

Information Technology Services



Hewlett-Packard Printer Setup for Secure Banner HTTPS Printing

Contents

Hewlett-Packard Printer Setup for Secure Banner HTTPS Printing.....	1
There Are A Few Knobs To Tweak.....	1
Printers That We Know Work	1
Updating the SSL Certificates	2
Authorization	2
Certificate One	3
Management Protocols.....	4
Certificate Two	5
Linux/UNIX Machine With nmap Installed.....	7
Command One	7
Command Two	8
Notes For Firmware Updates	9

Hewlett-Packard Printer Setup for Secure Banner HTTPS Printing

ITS has configured how to securely print via HTTPS from a Banner DB server to a remote Hewlett-Packard (HP) printer. We have not tested any other printer brands.

Disclaimer: This setup has been tested on newer HP printers, there may be unnecessary steps listed. If you have tips that can save others time, please share through email and we'll update this document.

There Are A Few Knobs To Tweak

- Ensure that your campus firewall is open to the Banner hosted networks printer from 168.25.50.0/24 and 168.25.55.0/24 for ports 443 (HTTPS or SSL), 515 (lpd), and 9100 (HP raw printing.)
- Ensure that the firmware is reasonably new. We have not found an exact cutoff for working versus nonworking firmware, but anything within the past two years should be fine. Please email more as you find them. Some firmware installation guidelines are included at the bottom of this document, if you need a refresher on installation.

Printers That We Know Work

HP M804:

Firmware Bundle Version: 3.2.5

Firmware Revision: 2302908_435012

Firmware Date Code: 20140529

HP Color LaserJet CP4025:

20150731 07.220.2 (from the diagnostics page)

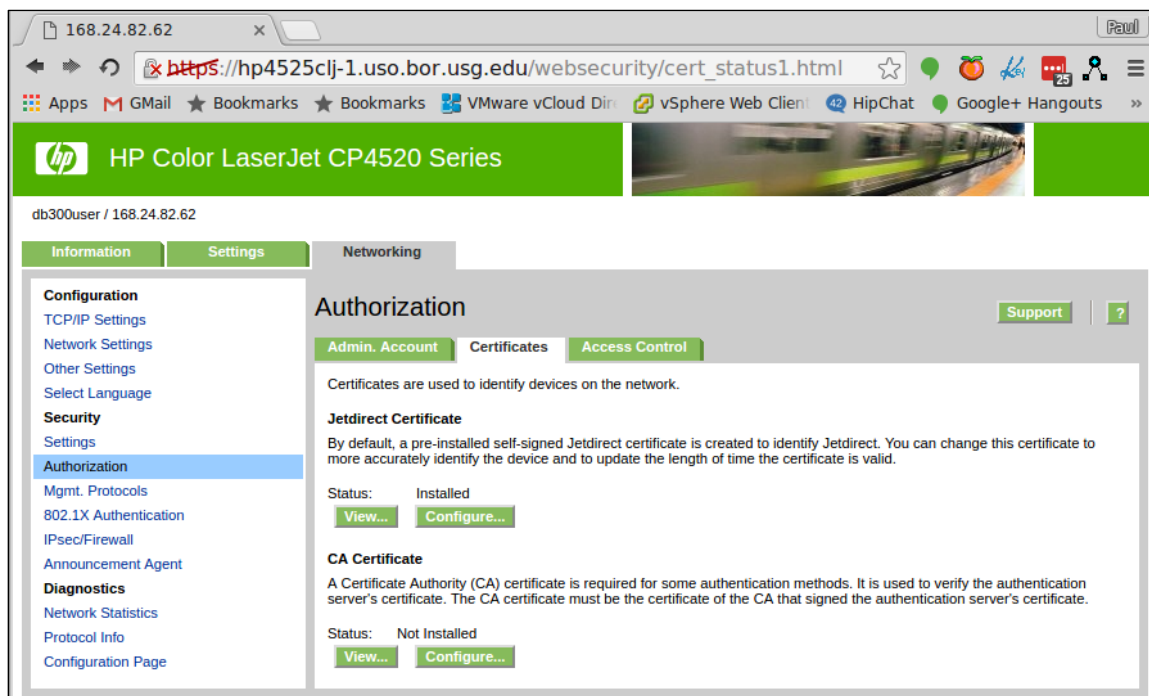
Updating the SSL Certificates

Two SSL certificates should be updated in the HP printer.

Authorization

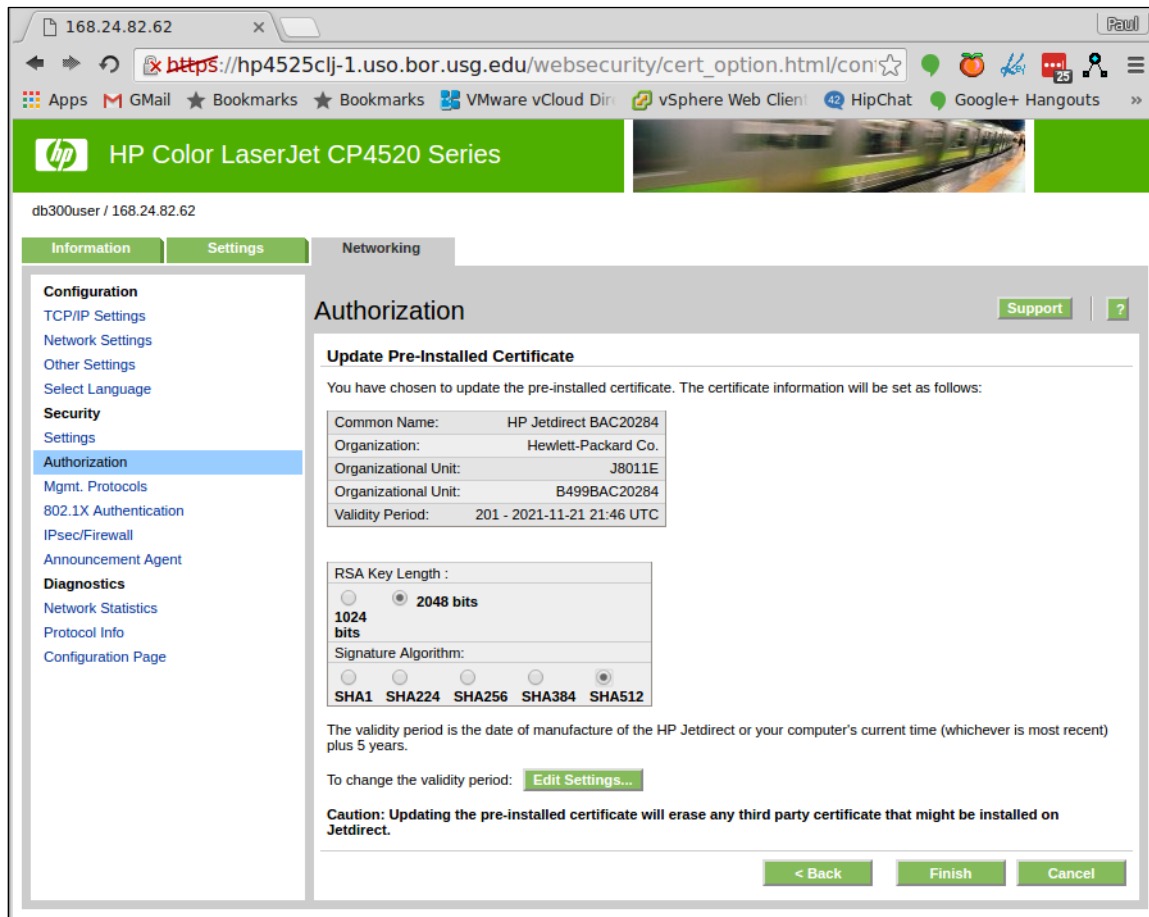
Start by selecting the **Networking** tab along the top.

- Select **Authorization** in the left navigation.
- Select the **Certificates** tab in the sub window.
- Select the **Configure** button under Jetdirect Certificate.



Certificate One

Create a new self-signed certificate with RSA Key Length: 2048 bits or higher, Signature Algorithm: SHA256 or higher.

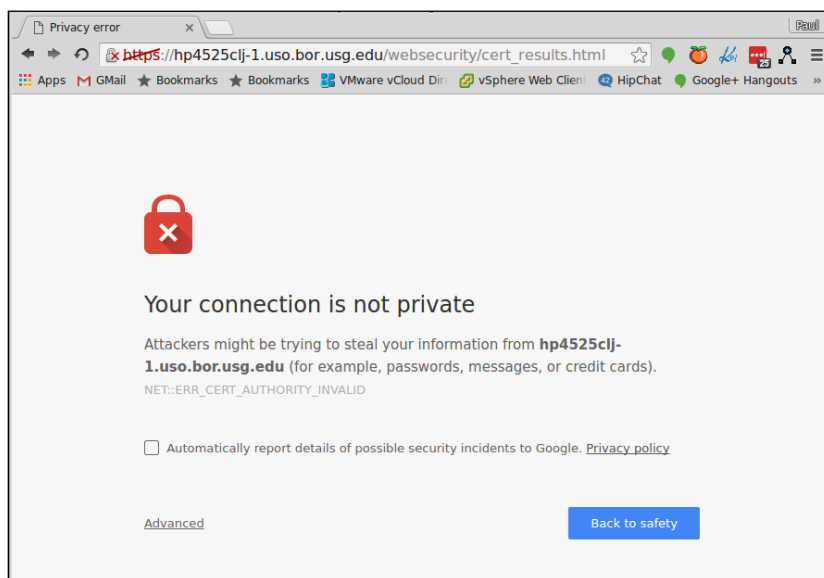


The screenshot shows the HP Jetdirect web interface for an HP Color LaserJet CP4520 Series printer. The user is logged in as 'db300user / 168.24.82.62'. The 'Authorization' tab is selected, and the 'Update Pre-Installed Certificate' section is active. The configuration details are as follows:

Common Name:	HP Jetdirect BAC20284
Organization:	Hewlett-Packard Co.
Organizational Unit:	J8011E
Organizational Unit:	B499BAC20284
Validity Period:	201 - 2021-11-21 21:46 UTC

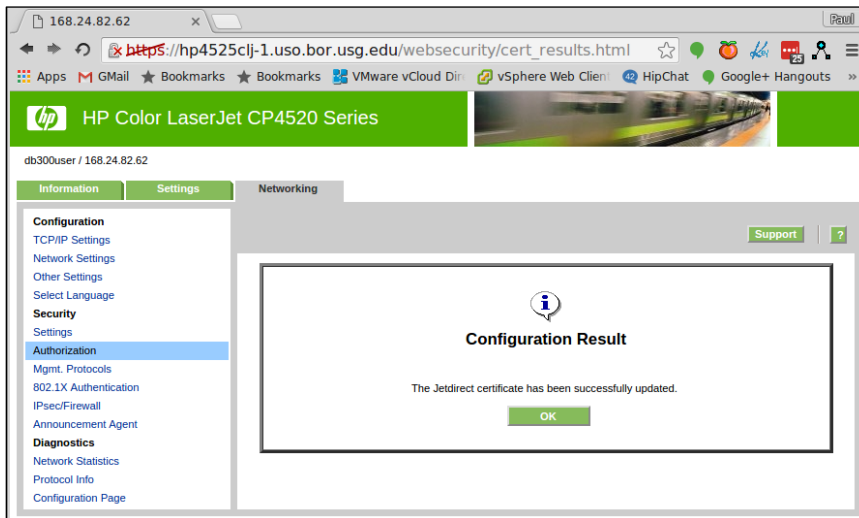
The RSA Key Length is set to 2048 bits, and the Signature Algorithm is set to SHA256. A caution message states: "Caution: Updating the pre-installed certificate will erase any third party certificate that might be installed on Jetdirect." Buttons for '< Back', 'Finish', and 'Cancel' are visible at the bottom.

You'll lose connection, then reconnect.



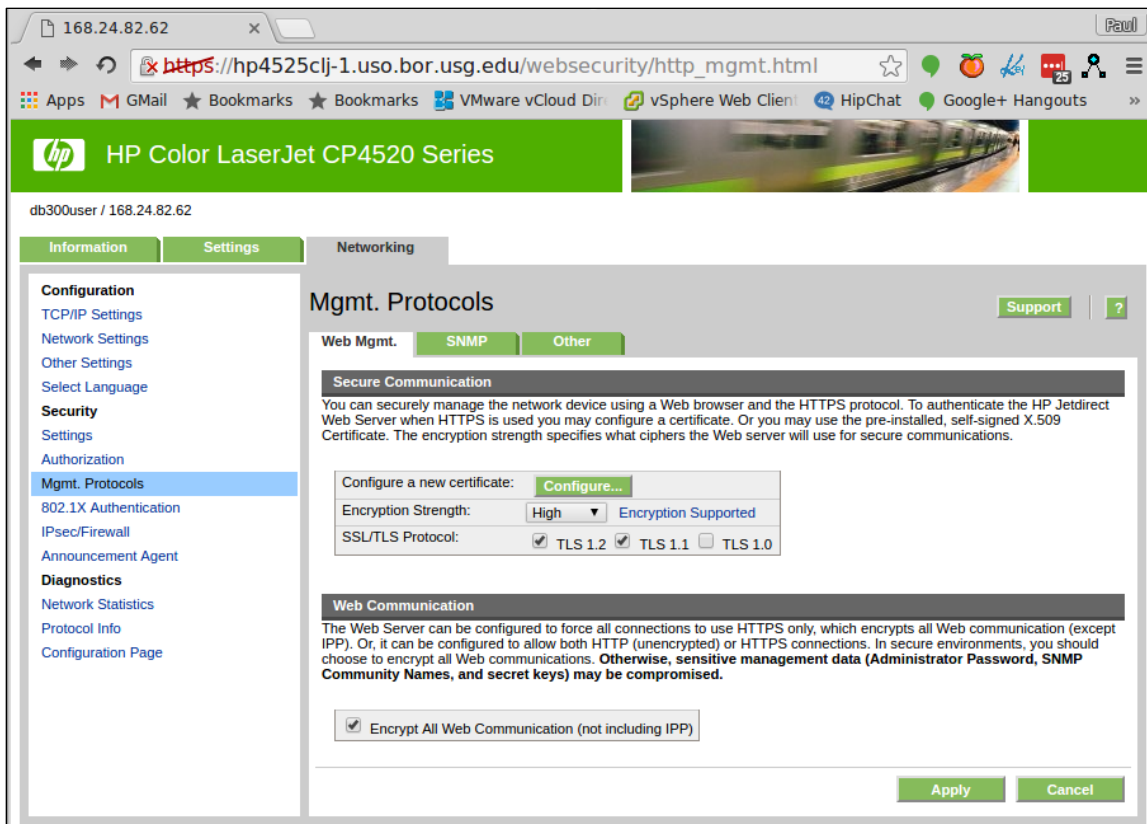
The screenshot shows a browser privacy error page with a red padlock icon and a white 'X'. The message reads: "Your connection is not private". Below this, it states: "Attackers might be trying to steal your information from hp4525cjl-1.uso.bor.usg.edu (for example, passwords, messages, or credit cards)." The error code is "NET::ERR_CERT_AUTHORITY_INVALID". There is a checkbox for "Automatically report details of possible security incidents to Google." and a "Back to safety" button.

Your browser will make you approve the new certificate, then you will see the success screen.



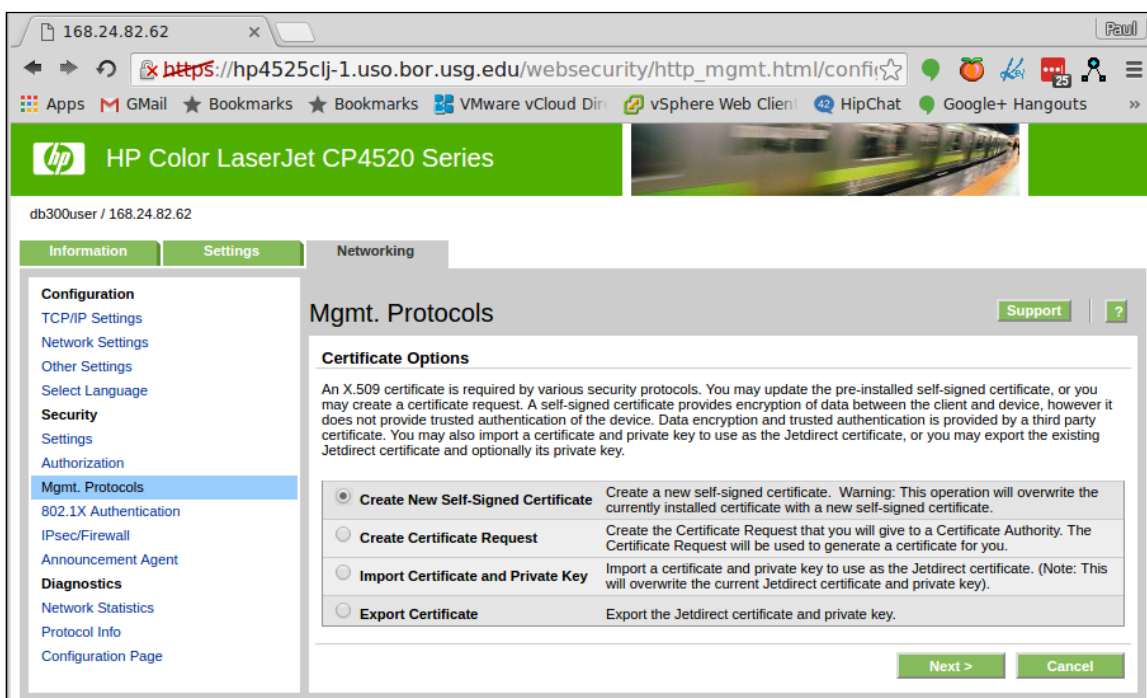
Management Protocols

- Select **Mgmt. Protocols** in the left navigation.
- In the **Configure a new certificate** box, adjust Encryption Strength to High. Uncheck TLS 1.0 and SSL 3.0 (which doesn't use TLS). Note: The lowest you should have is TLS 1.1. We have not been successful testing TLS 1.2.
- Check the “Encrypt All Web Communication” box if you like, which would make it more secure but could possibly make HTTP:// web access stop working.
- Select the **Apply** button to save the changes.

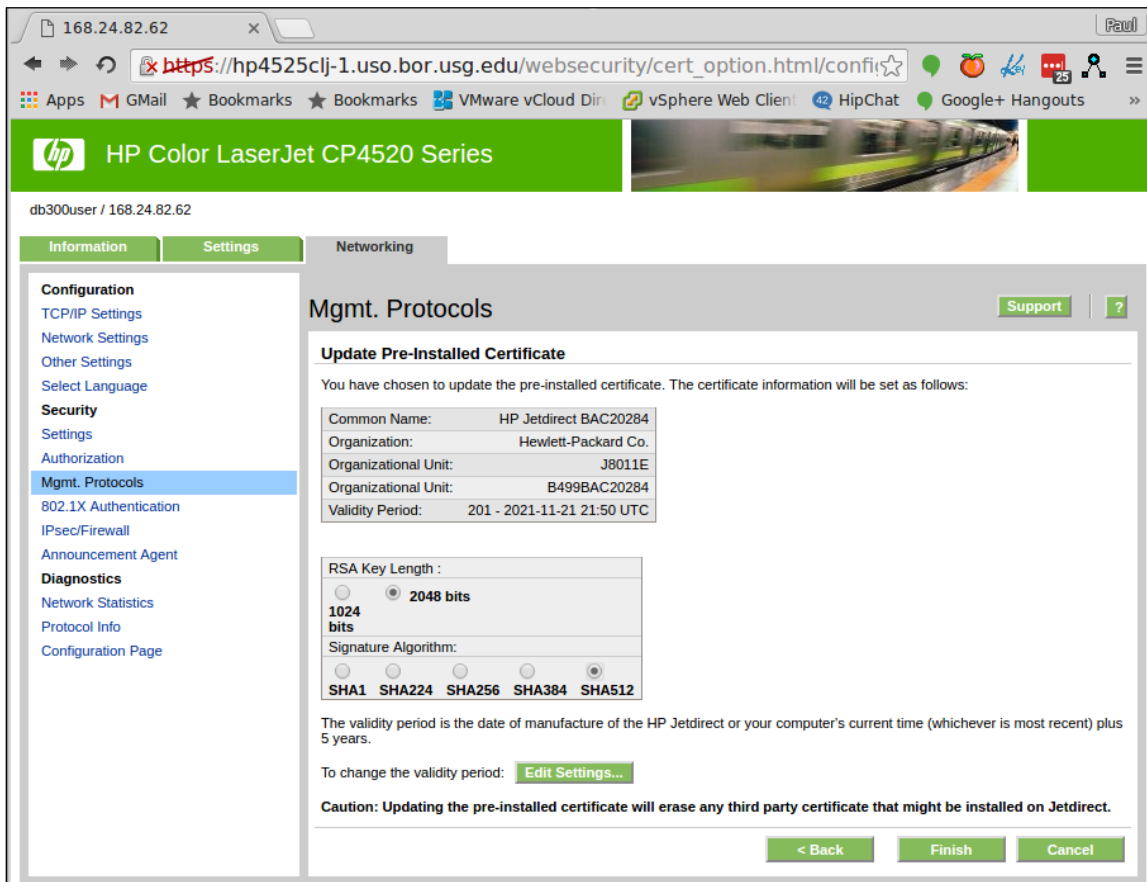


Certificate Two

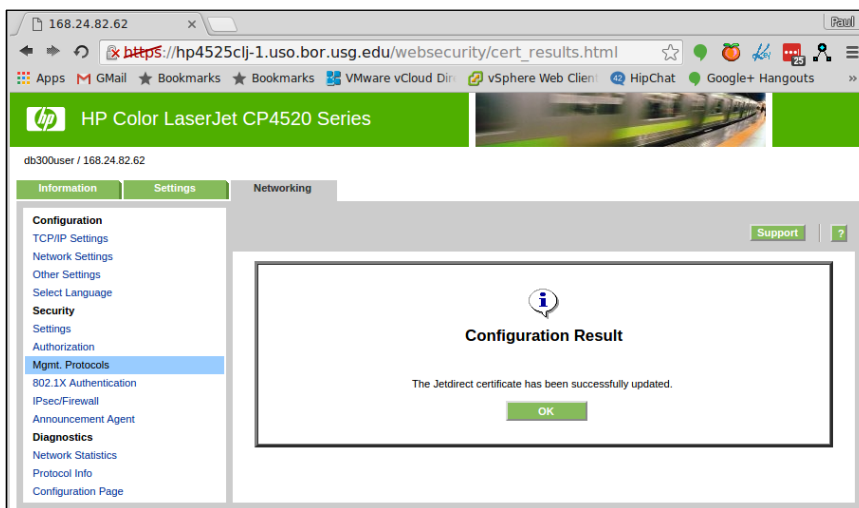
Create a new self-signed certificate for the management traffic in a different location. Note: ITS cannot verify that both certificates are needed.



Go as high as you can with RSA Key Length: 2048 bits or better, Signature Algorithm: SHA256 or better.



You'll lose connection, then reconnect. Your browser will make you reapprove the self-signed certificate, then you will see the success screen.



- Attempt a test print from the Banner server.
- Submit a ticket with the IP number and name of the printer queue. We will attempt to set it up.

Linux/UNIX Machine With nmap Installed

If you have access to a Linux/UNIX machine with nmap installed, check that you **do not have** TLS 1.0 or SSL 3 turned on with a command like below (may take 30-60 seconds).

Command One

Note: This command has outdated versions of TLS.

```
nmap --script ssl-enum-ciphers -p 443 168.18.x.y
```

```
Starting Nmap 5.51 ( http://nmap.org ) at 2016-12-02 14:27 EST
```

```
Nmap scan report for 168.18.x.y
```

```
Host is up (0.027s latency).
```

```
PORT      STATE SERVICE
```

```
443/tcp   open  https
```

```
| ssl-enum-ciphers:
```

```
| TLSv1.0
```

```
| Ciphers (3)
```

```
| TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

```
| TLS_RSA_WITH_AES_128_CBC_SHA
```

```
| TLS_RSA_WITH_AES_256_CBC_SHA
```

```
| Compressors (1)
```

```
| uncompressed
```

```
| TLSv1.1
```

```
| Ciphers (3)
```

```
| TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

```
| TLS_RSA_WITH_AES_128_CBC_SHA
```

```
| TLS_RSA_WITH_AES_256_CBC_SHA
```

```
| Compressors (1)
```

```
| uncompressed
```

```
| TLSv1.2
```

```
| Ciphers (7)
```

```
| TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

```
| TLS_RSA_WITH_AES_128_CBC_SHA
```

```
| TLS_RSA_WITH_AES_128_CBC_SHA256
```

```
| TLS_RSA_WITH_AES_128_GCM_SHA256
```

```
| TLS_RSA_WITH_AES_256_CBC_SHA
```

```
| TLS_RSA_WITH_AES_256_CBC_SHA256
| TLS_RSA_WITH_AES_256_GCM_SHA384
| Compressors (1)
|_  uncompressed
```

Nmap done: 1 IP address (1 host up) scanned in 60.60 seconds

Command Two

```
nmap --script ssl-enum-ciphers -p 443 168.24.x.y
```

Starting Nmap 5.51 (<http://nmap.org>) at 2016-12-02 14:30 EST

Nmap scan report for hpmxxxx.uso.bor.usg.edu (168.24.x.y)

Host is up (0.0010s latency).

```
PORT      STATE SERVICE
```

```
443/tcp   open  https
```

```
| ssl-enum-ciphers:
```

```
| TLSv1.1
```

```
| Ciphers (3)
```

```
| TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

```
| TLS_RSA_WITH_AES_128_CBC_SHA
```

```
| TLS_RSA_WITH_AES_256_CBC_SHA
```

```
| Compressors (1)
```

```
|  uncompressed
```

```
| TLSv1.2
```

```
| Ciphers (7)
```

```
| TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

```
| TLS_RSA_WITH_AES_128_CBC_SHA
```

```
| TLS_RSA_WITH_AES_128_CBC_SHA256
```

```
| TLS_RSA_WITH_AES_128_GCM_SHA256
```

```
| TLS_RSA_WITH_AES_256_CBC_SHA
| TLS_RSA_WITH_AES_256_CBC_SHA256
| TLS_RSA_WITH_AES_256_GCM_SHA384
| Compressors (1)
|_ uncompressed
```

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds

Note: We can scan from the Banner database server as long as port 443 is open, if you cannot do this locally.

Notes For Firmware Updates

Rough notes on how ITS has been updating firmware. The most modern versions can have a file uploaded through the web GUI, but somewhat older versions will need File Transfer Protocol (FTP).

- <http://support.hp.com/us-en/drivers>
- Enter model number (e.g., laserjet m806, color laserjet cp4025, etc.)
- Select your specific model, if known
- Select your product's operating system
- Try some version of Windows
- In the firmware section, download the biggest bundle or zipped Remote Firmware Update (rfu) file they've got!
- Unpack the zipped file and choose the rfu file you want.

FTP printername.yourschool.edu (Select, 'ENTER' twice rather than giving credentials)

bin

hash

Enter: blahblah.rfu

Select: Quit

Ping: printername.uso.bor.usg.edu|perl -n -e 'print " " x rand(5), \$_'

Watch the command stop answering, then start again after a few minutes.

Good luck, and feel free to ask questions!

- The GeorgiaBEST System Administrators