# Verslag zwakhedenonderzoek

Datum: 25-5-2023

Auteur: Emircan Yeni

## Opdrachtgever

Directeur Acme

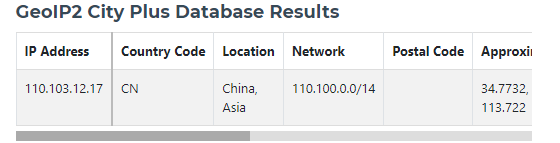
### Managementsamenvatting]

Extern ip   
Grote tijdverschil inlogpoging van Henk in de middag en avond van 12:32 tot 13:36 en 16:20 tot 17:26   
(waarschijnlijk aanwijzing aan datalek en zn traces verwijderd)   
Anne heeft wachtwoord maar staat niet dat het een credential is   
Anne werkt met een chinees IP?  
Anne is veel bestanden gaan kopiëren naar een externe IP   
Henk zonder wachtwoord maar staat wel bij hem dat het een credential is   
Henk heeft als user naam een hoofdletter H, maar in de logs zie je het staan als henk  
Bij Anne is het beide met hoofdletter A   
Bestandsoverdracht naar extern ip

### Overzicht onderzoek

[logboek van FTP server staat onder C:\Data\filezilla4.log,  
Beide gebruikers Anne en Henk hebben de FTP Server,  
De users ook bekeken, logboek bekeken alles sessions van Anne waren normaal   
maar die van Henk waren erg opvallend, maar dan nog dan heb je ook Anne die met een chinees IP werkt, GEOIP gebruikt   
]

### Gedetailleerde resutaten

[sessions van henk begint om 12:32 en stopt om 13:36 maar begint weer om 16:20 en stopt om 17:26, er is duidelijk een verwijdering van sessions hier tussen, Anne werkt met het IP 110.103.12.17 wat toelijd als een chinese IP,   
via GEOIP gezien dat dit een CN IP is  ]

### Conclusies

[Conclusie: Hoogstwaarschijnlijk is Anne de etische hacker, vooral omdat ze wel bestanden is gaan kopieren met een externe chinese IP, eerst dacht ik Henk vanwege hij een grote inlogtijd verschil had een verder in middag niet meer te zien was. Maar beide zijn IP was gwn als reserved IP address gezien, eerste IP die anne gebruikte was ook een reserved IP maar de 2e was gewoon een Chinese IP, en daar gaat het wel mis, ]

### Advies

[Extern IP = whitelisten/blacklisten-firewall-ACL   
Anne heeft wachtwoord maar staat dat ze geen wachtwoord hoeft = wachtwoord aanzetten voor anne.  
Henk heeft geen wachtwoord maar bij hem staat dat het aan is = geef henk een wachtwoord  
Bestandsoverdracht = Rechten]  
Anne’s details goed checken en bespreken

### Communicatieadvies

[De Directeur ]