

How I Met Your Printer

Tom Pohl
Pentest Team Manager



LMG
SECURITY



whoami

- **Tom Pohl @tompohl**
- Pentest Team Manager, LMG Security
- With SecDSM won CTF competitions at:
 - DEFCON
 - BSidesLV
 - THOTCON
 - 2 x Wild West Hackin' Fest
 - 3 x Circle City Con
- **An Evil Twin (Hi, Andy!)**



Hard at work!



greetz



Roadmap

- Why Hack Printers?
- How to Get Into the Printer
- Method #1: LDAP
- Method #2: Email
- Method #3: Scan-to-File-share
- Beyond Printers!
- How to Protect Your Organization

Before We Start

- Cell phones (you know the drill)
You WILL feel the need to call someone in the middle of the presentation, take a deep breath, it'll be ok.
- Shot glasses



Why Hack Printers?



How to Get into Printers...

Username and Password on Xerox Printers

Posted on February 2, 2022 by [Cheryl Otstott](#) | [Security, Support Tools](#) | [0 comments](#)

We receive many questions about the username and password on Xerox print multifunction devices (MFD). The username and password are required for system administrator access to the printer and the embedded web server (EWS). The password can help to safeguard your machine from unwanted settings changes.

The default password will be 1111 on most printers or the serial number of the printer. The password on most devices is case sensitive, so if your serial number contains letters, use the correct case.

<https://atyourservice.blogs.xerox.com/2022/02/02/username-and-password-on-xerox-printers/>

Default Credentials!
OR no credentials at all!

Default Passwords List

A few default device passwords that have come in handy over the years... [Drop me a line](#) if you have some to add and we would gladly do so :D

Dell	Laser Printer 3000cn / 3100cn	admin	password
Hewlett-Packard	LaserJet Net Printers	(none)	(none)
Hewlett-Packard	LaserJet Net Printers	(none)	(none)
Hewlett-Packard	LaserJet Net Printers	Anonymous	(none)
Hewlett-Packard	LaserJet Net Printers	(none)	(none)

<https://bizuns.com/default-passwords-list>



But Sometimes Default Credentials Don't Work...

RICOH

Web Image Monitor

Login User Name :

Login Password :

Login

Cancel

🌐 10.55.10.30

Authentication has failed.

OK




Let's Try the "Supervisor" Password...

RICOH
Web Image Monitor

Login User Name :

Login Password :



The password is blank!
(Yes, this really worked)



Now Let's Change the Admin Password!

RICOH MP C3004 Web Image Monitor

Home

Administrator

Program/Change Administrator

OK Cancel

User Administrator : ☒ Administrator 1 ☐ Administrator 2 ☐ Administrator 3 ☐ Administrator 4

Machine Administrator : ☒ Administrator 1 ☐ Administrator 2 ☐ Administrator 3 ☐ Administrator 4

Network Administrator : ☒ Administrator 1 ☐ Administrator 2 ☐ Administrator 3 ☐ Administrator 4

File Administrator : ☒ Administrator 1 ☐ Administrator 2 ☐ Administrator 3 ☐ Administrator 4

Administrator 1

Login User Name : admin

Login Password :

Administrator 2

Login User Name :

Login Password :

Administrator 3

Login User Name :

Login Password :

Administrator 4

Login User Name :

Login Password :

Supervisor

Login User Name : supervisor

Login Password :

Administrator 1

Login User Name : admin

Login Password :

[Note] SSL communication is currently unavailable. The following items will be transmitted without being encrypted.

New Password :

Confirm Password :

OK

Cancel

Success!


RICOH MP C3004 Web Image Monitor

English Switch Refresh ?

Home

Status/Information Device Management

Device Name : RICOH MP C3004 Comment :
Location : Host Name :
Control Panel : Smart Operation Panel



Alert

- Alert
- Messages (1item(s)) Toner Cartridge is almost empty. Magenta, Yellow
Prepare toner cartridge replacement(s).
Magenta, Yellow

Status

- System Status OK
- Toner Cartridge Almost Empty
- Waste Toner Bottle Status OK
- Input Tray Almost Out of Paper
- Output Tray Paper Left on Output Tray

Check Details



Why Steal Passwords...

- ...when printers will just GIVE them to you?
- Pass-back attacks
 - Get the device to send you a password
 - So you don't have to steal it
- Methods we will cover:
 - LDAP
 - SMTP
 - File Shares




LDAP – Lightweight Directory Access Protocol

- Stands for Lightweight Directory Access Protocol
- Provides a hierarchical structure for organizing directory information
- Used in authentication, authorization, email, file sharing, and other networked applications.



Let's Trick a Konica Minolta into Giving Us a Password




KONICA MINOLTA

is waiting phone
line connected to
network. Fax is
disabled.

Refresh

KONICA MINOLTA bizhub 4020
Address: 10.71.0.253
Contact Name:
Location:



- ▶ Device Status
- ▶ Scan Profile
- ▶ Copy Printer Settings
- ▶ Settings
- ▶ Reports
- ▶ Links & Index
- ▶ Applications
- ▶ Set up Scan to Network
- ▶ Remote Operator Panel

Online Assistance

Contact KM Support at:
www.konicaminolta.com

Settings

Network/Ports

- TCP/IP
- IPv6
- IPSec
- SNMP
- 802.1x
- AppleTalk
- Custom Link Setup
- General Network Settings (Active Card)
- Reset Print Server
- SMTP Setup
- Select Active Network Card
- Address Book Setup
- Standard Network
- Standard USB



KONICA MINOLTA bizhub 4020

10.71.0.253

KONICA MINOLTA

Refresh

KONICA MINOLTA bizhub 4020
Address: 10.71.0.253
Contact Name:
Location:

Device Status

Scan Profile

Copy Printer Settings

Settings

Reports

Links & Index

Applications

Set up Scan to Network

Remote Operator Panel

Online Assistance

Contact KM Support at:
www.konicaminolta.com

Settings

Address Book Setup

Server Address

hackme.local

Server Port

3268

Use SSL/TLS

None

LDAP Certificate Verification

Demand

Use GSSAPI

☒

Mail Attribute

mail

Fax Number Attribute

facsimiletelephonenumber

Search Base

Search Timeout

30

Range: 5-300 seconds.

Displayed Name

Longest of cn or (givenName + sn)

Max Search Results

100

Range: 5-500.

Use user credentials

☐

Device Credentials

Search Attributes

Search specific object classes

Manage LDAP Servers (Security)

Manage LDAP+GSSAPI Servers (Security)

Original Server Settings

Default 389 for LDAP. Choose 3268 for Global Catalog or 636 for SSL

After this setting is changed the device must be powered off (and then back on) for the changes to be applied.

English

Français

Deutsch

Italiano

Español

Dansk

Norsk

Nederlands

Svenska

Português

Suomi

Русский

Polski

Magyar

Türkçe

Česky

简体中文

繁體中文

한국어

日本語

ελληνικά

- ▶ Device Status
- ▶ Scan Profile
- ▶ Copy Printer Settings
- ▶ Settings
- ▶ Reports
- ▶ Links & Index
- ▶ Applications
- ▶ Set up Scan to Network
- ▶ Remote Operator Panel

Online Assistance

Contact KM Support at:
www.konicaminolta.com

Settings

Address Book Setup

Server Address	<input type="text" value="44.230.248.34"/>
Server Port	<input type="text" value="389"/>
Use SSL/TLS	<input type="text" value="389"/>
LDAP Certificate Verification	<input type="text" value="Demand"/>
Use GSSAPI	<input checked="" type="checkbox"/>
Mail Attribute	<input type="text" value="mail"/>
Fax Number Attribute	<input type="text" value="facsimiletelephonenumber"/>
Search Base	<div></div>
Search Timeout	<input type="text" value="30"/>
Displayed Name	<input type="text" value="Longest of cn or (givenName + sn)"/>
Max Search Results	<input type="text" value="100"/>
Use user credentials	<input type="checkbox"/>
Device Credentials	
Search Attributes	
Search specific object classes	
Manage LDAP Servers (Security)	

Attacker Server Settings




Default 389 for LDAP. Choose 3268 for Global Catalog or 636 for SSL

After this setting is changed the device must be powered off (and then back on) for the changes to be applied.

Range: 5-300 seconds.

Range: 5-500.



KONICA MINOLTA

▶ Device Status

▶ Scan Profile

▶ Copy Printer Settings

▶ Settings

▶ Reports

▶ Links & Index

▶ Applications

▶ Set up Scan to Network

▶ Remote Operator Panel

Online Assistance

Contact KM Support at:
www.konicaminolta.com

No scanning glass
lens connected to
network. Scan as
download.

Refresh

Server Port

Use SSL/TLS

LDAP Certificate Verification

Use GSSAPI

Mail Attribute

Fax Number Attribute

Search Base

Search Timeout

Displayed Name

Max Search Results

Use user credentials

Device Credentials

Search Attributes

Search specific object classes

Manage LDAP Servers (Security)

Manage LDAP+GSSAPI Servers (Security)

Submit

Reset Form

Test

test

Search Address Book

After submitting any changes, use this button to verify the authentic

```
> Frame 4: 111 bytes on wire (888 bits), 111 bytes captured (888 bits)
> Ethernet II, Src: 06:e1:c0:cc:81:2d (06:e1:c0:cc:81:2d), Dst: 06:f8:42:ec:58:93 (06:f8:42:ec:58:93)
> Internet Protocol Version 4, Src: 66.109.141.14, Dst: 172.26.8.21
> Transmission Control Protocol, Src Port: 60599, Dst Port: 389, Seq: 1, Ack: 1, Len: 45
> Lightweight Directory Access Protocol
  > LDAPMessage bindRequest(1) "ET0021B761CD91$" simple
    messageID: 1
    > protocolOp: bindRequest (0)
      > bindRequest
        version: 3
        name: ET0021B761CD91$
        > authentication: simple (0)
          simple: 42w7gK9M-b6(+676
```



SMTP – Simple Mail Transfer Protocol

- Standard protocol used for sending email messages between servers on the internet
- Defines how email messages are transmitted and delivered over networks
- Widely used for both personal and business email communication.



Let's Convince This Kyocera to Give Us an Email Password

- Why do printers have email access?
 - Send documents to your email!
- Scan a physical doc to a PDF and have it emailed
- Needs an email account to work
- That's where we come in...

Device	Status
Printer	Ready.
Scanner	Ready.
FAX	Ready.
Status Message	Ready.

Source	Size	Type	Capacity	Status
Cassette 1	Legal	Plain	500	70 %
Cassette 2	Ledger	Plain	500	100 %
Cassette 3	Letter	Plain	1500	100 %



SMTP

SMTP Protocol :

On

Note :

Settings must be made in SMTP (E-mail [Protocol](#))

SMTP Server Name :

smtp.office365.com

Note :

To specify the server name by domain name, set DNS server. [TCP/IP](#)

SMTP Port Number :

587 (1 - 65535)

SMTP Server Timeout :

60 seconds

Authentication Protocol :

On

Authentication as :

Other

Login User Name :

copier@

Login Password :

SMTP Security :

STARTTLS

Note :

Make settings here. [Proto](#)

Connection Test :

Test

The printer will login to office365.com with a domain username and password!

We'll change that to OUR evil server

The creds we want to steal

Testing will send the credentials!

Let's Turn TLS Off

Send Protocols

SMTP (E-mail TX) :

☒ On ☐ Off

Note :

For more settings, click here. [E-mail Settings](#)

SMTP Security :

✓ STARTTLS
SSL/TLS
Off

FTP Client (Transmission) :

☒ On ☐ Off

Port Number :

21 (1 - 65535)

FTP Encryption TX :

☐ On ☒ Off

Note :

To use these settings, enable SSL. [Network Security](#)

SMB :

☒ On ☐ Off

Port Number :

445 (1 - 65535)

Use Temporary File Name :

☐ On ☒ Off

We don't need security 😊



Come to Papa!



```
[SMTP] Cleartext Client      : [REDACTED]  
[SMTP] Cleartext Username   : copier@[REDACTED]  
[SMTP] Cleartext Password   : [REDACTED]  
[SMTP] Cleartext From       : [REDACTED]  
[SMTP] Cleartext To         : [REDACTED]
```



Now Let's Steal Creds From a Ricoh

- This was harder...
- There was no “test” button!
- But see all those warnings....?

RICOH MP C3004 Web Image Monitor

Home


English Switch Refresh ?

Administrator

Status/Information
Device Management

■ Device Name : RICOH MP C3004
■ Location :
■ Control Panel : Smart Operation Panel

■ Comment :
■ Host Name : [REDACTED]



Alert

■ Alert
■ Messages (1item(s)) Toner Cartridge is almost empty. Magenta, Yellow
Prepare toner cartridge replacement(s). Magenta, Yellow

Status

■ System
■ Toner
■ Waste Toner Bottle
■ Input Tray
■ Output Tray

■ Status OK
■ Cartridge Almost Empty
■ Status OK
■ Almost Out of Paper
■ Paper Left on Output Tray

Check Details



Reception

- Reception Protocol : SMTP ▾
- Email Reception Interval : ☒ On ☐ Off
: 15 minute(s)
- Max. Reception Email Size : 10 MB
- Email Storage in Server : Off ▾

SMTP

- SMTP Server Name : protection.outlook.com
- SMTP Port No. : 25
- Use Secure Connection (SSL) : ☐ On ☒ Off
- SMTP Authentication : ☐ On ☒ Off
- SMTP Auth. Email Address :
- SMTP Auth. User Name :
- SMTP Auth. Password : Change
- SMTP Auth. Encryption : Inactive ▾

The SMTP server name (we'll change this to our own evil server)

Authentication was turned off!
But there was a username and password stored in the system anyway

Reception

- Reception Protocol : SMTP ▾
- Email Reception Interval : ☒ On ☐ Off
: 15 minute(s)
- Max. Reception Email Size : 10 MB
- Email Storage in Server : Off ▾

SMTP






- SMTP Server Name :
- SMTP Port No. : 25
- Use Secure Connection (SSL) : ☐ On ☒ Off
- SMTP Authentication : ☒ On ☐ Off
- SMTP Auth. Email Address :
- SMTP Auth. User Name :
- SMTP Auth. Password : Change
- SMTP Auth. Encryption : Inactive ▾

Now this is our evil server

This time we want security 😊

javascript:wsMenu_jumpUrl('.././websys/netw/getSysLog.cgi',000);

- Now how do we trigger an email?
- We have to wait for someone to scan a document to email ...
- ... OR turn on ALL the notifications
- If there's any issues, send us the alerts! Instantly!
- Remember...

■ System	 Status OK
■ Toner	 Cartridge Almost Empty
■ Waste Toner Bottle	 Status OK
■ Input Tray	 Almost Out of Paper
■ Output Tray	 Paper Left on Output Tray

Auto Email Notification

■ Notification Message :

Groups to Notify

■ Group 1 :	Name : Group-1	<input type="button" value="Edit"/>
	Address List : <input type="text"/>	
■ Group 2 :	Name : Group-2	<input type="button" value="Edit"/>
	Address List : <input type="text"/>	
■ Group 3 :	Name : Group-3	<input type="button" value="Edit"/>
	Address List : <input type="text"/>	
■ Group 4 :	Name : Group-4	<input type="button" value="Edit"/>
	Address List : <input type="text"/>	

Select Groups/Items to Notify

	Group-1	Group-2	Group-3	Group-4
■ Call Service	: <input checked="" type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify
■ Out of Toner	: <input checked="" type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify
■ Toner Almost Empty	: <input checked="" type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify
■ Paper Misfeed	: <input checked="" type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify
■ Cover Open	: <input checked="" type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify
■ Out of Paper	: <input checked="" type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify
■ Almost Out of Paper	: <input checked="" type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify	<input type="checkbox"/> Notify

Instantly We Received an Email!

```
[SMTP] Cleartext Client : [REDACTED]  
[SMTP] Cleartext Username : [REDACTED]  
[SMTP] Cleartext Password : [REDACTED]
```

...along with the SMTP credentials!

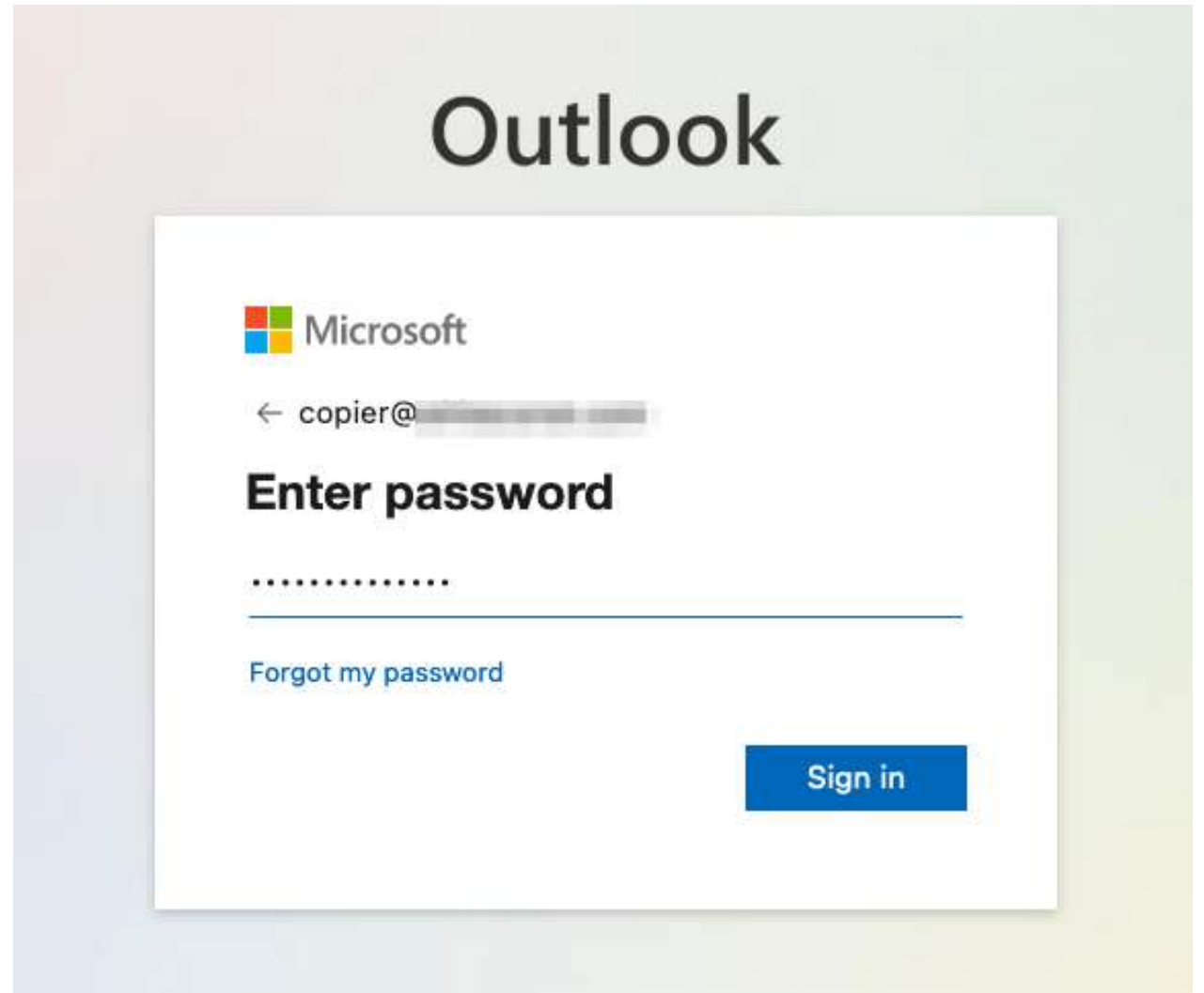
Oh and this account was a Domain Administrator.
So at this point, we ruled their ENTIRE network!

In our experience, 40% of the time, printer creds
are Domain Administrator 100% of the time!

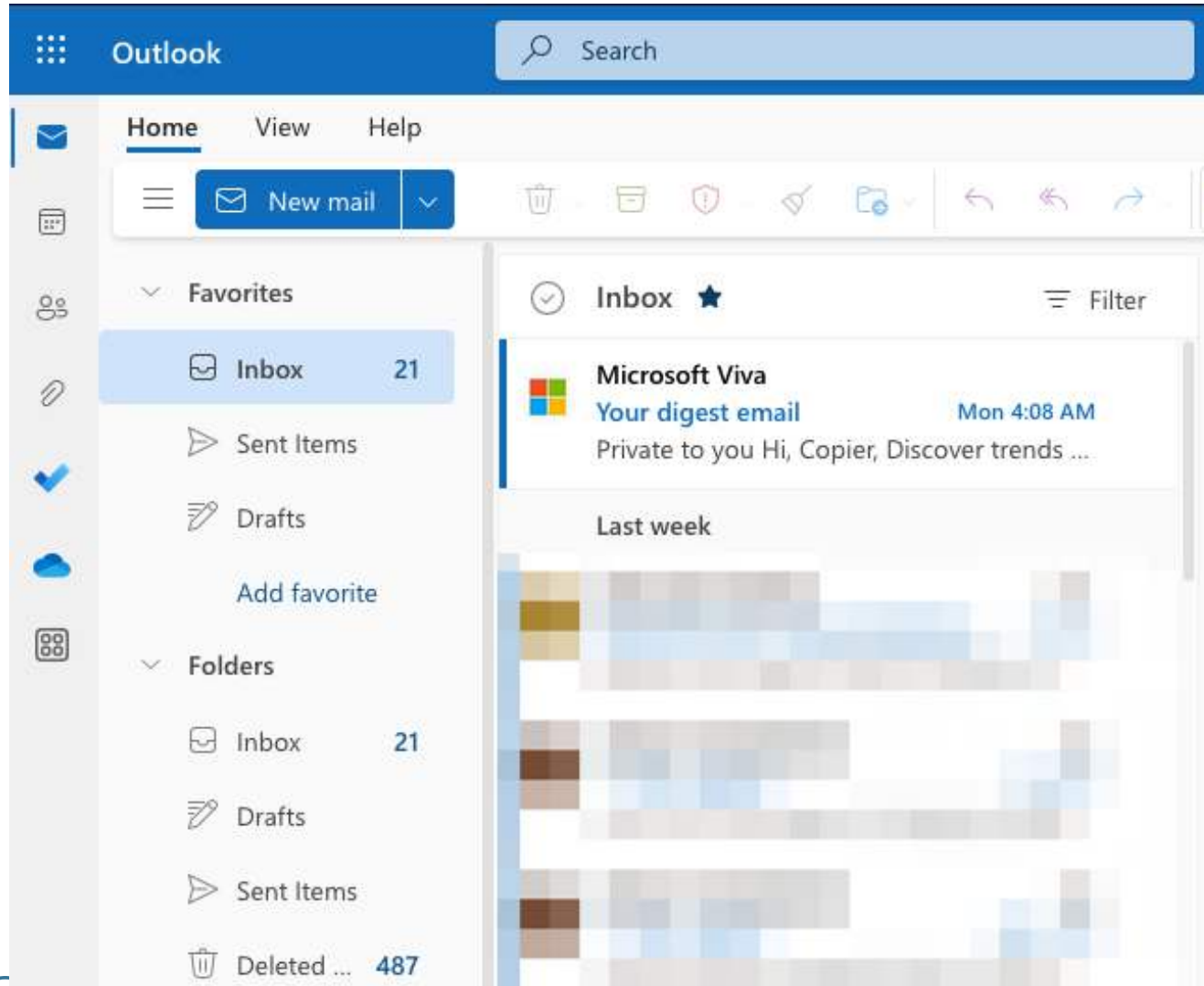


Taking it to the Next Level

- Let's try the stolen password in Microsoft 365
- It works!



The Copier's Inbox

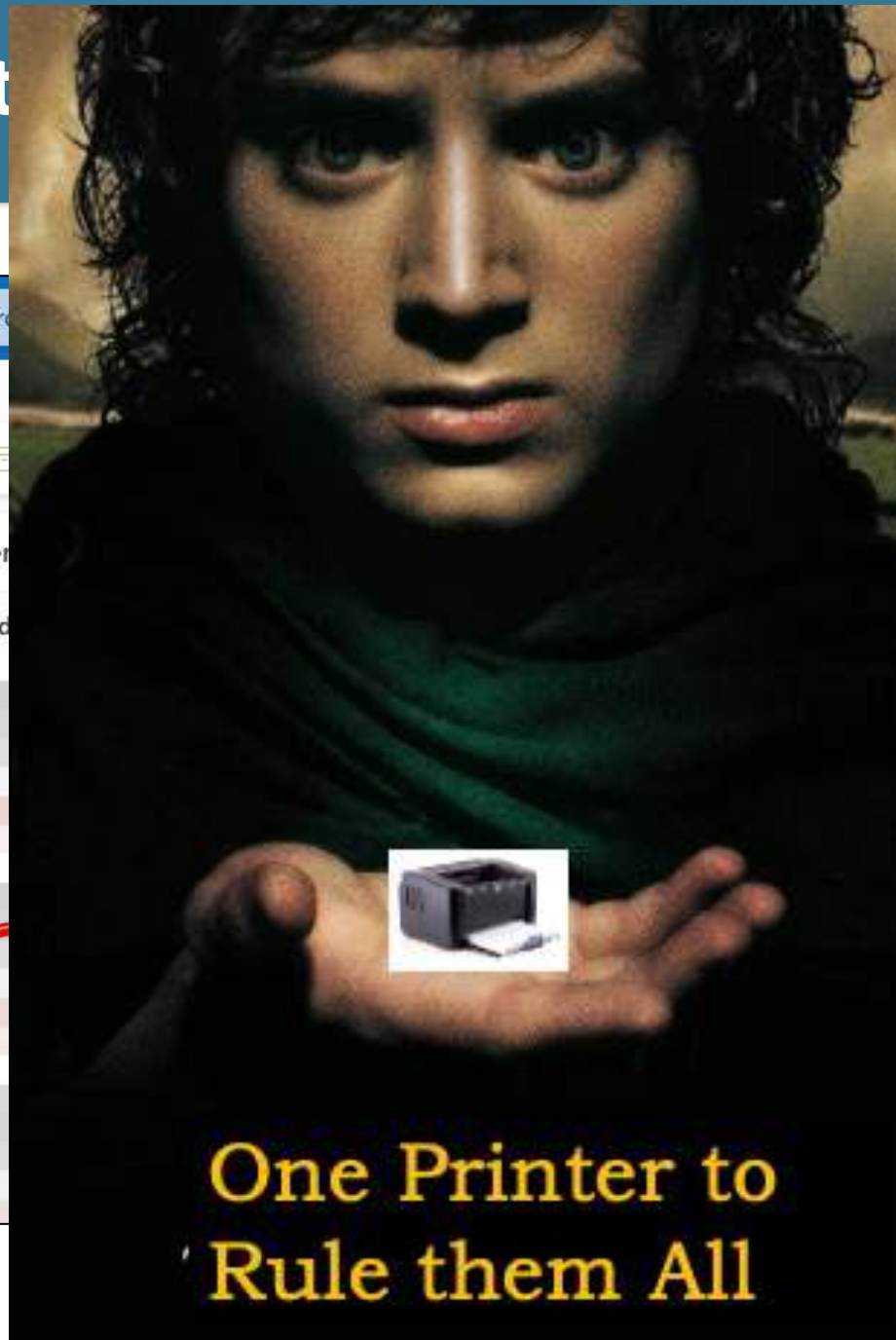
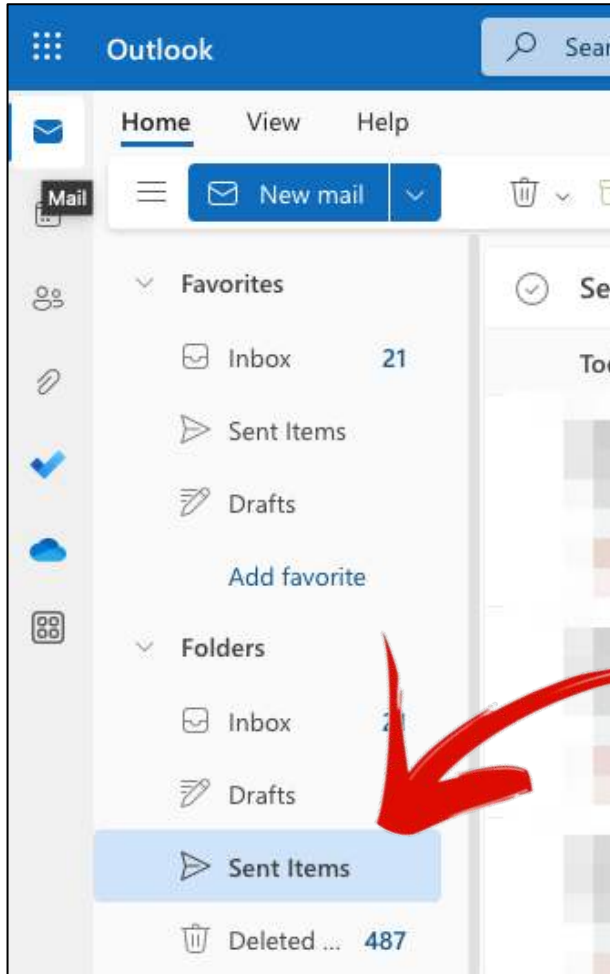


Typically the inbox contains autoreplies...



We Can See All t

Ever Scanned



tems has all the
ed documents
that printer,
very other printer
entire organization
not sorry for all the
tion...

was a lot of
ive stuff in there!



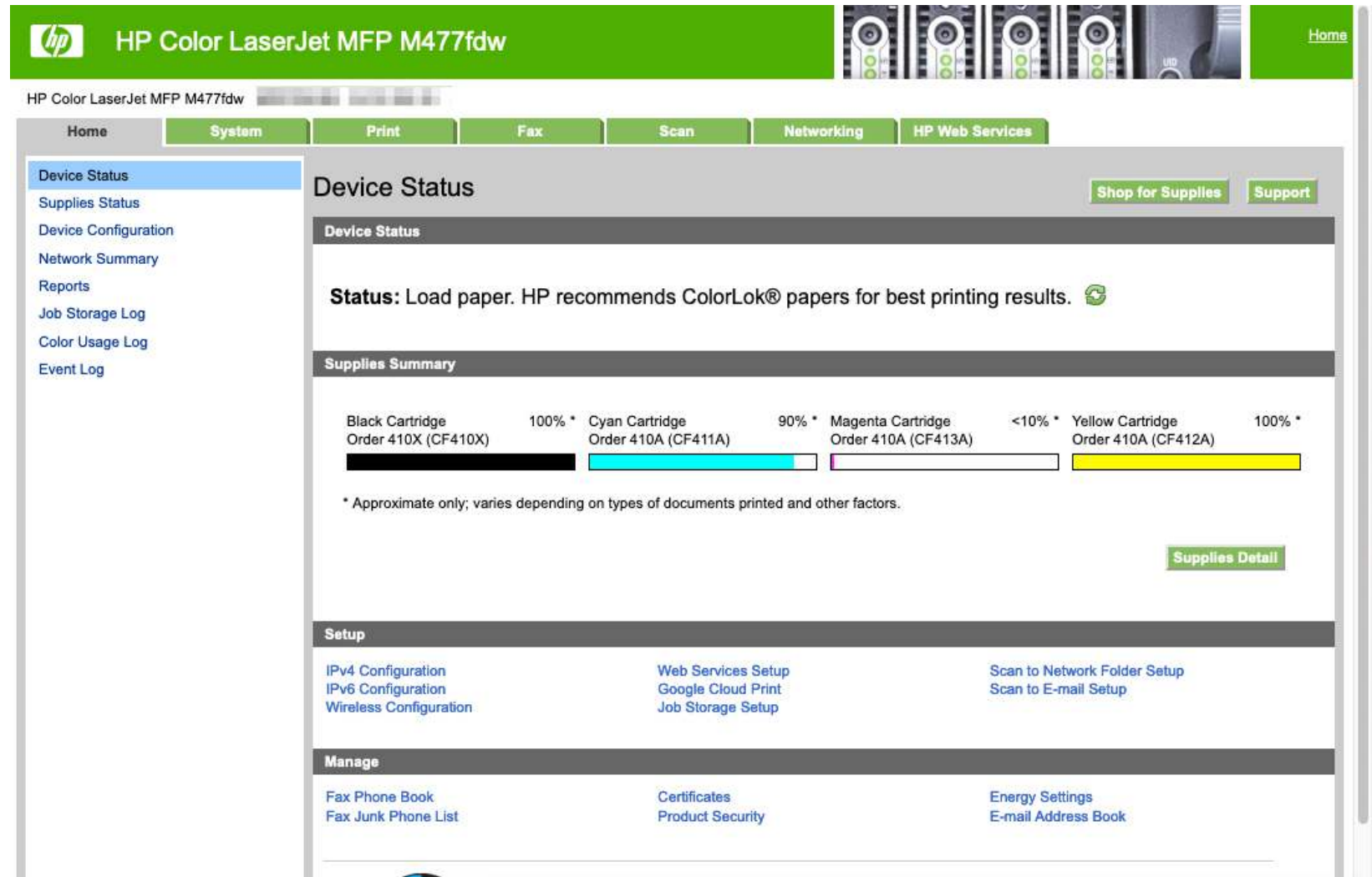
Scan to File Shares

- Uses SMB (Server Message Block)
- Network protocol used for file and printer sharing between computers on a local area network (LAN)
- Provides a way for computers running Windows operating systems to share files, printers, and other resources with each other.



Let's Attack an HP Printer

- Printer/scanner
- No authentication at all
 - Not even default creds
- Wide open



The screenshot displays the HP Color LaserJet MFP M477fdw web interface. The top navigation bar includes links for Home, System, Print, Fax, Scan, Networking, and HP Web Services. The left sidebar lists various status and configuration options. The main content area shows the Device Status, Supplies Summary, Setup, and Manage sections.

Device Status

Status: Load paper. HP recommends ColorLok® papers for best printing results.

Supplies Summary

Black Cartridge	Cyan Cartridge	Magenta Cartridge	Yellow Cartridge
Order 410X (CF410X)	Order 410A (CF411A)	Order 410A (CF413A)	Order 410A (CF412A)
100% *	90% *	<10% *	100% *

* Approximate only; varies depending on types of documents printed and other factors.

Setup

- IPv4 Configuration
- IPv6 Configuration
- Wireless Configuration
- Web Services Setup
- Google Cloud Print
- Job Storage Setup
- Scan to Network Folder Setup
- Scan to E-mail Setup

Manage

- Fax Phone Book
- Fax Junk Phone List
- Certificates
- Product Security
- Energy Settings
- E-mail Address Book



[Home](#)

HP Color LaserJet MFP M477fdw

[Home](#)

System

Print

Fax

Scan

Networking

HP Web Services

Scan to Network Folder

Network Folder Setup

Scan to E-mail

[Scan to E-mail Setup](#)

Outgoing E-mail Profiles

Default SMTP Configuration

[E-mail Address Book](#)

Network Contacts Setup

E-mail Options

Scan to Network Folder

[Shop for Supplies](#)

Support

Network Folder Configuration

To add a new network folder entry, click [New] and enter the required information, then click [Save and Test] or [Save Only] at the bottom of the page. The new entry will be added to the list.

Note: The folder you are using must already exist on a computer co

Now

Delete

Network Folder Information

Select	Display Name	Network Path	
<input type="checkbox"/>	Scan to S: drive	\\[redacted]Scans	Edit Test

Anything you scan goes to a folder on the "S:" drive

Scan to Network Folder

[Shop for Supplies](#)[Support](#)

Network Folder Information

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

[Go to HTTPS Enforcement page.](#)

* required field

Display Name *

e.g. Invoices

Network Path *

e.g. \\mypc\sharedfolder

We changed the path to be our evil server

The printer might need to authenticate itself on your network before it can save documents to a network folder. Enter your username and password to allow this authentication to take place so that the printer can have write access to the selected network folder.

Username

e.g. Bob, BOBSPC\Bob, BOBDOMAIN\Bob

Password

The creds we want to steal

Scan to Network Folder

[Shop for Supplies](#)

[Support](#)

Network Folder Configuration

To add a new network folder entry, click [New] and enter the required information, then click [Save and Test] or [Save Only] at the bottom of the page. The new entry will be added to the list.

Note: The folder you are using must already exist on a computer connected to the network.

[New](#)

[Delete](#)


Let's test it! (This will trigger an NTLMv2 handshake with our evil server)

Network Folder Information

Select	Display Name	Network Path	
<input type="checkbox"/>	Scan to S: drive	\\[redacted]Scans	Edit Test

On Our Evil Server...

```
[SMB] NTLMv2-SSP Client      : [REDACTED]  
[SMB] NTLMv2-SSP Username   : [REDACTED] ecopy  
[SMB] NTLMv2-SSP Hash       : ecopy::[REDACTED]
```



We've received an NTLMv2 handshake, which means now we have a hash that we can try to crack!

```
[SMB] NTLMv2-SSP Client      : [REDACTED]  
[SMB] NTLMv2-SSP Username   : [REDACTED] ecopy  
[SMB] NTLMv2-SSP Hash       : ecopy::[REDACTED]
```



Password Cracking

- Let's toss that in LMG's password cracking rigs!
- Attempt BILLIONS of guesses per second
- If the encrypted hash matches, the guess is right
- Took 1.5 seconds to crack the password
 - It was "canon1"



LMG Security @LMGSecurity · Jul 27

Brand new UberKraken brains! 6 @nvidia GTX1080s. Capable of cracking pwds at 9.84 billion NTLMv2/s!!



Beyond Printers...

- Same tactics, different devices
- Here we see a Supermicro server
- Use it to build/reboot a box
- Logged in w default creds
- Uses domain creds to pull data off a network share
- Yeah, we stole those...

The screenshot shows the Supermicro server management web interface. The browser address bar displays a URL ending in `cgi/url_redirect.cgi?url_name=mainmenu`. The page header includes the Supermicro logo and a 'Host Identification' box showing 'Server: [redacted]' and 'User: ADMIN (Administrator)'. A navigation menu contains tabs for System, Server Health, Configuration, Remote Control, Virtual Media, Maintenance, and Miscellaneous. On the left, a sidebar lists 'Virtual Media', 'Floppy Disk', and 'CD-ROM Image' (the active section). The main content area is titled 'CD-ROM Image' and contains a text box explaining that this option allows sharing a CD-ROM image over a Windows share with a maximum size of 4.7GB. Below this, there are three rows for 'Device 1', 'Device 2', and 'Device 3', each with the status 'No disk emulation set.' and a 'Refresh Status' button. At the bottom, there are input fields for 'Share Host', 'Path to Image' (containing '\\iso\truenas12.iso'), 'User (optional)', and 'Password (optional)'. A red arrow points to the 'Path to Image' field. To the right of the arrow, a text box says 'The creds we want to steal'. At the bottom of the form are 'Save', 'Mount', and 'Unmount' buttons.



Now You Know Why

i



The Road We've Traveled

- Printers are everywhere!
- Pass-Back Attacks
 - Email
 - SMTP
 - File Shares
- Beyond Printers
- How Can You Protect Your Printers?



Tips to Defend Yourself & Your Printers

1. Segment your network
 - Don't let random people even reach the mgmt. interface
2. Require Authentication for Printer Interfaces
3. Use STRONG passwords (no default pwds!)
4. Require encrypted authentication
5. Use app passwords on cloud interfaces
6. Deploy Identity and Access Management
 - Detect printer account abuse
7. Burn your printers



Questions?

- Tom Pohl, Pentest Team Manager
- info@LMGsecurity.com



@tompohl



tompohl@infosec.exchange

- Find me on **LinkedIn**





Please contact us any time you have a question or need additional support.

145 W Front Street
Missoula, Montana 59802

406-830-3165
1-855-LMG-8855

info@LMGsecurity.com
[LMGsecurity.com](https://www.LMGsecurity.com)