Offensive Network Security and Pentesting

Khizr Ali Pardhan

November 9th 2015

#1 webcam hacking (no sound, necessarily)

Resources used:

https://www.youtube.com/watch?v=scrHYlLIzM0

http://elitebloggerz.blogspot.ca/2014/09/hack-webcam-using-metasploit-backtrack.html

http://xeushack.com/hacking-webcams/

Outline of what I did:

- metasploit
- use "reverse_tcp" payload
- Use multi/handler
- set lhost
- set lport
- exploit
- rhost = [target's ip]
- lhost [user's ip]

I tested this out, but it did not work. The video showed this is tested for windows XP, but it did not work on either of my 2 target computers which are both windows 8.1. It most likely have been patched.

#2 mobile webcam hacking (patched for android 4.2 and above)

Resources used:

https://www.youtube.com/watch?v=lsVBQWWjiFQ

- Outline of what I did
- Metasploit
- Using msfvemon –p [reverse_tcp (payload)]
- Create the .apk
- Use exploit(handler) and set payload,lhost,lport and execute it
- Install .apk

1. Type sysinfo for information
2. Type help for commands

I tried this lab out by following a YouTube tutorial out instead of other source, because it would be less outdated. I found out it would not be possible for me to test this out because it is patched by google in android 4.2 and above. I considered emulating an android environment and continuing that way but my desktop does not have a webcam and compatibility would be a very big point of error.

#3 man in the middle attack

Resources used:

https://www.udemy.com/kali-linux-backtrack-evolved/learn/#/

Lesson #32 involved for faking a website

https://www.cbtnuggets.com/it-training/penetration-testing-backtrack-kali-linux

Lesson #12 involved

Basic outline of what I did

- Cat /…/ip_forward (must = 1 value)
- ARP spoof targets' IP (-t [ip #1] [gateway])
- ARP spoof target's IP (-t [[gateway] [ip #1])
- Use drift net or wireshark or other program + For password and other encrypted contact use SSLstrip will be needed

1. Additionally SET can be used to clone a site and to trick a user into logging into fake site then you are hosting.
2. By DNS spoof. Make a new web site which will only be found in the network. (Like login.facebook.com)
3. You might be able to use "punycode" instead of Unicode in DNS for URL. DNS only accepts ASCII (yΦutube.com)
4. A clever trick might be to use "A or X in the Cyrillic script" instead of normal Latin alphabet(which I am currently using).
5. With further research I found out Cyrillic will not work and will be a dead giveaway.

In conclusion this unfortunately this did not work, I attempted this about 6 this following different procedures by different people. If this would have worked I would be able to capture a particular target's log in info in plain text.

#4 man in the middle for unencrypted traffic

Resources used:

https://www.udemy.com/kali-linux-backtrack-evolved/#/

Involves lesson #36

I tested out a program called ettercap. An outline of what i to configure was:

- Start ettercap
- Select interface
- Scan for hosts
- Host list
- Arp poison -> sniff remote connection
- Start sniffing
- Console will display IP, USER, PASS and INFO (site URL)

In Order to test, I opened another computer on my network and went to unencrypted pages and was able to successfully capture the information (IP, USER, PASS and INFO)

In conclusion this was successful but can be used for Facebook or other popular sites today (In the past sites like Facebook have used HTTP instead of HTTPS)

#5 DDOS using LOIC

Resources used:

https://www.youtube.com/watch?v=_nPcysStRio

I researched A basic DDOS attack program called “Low Orbit Ion Cannon” It is very simple to use.

A basic outline is:

- Input URL or IP
- Select port (80 or other port number)
- Select TCP or UDP
- Select threads (this is CPU intensive!, 1000-3000 recommended)

Be sure to use VPN or other method on keeping your own identity private.

A DDOS attack using NTP over UDP has the Bandwidth Amplification Factor of 556.9.

In conclusion launching a DDOS via a program has been made very easy.

#6 SQL injection

Resources used:

https://www.udemy.com/advanced-ethical-hacking-vtc/

Section #3 and 12

https://www.youtube.com/watch?v=rdyQoUNeXSg

https://www.youtube.com/watch?v=7Wkk_mgAzXU

http://waziristanihaxor.blogspot.ca/2015/08/updated-5000-Fresh-SQL-Injections.html

I learned how to do an SQL injection and how to find a target with the needed vulnerability. An example of vulnerability found while doing a google search:

- http://www.cobranet.org/about.php?id=1%27
  After I searched for a list of dorks and I found this reference
- https://docs.google.com/document/d/1VjIvk9VvzEWq3Gfl8vvmE6fzSV9d-zGIRllDdX4WMs/edit

To top it off I discovered the following site which sells products had the vulnerability. The database may contain user credentials, and payment information.

example of marketplace with sql error:

- http://www.spot911.com/en/index.php?cid=122 (open URL and add a single quote mark-> ' <-) (I found in late October and possible patched)
- http://www.hueso-records.com/album.php?id=366 (open URL and add a single quote mark-> ' <-)

To sum it up, I found even updated and "maintained" sites will have SQL errors, as well as long forgotten ones.

#7 password cracker

Resources used:

https://www.youtube.com/watch?v=HSksKRyyCMY

https://www.udemy.com/kali-linux-backtrack-evolved/learn/#/

Lesson #38-40

I learned a program called hydra can be used for gaining access to FTP servers and a variety of other things such as internet password. Also there are programs like john the ripper that do the same but for local file such as .pdf or .doc.

On the windows side there is "passware kit forensic" which can be used on many versions of windows and gets the jobs done for obtaining password for archives and office files. It also has GPU acceleration to speed out the process. I used this to get password for a .pdf before and process took less than 40 seconds.

#8 browser password decryptor

Resources used:

http://securityxploded.com/browser-password-decryptor.php

https://www.raymond.cc/blog/hack-u3-usb-smart-drive-to-become-ultimate-hack-tool

Browser password decryptor works too well. I can confirm it works on IE and Chrome. It can show Email/Username & Passwords for Facebook, Google services and even PayPal. on older version of windows you were able to automate the whole process. meaning all you needed to do was plug in the U3 USB drive in and the software will get the credentials and store them on the usb and then made a sound you can can plug the drive and walk away. this is called a USB switchblade and i tested it and found out it does not work on newer versions of windows

#9 changing IP address, mac address and bypassing filters

Resources used:

https://www.cbtnuggets.com/it-training/penetration-testing-backtrack-kali-linux

http://linuxconfig.org/change-mac-address-with-macchanger-linux-command

8 & 6

- Changing my IP address in windows and kali Linux were both successful.
- Changing my mac address in kali Linux was also fully successful.
- Since MAC address is changed, I would be able to enter a network which has mac filter MAC spoofing can be very useful for bypassing parental controls or staying anonymous.

#10 (mis-association attack)

Resources used:

http://www.aircrack-ng.org/doku.php?id=airbase-ng

Video #38 (wireshark) - of unknown resource

Using airbase-ng's Ability to act as a full Access Point, and few other programs I was able to create and name an SSID "ShawOpen". I named it that so a computer would automatically connect to it. All traffic in and out going to route through my networks card. After I can simply open up wireshark and start reading the packets

I follow thought was resources and got stalled when it was time to testing the fake access point. I used one of my computer to connect to network (which it did) but was unable to access the internet. I later opened up wireshark and was able to get that working fine.

If I was able to create the access point successfully Ii could have captured and recorded the traffic/data with wireshark, ettercap or possible driftnet

#11 accessing unprotect camera

Resources used:

https://www.youtube.com/watch?v=9QStMgAxWqk

After watching a YouTube tutorial I googled and opened up the first few links and any, which seemed relevant or interesting I found these

- inurl:/view/index.shtml
- intitle:"Live View / - AXIS"

After opening url, you can fully control the cameras.

- -pan/move left and right
- -zoom
- -focus

In conclusion there are plenty of unsecured cameras connect to the internet, some outdoors on private property, inside homes and in lobbies. If one was to trace the IP, this could be for criminal intent.