Identification of Vulnerabilities

### 5.1 Network Scanning

Text

Description automatically generatedDoor het scannen van een netwerk ontstaat een beter beeld van een onbekende omgeving. Door een scan uit te voeren, ontdekt men bijvoorbeeld hoeveel hosts er op het netwerk zitten, of welke poorten open staan. Vaak wordt hiervoor “nmap” gebruikt. Via nmap wordt het gespecificeerde netwerk gescand, en krijgt de gebruiker dus een goed beeld van de digitale infrastructuur. Het nadeel aan nmap is het hoge dataverbruik, en dus de hoge belasting om een netwerk. In het screenshot hiernaast is weergegeven wat “nmap” precies weergeeft. Het netwerk dat hier gescand wordt, bestaat uit twee routers, een kali machine en een DVWA. Voor deze scan wordt de router gescand, waarmee drie andere hosts verbonden zijn, zoals in de laatste regel van het screenshot te zien is(de vierde is de router zelf). Per host wordt het IP-adres, het aantal poorten en het aantal poorten dat in gebruik is weergegeven. Voor de routers wordt ook weergegeven welke protocollen gebruikt worden. Zoals we hierboven zien, zijn alle poorten van de kali machine, met IP 172.16.0.16, gesloten. Voor de DVWA, met IP 172.16.0.17, staat er wel één poort open. Via deze poort is het mogelijk om de webapplicatie te benaderen. Tenzij iets anders aangegeven is, scant Nmap altijd 1000 TCP poorten. In werkelijkheid heeft een machine 65535 poorten, maar om deze allemaal te scannen, is enorm zwaar op het netwerk.

Met Nmap is het ook mogelijk om meer data over een specifieke host te vergaren. Door bijvoorbeeld “nmap -A {IP}” uit te voeren, wordt informatie weergegeven over de OS van de host op het gespecificeerde IP-adres. In het screenshot hiernaast is te zien dat de DVWA webshop draait op Apache versie 2.4.29. Via Nmap zijn er enorm veel mogelijkheden om gegevens te verzamelen over een netwerk, en de individuele hosts binnen het netwerk.

### 5.2 Footprinting, Reconnaissance and Social Engineering

De eerste fase van het pentest-proces is het vergaren van informatie. Het verzamelen van zoveel mogelijk informatie is cruciaal voor een goede pentester. Op basis van deze informatie wordt de rest van de pentest namelijk uitgevoerd. Zonder informatie is het niet mogelijk om een pentest uit te voeren. Een werkwijze die heel effectief kan zijn in het vergaren van informatie is Social Engineering.

### 5.2.1 Footprinting/Reconnaissance

Tijdens deze Reconnaissance-fase worden de volgende middelen gebruikt om zoveel mogelijk informatie te verzamelen over het doelwit:

* Open-source Intelligence, oftewel informatie die uit publieke bronnen gehaald kan worden. Denk hierbij aan het internet, traditionele media. Ook sociale media, zoals LinkedIn kunnen veel informatie bieden over de mensen die betrokken zijn bij het doelwit.
* Google searching/search engine hacking, oftewel het zoeken van kwetsbaarheden met behulp van geavanceerde search engines.
* Network information discovery, nmap. Het doel hiervan is het achterhalen hoe het netwerk eruit ziet, en wat voor apparaten er verbonden zijn.
* Social network analysis, oftewel onderzoek naar de sociale structuur van het doelwit. Hierbij worden tools zoals LinkedIn, Facebook en andere sociale media gebruikt.

### 5.2.2 Social Engineering

Social engineering is een vorm van hacking waarbij de focus ligt op psychologische manipulatie van mensen. De zwakste schakel van ieder systeem is natuurlijk de mens, waardoor social engineering veel resultaten kan opleveren. Een voorbeeld hiervan is de zogenaamde Confidence Trick, waarbij eerst het vertrouwen van één of meerdere personen gewonnen wordt, om vervolgens informatie te ontfutselen. Veel bedrijven zijn tegen Social Engineering tijdens een pentest, omdat het gezien kan worden als fraude, of het misbruiken van vertrouwen. Gelukkig hebben wij, als ICT’ers, niet voldoende sociale vaardigheden om misbruik te maken van de goedheid van mensen.

# 6 Protect the Network

Information security policies zetten eisen voor de beschikbaarheid, integriteit en de betrouwbaarheid van data. Om de risico´s op datalekken en dergelijken te verminderen, worden zakelijke netwerken opgedeeld in gesegmenteerde netwerken. Ook wordt verkeer dat het netwerk uit gaat gefilterd, om onveilig verkeer zoveel mogelijk af te houden.

### 6.1 Network Seperation and Segmentation with Firewalls

Een gesegmenteerd netwerk is altijd veiliger dan een netwerk dat niet gesegmenteerd is. Hieronder staat beschreven hoe een gesegmenteerd netwerk opgezet is. Het netwerk bestaat uit drie segmenten:

* VLAN-A met subnet 172.16.0.0/24. Apparaten op dit subnet kunnen verbinding maken met vanaf het internet beschikbare systemen. Een subnet als dit wordt vaak de ‘DMZ Zone’ genoemd(demilitarized zone).
* VLAN-B met subnet 172.16.1.0/24. Dit subnet is voor de kantooromgeving en Active Directory(AD). Een subnet als dit wordt vaak de ‘Management Zone’ genoemd.
* VLAN-C met subnet 172.16.2.0/24 voor monitoring en eventueel beheer. Een subnet als dit wordt vaak de ‘LAN Zone’ genoemd.

Diagram

Description automatically generatedDe onderstaande afbeelding laat zien hoe het hierboven beschreven netwerk eruit komt te zien. Helemaal links, in het rode vak, is een apparaat te zien dat van buitenaf verbinding maakt met de router via een VPN. Wanneer er geen VPN-verbinding opgezet is vanaf de thuiswerkplek, is het niet mogelijk om de eerste router(R1) te benaderen, en dus is het onmogelijk om de services op het netwerk te benaderen. R1 zorgt ervoor dat het netwerk verbonden is met het internet. Vervolgens is er een switch(S1) aangesloten. Onder S1 valt het eerste subnet, de DMZ Zone. Dit netwerk is dus te benaderen vanaf het internet. Hierop wordt een webserver en een NextCloud server gehost. In het witte vak aan de rechterkant zien we de LAN Zone. Binnen dit subnet vinden we de AD/file server en een werkstation. Omdat op beide hosts natuurlijk vrij gevoelige data kan staan, hoort deze afgeschermd te zijn van de buitenwereld. Daarom zit het afgesloten achter een tweede router(R2). R2 zorgt ervoor dat er geen verkeer toegestaan is vanaf de andere subnetten, of van buitenaf, naar de LAN zone toe. R2 zet ook nog een laatste subnet op, namelijk VLAN-C. Op VLAN-B(groen vak) wordt enkel een Monitoring Server aangesloten. Deze server heeft toegang tot alle subnetten, zodat het gehele systeem vanaf een veilige omgeving gemonitord kan worden.

Door het segmenteren van het netwerk zijn de kwetsbaarheden beperkt. Wanneer een aanvaller toegang weet te krijgen tot het VLAN-A subnet, heeft hij echt alleen toegang tot dat subnet, en niet tot de andere subnetten. Ook wordt de hack geregistreerd door de monitoring server, waardoor de beheerder van het netwerk bewust is van de hack en actie kan ondernemen.

## 6.2 Firewall Rules

Een firewall is een service die inkomend en uitgaand netwerkverkeer bewaakt en bepaalt welk verkeer wel of niet toegestaan wordt. Op basis van ingestelde firewall rules wordt bepaald wat er wel en niet toegestaan wordt. Het gesegmenteerde netwerk dat in hoofdstuk 6 beschreven staat, kan uiteraard ook wat firewall rules gebruiken. Hieronder staat, in een tabel welke regels ingesteld dienen te worden, met een korte beschrijving waarom de specifieke regels relevant zijn.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Router 1 |  |  |  |  |  |  |
| Source | Destination | Protocol | Poort | Applicatie | Allow/Deny | Verklaring |
| DMZ-subnet | LAN | TCP | 10051 | Zabbix Client | Allow | Monitoring van webserver |
| Buitenaf | DMZ | TCP | 443 | HTTPS | Allow | Benaderen webserver van buitenaf |
| Thuiswerkstation | LAN | TCP | 22 | SSH | Allow | Vanuit huis werken mogelijk maken |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Router 2 |  |  |  |  |  |  |
| Source | Destination | Protocol | Poort | Applicatie | Allow/Deny | Verklaring |
| LAN-subnet | \* | TCP | 80 | HTTP | Deny | HTTP is onveilig |
| LAN-subnet | \* | TCP | 443 | HTTPS | Allow | Veilig internetten |
| LAN-subnet | \* | TCP | 22 | SSH | Allow | Secure remote acces werknemersportaal |
| LAN-subnet | \* | UDP | 53 | DNS | Allow | Voor time-sensitive transmissies |
| LAN-subnet | \* | ICMP | nvt | Ping | Allow | Testen of een host nog wel online is |
| MON-subnet | LAN | TCP | 10051 | Zabbix Client | Allow | Netwerk monitoring vanaf werk-PC |
| DMZ-subnet | LAN | TCP | 389 | LDAP | Allow | LDAP moet gegeven uit AD-server halen |

## 6.3 Secure Network Connections(HTTPS/TLS/SSH)

Een goede verbinding is natuurlijk veilig. Om deze veiligheid te waarborgen zijn verschillende protocollen beschikbaar. Hieronder staan een aantal beschreven:

### HTTPS

Jaren geleden gebruikten wij allemaal HTTP voor ons webverkeer. HTTP(HyperText Transfer Protocol) is een protocol dat gebruikers de mogelijkheid geeft om te communiceren over het internet. Nagenoeg iedere URL begint met “http://” of “https://”. Deze protocollen worden dus enorm veel gebruikt, maar wat is het verschil tussen HTTP en HTTPS? Zowel HTTP als HTTPS zorgt ervoor dat een gebruiker data kan versturen en ontvangen op het internet. HTTP doet echter letterlijk dat, het opsturen en ontvangen van data, terwijl HTTPS het internetverkeer versleutelt. Een HTTP verbinding is dus een onveilige verbinding, omdat al het verkeer door iedereen die toevallig aan het luisteren is te lezen is. HTTPS daarentegen, versleutelt al het verkeer dus, en enkel de ontvanger en de verzender hebben de benodigde sleutel om het verkeer te ontsleutelen, waardoor het een stuk lastiger is om het verkeer af te lezen.

### TLS

TLS, oftewel Transport Security Layer, is een encryptie-protocol dat de communicatie tussen computers beveiligt. TLS maakt gebruik van asymmetrische encryptie om de identiteit van beide partijen te bevestigen. Vervolgens wordt de communicatie tussen beide partijen versleuteld door middel van symmetrische encryptie. TLS wordt dus voornamelijk gebruikt om de identiteit van een benaderde server te bevestigen.

### SSH

SSH staat voor Secure Shell, en wordt vooral gebruikt voor ‘remote login en command line’. SSH biedt dus de mogelijkheid om van afstand veilig een verbinding te kunnen maken met een SSH server. Er wordt gebruik gemaakt van Public Key-cryptografie, waarbij iedereen met een public key een bericht kan versleutelen, maar enkel degene die de bijbehorende private key hebben, kunnen het bericht weer ontsleutelen.

## 6.4 VPN Setup

Om veilig te kunnen werken op het internet staat hieronder een beschrijving over het opzetten van een VPN via een PFSense router en OpenVPN:

Certificate Authority

Allereerst dient een “Certificate Authority aangemaakt te worden. Hiermee wordt de identiteit van de server gevalideerd. Ook is het mogelijk om met deze CA gebruikerscertificaten te valideren als dit nodig is. OpenVPN biedt een aantal opties voor de lengte van de key en het type key. Hierbij geldt natuurlijk dat een langere key, met complexere encryptie veiliger is. Vervolgens moet ingesteld worden hoe lang het certificaat geldig blijft. In dit geval hoeft dit niet heel lang te zijn, aangezien deze VPN niet langdurig gebruikt zal gaan worden.

Server Certificate

Een server certificate is een SSL-certificaat dat ervoor zorgt dat een host een naam krijgt. Deze naam kan een machine-naam zijn(bijv. XYZ-SERVER-01), of een domein naam, zoals [www.nu.nl](http://www.nu.nl). Als een client vervolgens een request verstuurt, wordt het certificaat van de server gecontroleerd om te achterhalen of de webserver wel legitiem is. Daarnaast verzorgt het certificaat een veilige verbinding met de client via Public Key Infrastructure(PKI).

Users en User Certificate

Het is natuurlijk niet de bedoeling dat de VPN voor iedereen toegankelijk is. Daarom worden een aantal gebruikers aangemaakt. Enkel deze gebruikers kunnen verbinding maken met de server. Hoe ziet de server nou wie er wel mag verbinden en wie niet? Aan de hand van een User Certificate. Dit certificaat wordt, net zoals een Server Certificate, gebruikt om de veiligheid van een gebruiker te waarborgen. Op basis hiervan wordt gevalideerd of de gebruiker legitiem is.

OpenVPN Server

Natuurlijk zal er een server opgezet moeten worden waarop de VPN gedraaid wordt. Clients kunnen een verbinding opzetten met deze server. Dit zorgt ervoor dat het internetverkeer van de client naar de server versleuteld is.

OpenVPN Firewall Rules

Om de VPN naar eigen wens in te stellen, is het mogelijk om bepaalde regels in te stellen, namelijk firewall rules. Met deze regels wordt gedefinieerd wat er wel en niet toegelaten wordt op de server. Zo wordt in dit geval een regel aangemaakt waarin gespecificeerd staat dat IPv4 gebruikt wordt, en IPv6 niet toegestaan is. Ook is het mogelijk om bijvoorbeeld in te stellen welk protocol gebruikt wordt. Ook is er de mogelijkheid om het IP-adres van de server en het subnet te specificeren. Er zijn enorm veel mogelijkheden qua regels. Hiermee hebben gebruikers aardig wat grip op wat ze wel of niet op hun netwerk willen hebben.

# 7 Attack the Network and Defend

## 7.1 Network spoofing and Man in The Middle Attacks

### Sniffing

Met network sniffing wordt het afluisteren van internetverkeer op een netwerk of netwerksegment bedoeld. Wanneer iemand binnen een netwerk aan het internetten is, kan dat afgeluisterd worden. In principe is al het verkeer binnen een geselecteerd netwerk af te luisteren. Wanneer het internetverkeer echter versleuteld is, zoals bij een HTTPS-verbinding altijd het geval is, zal deze data niet te lezen zijn. In dat geval zijn er enkel rare tekentjes te zien, waar een mens niks zinnigs uit kan halen. Wanneer het verkeer echter niet versleuteld is, kan iedereen dit eenvoudig uitlezen. Hieronder staat een klein voorbeeld van sniffing in Wireshark.

Wireshark is een heel nuttige tool om dit verkeer uit te lezen. Hieronder is een screenshot te zien van een HTTP-pakket. Hierin is de HTTP-data weergeven. Hierin is in plaintext uit te lezen wat er precies uitegvoerd wordt op het internet. Wanneer we een beveiligde verbinding pakken, zoals HTTPS, of bijvoorbeeld ook TCP, UDP of DHCP, zien we dit niet. Er is nog steeds te zien wat het source-IP en destination IP is. Echter is er niet uit te lezen wat er precies gezegd wordt. Aangezien nagenoeg al het verkeer tegenwoordig versleuteld is, zal sniffing steeds lastiger worden.

Text

Description automatically generated

### Spoofing

Bij spoofing hebben we het over het vervalsen van de identiteit van een computer. Door bijvoorbeeld de ING te imiteren, is het mogelijk enorm veel schade aan te richten. In dat geval communiceert een gebruiker met de malafide host, die vervolgens communiceert met de ING. Zo lijkt het alsof een gebruiker met de ING communiceert, maar stiekem zit er iemand tussenin die alle data kan onderscheppen en aanpassen.

Een andere vorm van spoofing is E-mail spoofing. Hierbij wordt dus een mail verstuurd vanaf een malafide mailadres, maar het lijkt alsof het vanaf een ander adres afkomstig is. In de screenshots hieronder is een E-mail te zien die afkomstig lijkt te zijn van ene Rudy Bouland. Op het eerste aanzicht lijkt de mail legitiem. De mail is echter alles behalve legitiem. Deze mail is verstuurd via een service(<https://emkei.cz>) waarbij gebruikers zelf kunnen kiezen vanaf welk mailadres de mail lijkt te komen. Echter wordt het verstuurd vanaf een mailadres van deze service, wat niet zichtbaar is op het eerste opzicht.

Graphical user interface, application

Description automatically generated

## Graphical user interface, text, application, email Description automatically generated

## 7.2 Network/Host Intrusion Detection and Prevention

Natuurlijk is het gevaarlijk als iemand een netwerk/host binnen kan komen zonder autorisatie. Wanneer dit toch gebeurt, is het belangrijk om hier zo snel mogelijk vanaf te weten. Hiervoor wordt gebruik gemaakt van Host Intrusion Detection Systems(HIDS) en Network Intrusion Detection Systems(NIDS). Een HIDS wordt gebruikt om invallen op een host te detecteren(computer/server bijvoorbeeld). NIDS wordt gebruikt om invallen te detecteren op een netwerk. Beide doen dus in principe nog niks om invallen tegen te gaan, maar enkel om ze te detecteren. Aangezien een HIDS enkel voor één specifieke host werkt, is af te raden om dit op ieder apparaat binnen een netwerk op te zetten. NIDS is veel praktischer, en vangt een veel groter gebied af, waardoor dit natuurlijk grote voordelen heeft ten opzichte van een HIDS.

# 8 Identity & Access Management

Identity & Access Management(IAM) gaat over het voeren van een beleid waarbij de juiste gebruikers de juiste rechten en toegangen hebben tot specifieke IT-resources met behulp van authenticatie en autorisatie. Authenticatie is een proces waarbij gecontroleerd wordt of een gebruiker daadwerkelijk is wie hij beweert te zijn. Autorisatie is het verlenen van toestemming aan een geauthentiseerde gebruiker om toegang te krijgen tot een bepaalde dienst. IAM bestaat uit een aantal verschillende onderdelen:

Registratie betreft het plaatsen van de juiste identiteitsinformatie van bronsysteem naar doelsysteem. Binnen een bedrijf kan dit op verschillende manieren aangepakt worden. Zo kunnen bijvoorbeeld gegevens van een HRM systeem naar een Active Directory worden gezet. Vanaf deze centrale directory is het eenvoudig om accountgegevens te koppelen aan andere services binnen een organisatie, zoals mailservers, portalen of HR systemen.

Autorisatie is dus het toekennen van de rechten om gebruik te mogen maken van een bepaalde dienst. Het autorisatieproces is enorm belangrijk binnen IAM, aangezien het bepaalt welke gebruikers wel of geen toegang hebben tot een dienst. Zo is het bijvoorbeeld belangrijk dat werknemers in het portal van het bedrijf kunnen, en er dus rechten toegekend moeten worden voor alle werknemers om gebruik te maken van deze dienst. Echter is het niet de bedoeling dat alle werknemers toegang krijgen tot bijvoorbeeld een management portaal.

Om te weten of iemand wel echt is wie hij zegt te zijn, wordt gebruik gemaakt van authenticatie. Tijdens het authenticatieproces wordt gebruik gemaakt van authentication credentials. Dit kunnen wachtwoorden zijn, maar ook asymmetrische of symmetrische encryptie, biometrische scans, of nog een hoop andere vormen. Om de veiligheid van een systeem te vergroten, is het aan te raden om meerdere credentials te combineren. Een extra slot op de deur is natuurlijk lastiger te kraken. Wat deze authentication credentials precies zijn en hoe ze werken wordt hieronder beschreven.

**Wachtwoorden**

Wachtwoorden worden nagenoeg altijd gebruikt als menselijke interactie vereist is voor authenticatie, zoals bij het inloggen op een mailserver. Vaak wordt gebruik gemaakt van statische wachtwoorden. Statische wachtwoorden veranderen nauwelijks, wat voor kwetsbaarheden zorgt. Uiteraard is het enorm praktisch voor gebruikers om altijd hetzelfde wachtwoord te gebruiken, aangezien het makkelijk te onthouden is. Echter zijn statische wachtwoorden relatief eenvoudig te achterhalen, omdat ze niet vaak veranderen en een hacker dus uitgebreid de tijd heeft om het te kraken.

Als een wachtwoord constant verandert, is er minder tijd om deze te achterhalen. Daarom zijn one-time passwords, oftewel OTP, moeilijker te achterhalen. Een OTP is een wachtwoord dat bij elk gebruik wijzigt. Doordat het wachtwoord snel verandert, wordt het een stuk lastiger om ongeautoriseerd toegang te krijgen tot vertrouwelijke digitale bronnen, zoals gebruikersaccounts. OTP wordt bijvoorbeeld gebruikt door de meeste Nederlandse banken. Zij maken gebruik van een kaartlezer(bijvoorbeeld een Rabo-scanner) die, samen met een bankpas, ter plekke een OTP genereert. Met dit OTP wordt vervolgens toegang tot een bankaccount verstrekt.

**Asymmetrische en symmetrische cryptografie**

Symmetrische encryptie is een vorm van cryptografie waarbij zowel voor het versleutelen als het ontsleutelen van een bericht dezelfde sleutel gebruikt wordt. Omdat de ontvanger dezelfde sleutel moet gebruiken om het bericht te ontsleutelen als de sleutel waarmee de verzender het bericht versleuteld heeft, ontstaat een probleem. Hoe komt de sleutel veilig van verzender tot aan ontvanger? Deze zal via het internet verstuurd moeten worden naar de ontvanger, waardoor de kans aanwezig is dat een derde partij de sleutel kan onderscheppen, en dus al het verkeer tussen ontvanger en verzender af kan lezen.

Om dit probleem op te lossen, wordt gebruik gemaakt van asymmetrische encryptie. Bij asymmetrische cryptografie wordt gebruik gemaakt van twee verschillende sleutels. De ene sleutel versleutelt het te versturen bericht, terwijl de andere sleutel, de private key van de ontvanger van het bericht, het bericht weer kan ontsleutelen. Deze private key is dus de sleutel om berichten te ontsleutelen, en is enkel voor de ontvanger bekend. Niemand anders mag weten wat de private key van de ontvanger is. Als iemand bijvoorbeeld de sleutel van je brievenbus heeft, kan die persoon al je post lezen. Een populaire methode om asymmetrische encryptie toe te passen is het RSA-algoritme. Dit algoritme genereert verwante private en public keys, maar het is niet mogelijk om de private key te herleiden op basis van de public key.

Om asymmetrische encryptie toe te passen, moeten allereerst public keys uitgewisseld worden. Vervolgens gebruikt de verzender de public key van de ontvanger om het te verzenden bericht te versleutelen. Het verzonden bericht is enkel te ontsleutelen met de private key van de ontvanger. Zelfs de verzender kan dus het bericht niet meer ontsleutelen nadat het verstuurd is. Asymmetrische encryptie wordt bijvoorbeeld gebruikt door HTTPS websites en crypto wallets.

# 9 Business Continuity & Risk Mitigation

Business Continuity Management(BCM) is het maken van afspraken en het treffen van maatregelen met als doel de continuïteit van de werkzaamheden binnen een bedrijf te waarborgen. BCM is dus bedoeld om, in het geval van een incident, de effecten van dit incident te minimaliseren of, indien mogelijk, zelfs te voorkomen. Om goed in te kunnen schatten hoe groot de impact van een incident kan zijn, maakt men gebruik van Business impact analysis(BIA). Een BIA maakt onderscheid tussen verschillende risico’s op basis van de impact van een incident.

Risk mitigation is het voorbereiden en beperken van de effecten van een bedreiging. Er worden dus stappen genomen om de negatieve effecten van dreigingen te beperken.

### RTO en RPO

RTO, oftewel Recovery Time Objective is het streven om te voldoen aan een vooraf afgesproken hersteltijd na een incident. Een RTO van nul is natuurlijk niet haalbaar, maar een zo kort mogelijke hersteltijd is uiteraard wel het streven van ieder bedrijf. Om een RTO op te stellen moet bekend zijn hoelang het duurt om systemen opnieuw op te starten en wat de reactietijd van de IT-afdeling is. Natuurlijk geldt hierbij dat de RTO zo kort mogelijk hoort te zijn. Als het een week kost om weer volledig operationeel te zijn na een incident, loopt een bedrijf natuurlijk enorm veel geld mis, terwijl een kwartiertje te overzien is qua kosten.

Dat het systeem weer online is, betekent nog niet dat alle problemen verholpen zijn natuurlijk. Er is natuurlijk sprake van dataverlies als een systeem plotseling offline gaat. Om te voorkomen dat er teveel data en werk verloren gaat, wordt een Recovery Point Objective, oftewel RPO, afgesproken. Een RPO is het punt vanaf waar het systeem weer opgestart wordt na downtime. Een systeem wordt altijd vanaf een back-up weer opgestart, dus door zo vaak mogelijk back-ups te maken van een systeem, gaat zo min mogelijk werk verloren in het geval van een security-incident. Als de laatste back-up vijftien minuten geleden gemaakt is, raakt het bedrijf slechts vijftien minuten aan werk kwijt. Als de laatste back-up een uur geleden gemaakt is, kost het ineens een uur aan werk. Hoe meer werk er verloren gaat, hoe meer geld het kost.

# 10 IT System Hardening

System hardening is het proces van het zo moeilijk mogelijk maken om ongeautoriseerd toegang te krijgen tot een systeem door zoveel mogelijk veiligheidsrisico’s te elimineren. Door het aantal aanvalsvectoren te verkleinen, wordt gestreefd naar een veiligere applicatie. Om het aantal aanvalsvectoren te verminderen, is aan te raden om een systeem zo klein en compact mogelijk te houden. Dit houdt in dat overbodige functionaliteiten verwijderd dienen te worden. Hieronder staan een aantal potentiële aanvalsvectoren beschreven. Ook wordt beschreven hoe deze(gedeeltelijk) af te dekken zijn.

* **Default passwords.** Met geautomatiseerde password crackers zijn veel simpele wachtwoorden relatief snel te achterhalen. Wanneer een malafide gebruiker een wachtwoord achterhaalt, is de integriteit van het systeem in gevaar. Om dit te voorkomen, worden strengere eisen gesteld aan een wachtwoord. Zo moet een wachtwoord bijvoorbeeld minsten x aantal karakters bevatten, waarvan minstens één hoofdletter, één nummer en één ander teken. Zelfs met deze complexe wachtwoorden is het mogelijk om de wachtwoorden te kraken, het duurt alleen enorm lang.
* **Hardcoded passwords en andere credentials opgeslagen in plain text files.** Wanneer wachtwoorden en andere credentials in plain text, oftewel niet-versleuteld opgeslagen staan in een database, ontstaat er natuurlijk een enorm risico. Als iemand toegang tot de database weet te krijgen, liggen alle credentials van je systeem op straat, en zijn dus al je gebruikersaccount onveilig. Ook wachtwoorden en dergelijken in code zijn een risico. Wanneer bijvoorbeeld het wachtwoord van de database in de code te vinden is, en in de database alle wachtwoorden in plain text staan, is het heel eenvoudig om gevoelige data te achterhalen, want inbreken is niet moeilijk als de deur openstaat. Om dit te voorkomen, is aan te raden om alle credentials, overal in een systeem versleuteld op te slaan. Daarnaast is het aan te raden om zo min mogelijk wachtwoorden op te slaan buiten de centrale directory. Als een wachtwoord op meerdere plekken te vinden is, wordt de kans natuurlijk groter dat deze gevonden wordt.
* **Kwetsbaarheden door verouderde software.** Zorg er altijd voor dat alle services binnen je netwerk up-to-date zijn. Door middel van een update kunnen kwetsbaarheden gemitigeerd worden. Desondanks worden niet alle kwetsbaarheden verholpen met patches en updates. Bijvoorbeeld zero day kwetsbaarheden zullen niet gelijk gepacht kunnen worden.
* **Gebrek aan privileged acces control.** Wanneer acces control niet goed opgezet is, bestaat de kans dat gebruikers toegang hebben tot data of services die helemaal niet voor deze gebruiker bedoeld zijn. Een goede manier om met acces control om te gaan is “principle of least privilege”. Dit houdt in dat iedere gebruiker in principe geen enkel recht heeft, afgezien van eventuele publieke resources die voor iedereen toegankelijk zouden moeten zijn. Wanneer een gebruiker dan toch toegang moet krijgen tot bepaalde services of resources, kan alsnog toegang verleend worden. Op deze manier wordt voorkomen dat overbodige rechten toegekend worden.
* **Niet-versleuteld netwerkverkeer.** Als al het verkeer binnen je netwerk niet versleuteld is, geef je malafide gebruikers de mogelijkheid om alles af te lezen. Om dit te voorkomen, is het aan te raden om netwerkverkeer te versleutelen met behulp van een VPN. Een VPN, oftewel virtual private network, verbergt je daadwerkelijke IP-adres en versleutelt al het internetverkeer. Hierdoor is het een stuk lastiger om verkeer af te luisteren.

# 11 Wireless hacking

Als we spreken over wireless hacking, gaat het over het hacken van draadloze verbindingen, zoals wifi of bluetooth. Hieronder staat beschreven hoe een wifi netwerk dat gebruik maakt van WPA2 te hacken is met behulp van een “deauth” aanval en aircrack-ng.

1. Sluit een wifi-adapter aan en zet deze in monitor mode. Om deze adapter in monitor mode te krijgen moeten een aantal commando’s uitgevoerd worden.
   1. Allereerst is het belangrijk om airmon-ng check kill uit te voeren. Met dit commando worden alle netwerkmanagers uitgeschakeld. Hierdoor krijgt airmon-ng vrij spel.
   2. Nu alle netwerkmanagers uitgeschakeld zijn, is het tijd om de netwerkadapter in monitor mode te zetten, door middel van het volgende commando: airmon-ng start wlan0. Wlan0 is hierin dus de naam van de adapter interface. De adapter staat nu in monitor mode. Om te controleren of de adapter daadwerkelijk in monitor mode staat, wordt het volgende commando uitgevoerd: iwconfig.Graphical user interface, text

      Description automatically generated
2. Start airodump-ng om een handshake op te vangen. Met airodump-ng is het mogelijk om al het verkeer over een netwerk af te lezen en op te slaan in een lokaal bestand. Wanneer een device verbinding wil maken met het netwerk, wordt het wachtwoord dus vanaf dit device naar de access point verstuurd. Het wachtwoord wordt dus ook gelezen en in een file gedumpt.
   1. Om het netwerkverkeer af te lezen, moeten we natuurlijk wel een target kiezen. Door airmon-ng wlan0mon uit te voeren, wordt een lijst weergegeven met alle gevonden netwerken in de buurt. Hieruit wordt het target gekozen, en wordt het bijbehorende MAC-adres en channel genoteerd.
   2. Nu er een target gekozen is, in dit geval het netwerk behorende bij MAC-adres 2E:5F:FD:BF:E2:79(LucsNetwerk), kan het echte werk beginnen. Al het verkeer dat op dit access point voorbij komt dient afgelezen te worden, aangezien de volgende stap ervoor gaat zorgen dat er een handshake plaats gaat vinden. Met het volgende commando kan het verkeer afgelezen en opgeslagen worden: airodump-ng -c 1 --bssid 2E:5F:FD:BF:E2:79-w test wlan0mon. Hierin staat [-c 1] voor het gebruikte wifi kanaal, [-w test] is het bestand waar het verkeer in opgeslagen wordt. BSSID is het MAC-adres van het access point en wlan0mon is nog steeds de interface van de wifiadapter.

Text

Description automatically generated

1. Gebruik aireplay-ng om een deauth-aanval uit te voeren. Een deauth-aanval is het verstoren van de verbinding tussen een device en de access point. Omdat deze verbinding verstoord wordt, moet dit device opnieuw verbinden met het access point, en wordt de handshake dus opnieuw uitgevoerd. Aircrack kan hierdoor het wachtwoord afvangen.
   1. Met het volgende commando wordt een deauth-aanval gestart, en dus de verbinding tussen een voorheen verbonden apparaat en de access point verbroken: aireplay-ng -0 0 -a 2E:5F:FD:BF:E2:79 wlan0mon. hierin staat [-0] voor deauthentication, oftewel een deauth-aanval. [0] staat voor het aantal deauths dat verstuurd moet worden. In dit geval wordt 0 ingevoerd, wat inhoudt dat er deauths verstuurd blijven worden, tot het commando handmatig gestopt wordt. [-a 2E:5F:FD:BF:E2:79] staat voor het MAC-adres van het access point. Het is mogelijk om het MAC-adres van de client toe te voegen aan dit commando, door achter het MAC-adres van de access point [-c {MAC}] toe te voegen. Aangezien er geen MAC-adressen van clients bekend zijn, doen we dat in dit geval niet.

Text

Description automatically generated

1. Gebruik aircrack-ng om het wachtwoord te kraken. Aircrack-ng maakt gebruik van een password.lst-bestand, met daarin een hele verzameling van de meest voorkomende wachtwoorden. De hashes van deze wachtwoorden worden vergeleken met de hash van het onderschepte wachtwoord. Is er een match? Dan is het wachtwoord gekraakt.
   1. Indien de handshake opgevangen is met behulp van de deauth-aanval, kunnen we gaan proberen om het wachtwoord van het wifi netwerk te achterhalen. Hiervoor wordt het volgende commando gebruikt: aircrack-ng -w password.lst -b 2E:5F:FD:BF:E2:79 test\*.cap. [password.lst] staat hierin voor de dictionary file met daarin een lijst van veel voorkomende wachtwoorden. [test\*.cap] betekent dat de password.lst vergeleken moet worden met de alle data in alle bestanden die beginnen met test.

Calendar

Description automatically generated