Cyber security assignment

Submitted by -Ritik dewan

Email id-
hritik22dewan@gmail.com

Day6 Assignments

Question 1:

- Create payload for windows .
- Transfer the payload to the victim's machine.
- Exploit the victim's machine..

Answer

First we have install Git on our system

Steps to install git

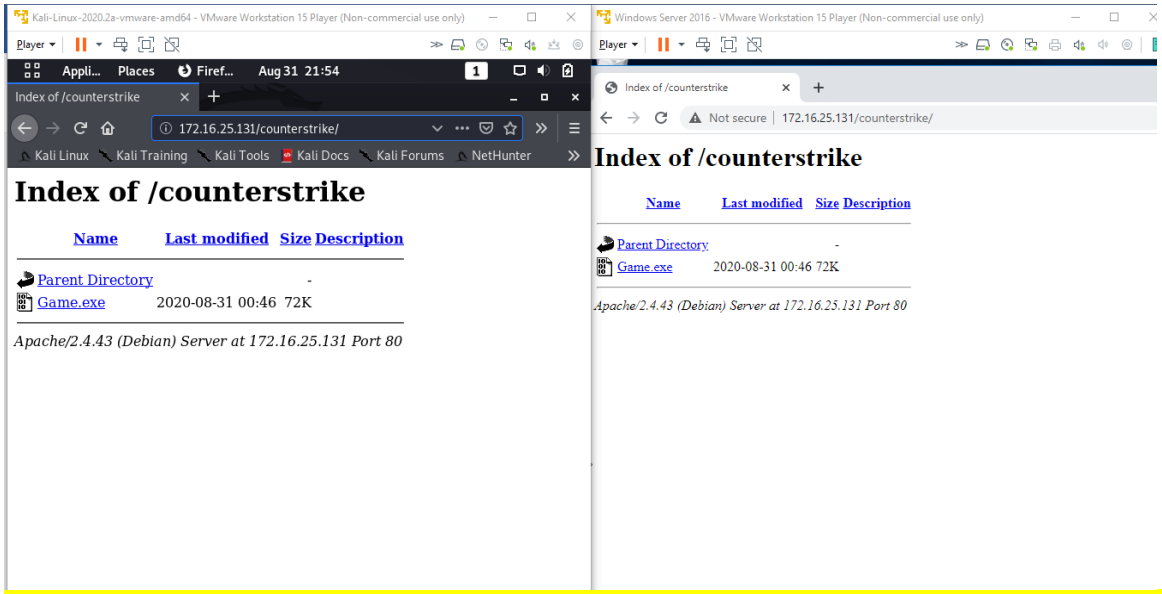
Step1-visit https://git-scm.com/

Step2-Download git into your system

Step3-after downloaded git now install git & set the installing path where you have to place it in your system like in c drive &etc

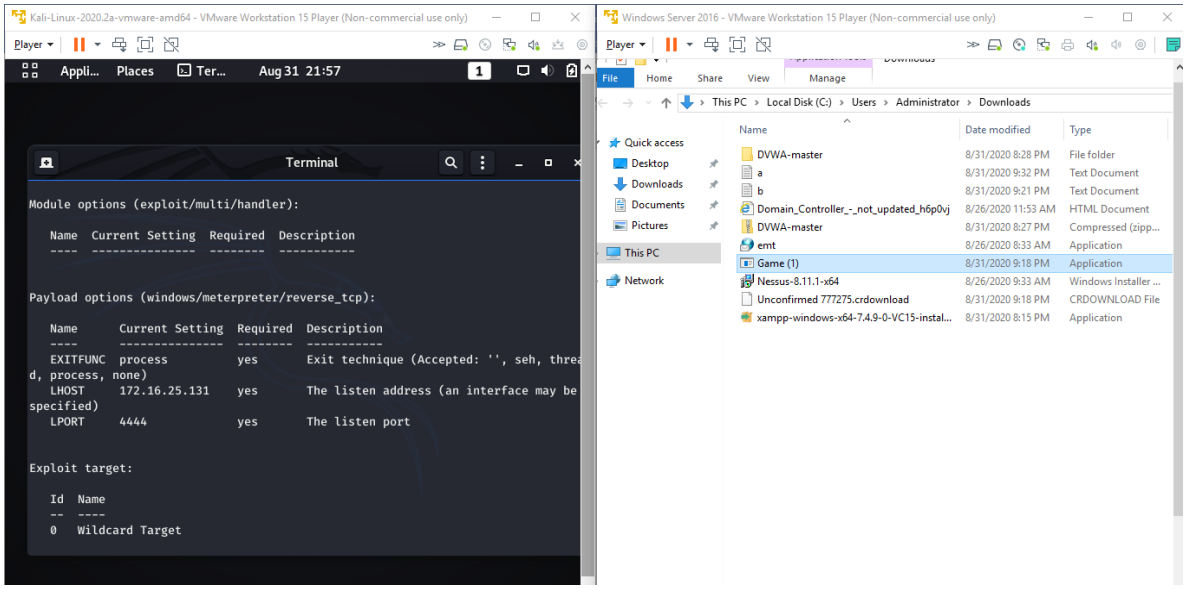
Step4-Now open git & create payload using commands like we

create a game.exe in Kali and tried opening In Victim Machine



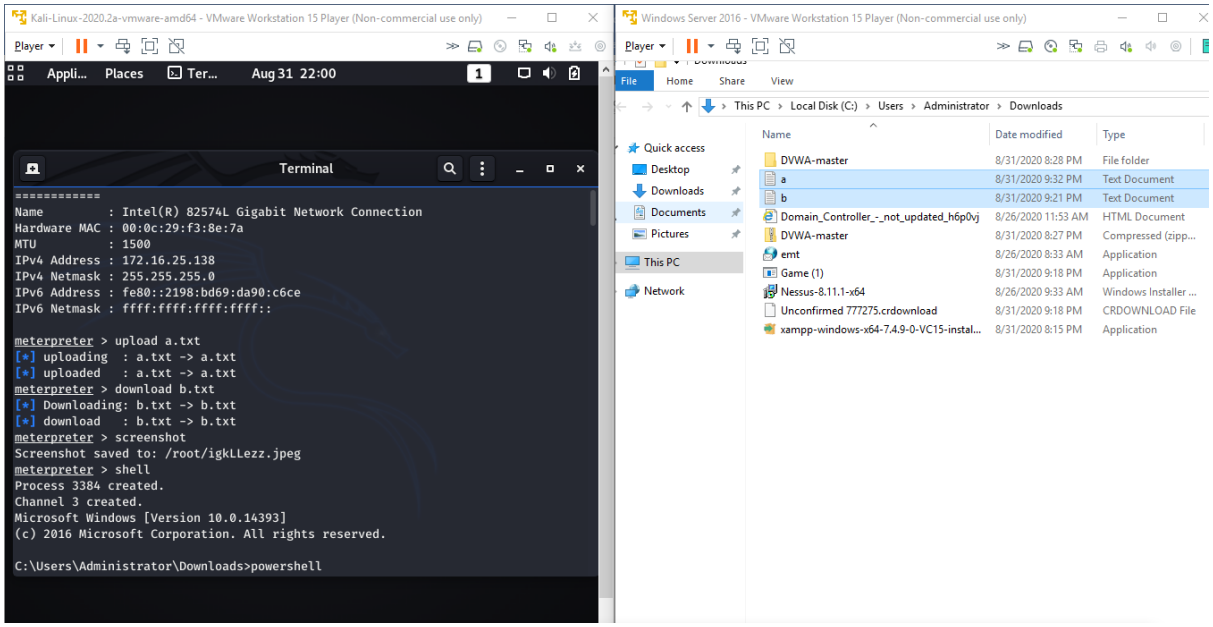
Step5- As you can see in above screenshot I create counterstrike game & its ready to transfer in victims machine

You can send it this link by whatsapp,email,& anyother social media platflorm



Step6-As you can see i download counter strike game in victims machine & now I install it

Step7-now I transfer some file from my machine to victims machine



As you can see in above screenshot I create a & b file I transfer it into victims machine

Now the victims windows is hacked .

Question 2:

- Create an FTP server
- Access FTP server from windows command prompt

- Do an mitm and username and password of FTP transaction using wireshark and dsniff

Answer

File Transfer Protocol

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture using separate control and data connections between the client and the server.

Man-in-the-middle attack

In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other

over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within the reception range of an unencrypted Wi-Fi access point could insert themselves as a man-in-the-middle.

As it aims to circumvent mutual authentication, a MITM attack can succeed only when the

attacker impersonates each endpoint sufficiently well to satisfy their expectations. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, TLS can authenticate one or both parties using a mutually trusted certificate authority

dSniff

---

dsniff is a set of password sniffing and network traffic analysis tools written by security researcher and startup founder Dug Song to parse

different application protocols and extract relevant information. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.). arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g., due to layer-2 switching). sshmitm and webmitm implement active man-in-the-middle attacks against redirected SSH and HTTPS

sessions by exploiting weak bindings in ad-hoc PKI.

Wireshark

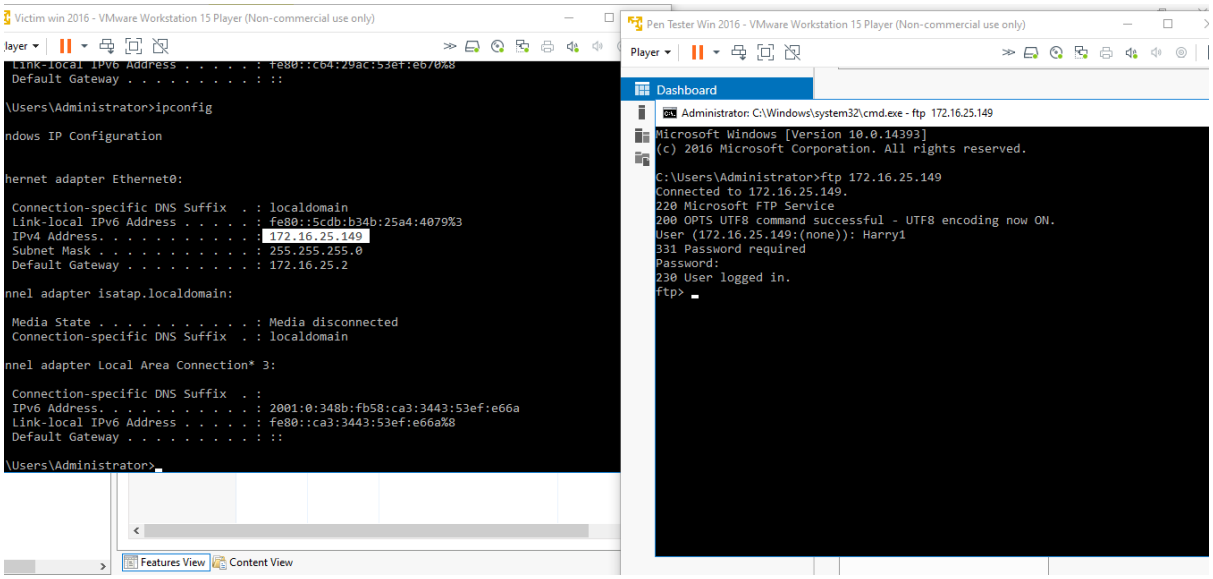
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues.[4]

Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement

its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

Steps: -

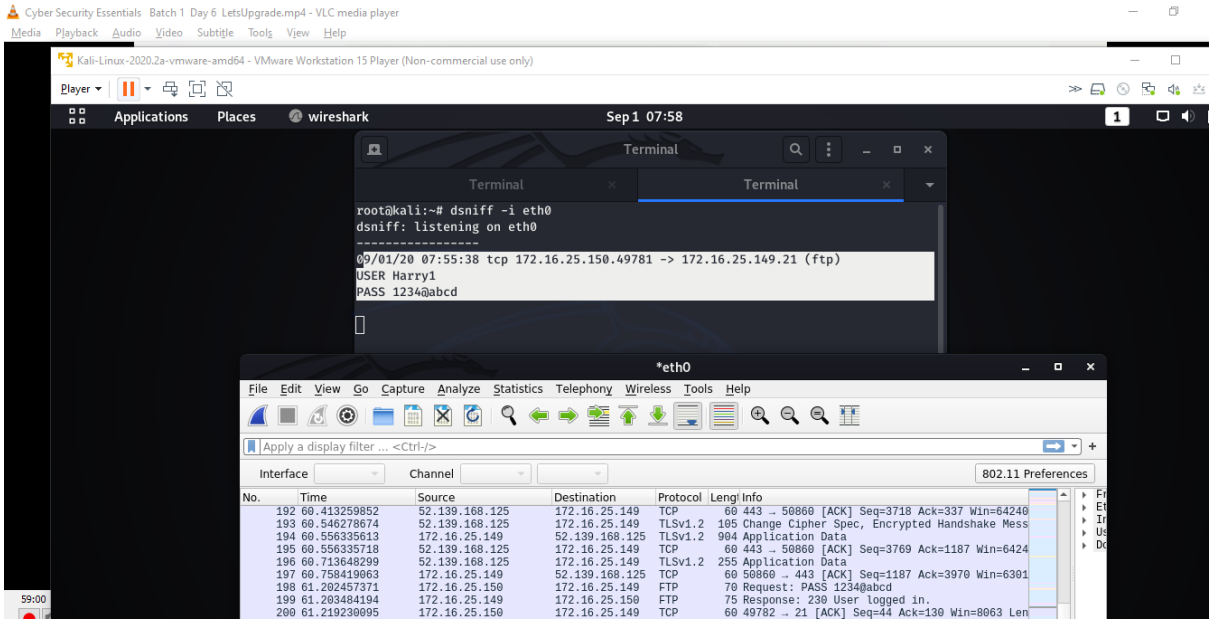
Created FTP in Victim and Able to log in in FTP from Pen Tester System



Using dsniff Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd



Using Wireshark Username & Password of Ftp transaction is displayed below

Username of FTP: - Harry1

Password: - 1234@abcd