MOHAMMAD **MUFTI**

Senior Penetration Tester at ZENDATA

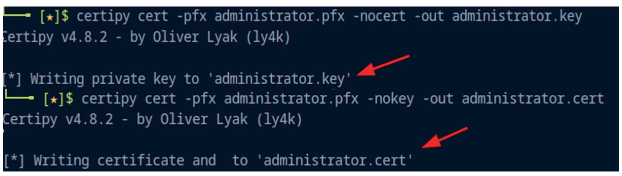
How I Took Over a Domain Controller with SentinelOne and FortiWeb Client Installed.

This is the story of how ZENDATA successfully took control of a domain during a Blackbox internal penetration test.

As always, we went through our checklists - most of the attacks where getting blocked by SentinelOne and FortiWeb, from dumping hashes, trying to achieve lateral movement and persistence. Our investigation revealed that the SMB shares on the Domain Controller had the CertEnroll Share open with read access.. And upon enumerating the certificates on the Domain Controller we identified vulnerabilities in ESC1, ESC4 and ESC8. ZENDATA consultants managed to fully exploit ESC1 and take over the domain by exploiting the "DC01-ca" certificate authority. Remarkably, this was accomplished using a non-domain joined machine with valid domain user credentials, thanks to a tool called "Certipy."

We added our own computer, named "ZENDATA_computer" to the Domain Controller using the pentest user credentials ("zendata") via the LDAP service. This was achieved by having a quota to add 100 computers (a privilege granted to any domain-joined user like ourselves.) - We verified this capability using netexec, an updated version of CrackMapExec (CME).

Subsequently we requested the CA "DC01-ca" and the template using the new computer we added to the DC "ZENDATA_computer" This process was successful, and we saved the administrator.pfx file to our local machine. Next, we converted the administrator.pfx file into a certificate and key.

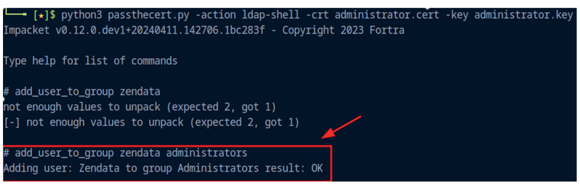


```
└──╼ [★]$ certipy cert -pfx administrator.pfx -nocert -out administrator.key
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing private key to 'administrator.key'
└──╼ [★]$ certipy cert -pfx administrator.pfx -nokey -out administrator.cert
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Writing certificate and  to 'administrator.cert'
```

Passing the cert and key, gave us access fully as an administrator through the LDAP service where we added the "zendata" user to the domain administrators and Remote Desktop Users group granting us complete access to both the Primary and Secondary Domain Controllers..



```
└──╼ [★]$ python3 passthecert.py -action ldap-shell -crt administrator.cert -key administrator.key
Impacket v0.12.0.dev1+20240411.142706.1bc283f - Copyright 2023 Fortra

Type help for list of commands

# add_user_to_group zendata
not enough values to unpack (expected 2, got 1)
[-] not enough values to unpack (expected 2, got 1)

# add_user_to_group zendata administrators
Adding user: Zendata to group Administrators result: OK
```

Attacks such as DCSync can be achieved using a tool called "impacket-secretsdump" (not limited to this tool though) which will allow the dump of all machines and users credentials, leading to a complete domain takeover. - PTH (Pass-The-Hash) can be used to login to any machine on the domain.

> "We had full access to Primary and Secondary Domain Controllers.
>
> Mohammad MUFTI
> Senior Penetration Tester at ZENDATA

Always in movement to protect

our team.