PRACTICAL NO 1(a)

Encrypting and decrypting data using a Hacker tool

1. How long does it take to discover the password?

→ It takes less than a second.

2. How long does it take to discover the password?

→ It should take about a second

3. How long does it take to discover the password?

→ Answer will vary depending on platform and actual password used but it should about a second or two.

4. How long do you think it would take fcrackzip to discover a 6-character password?

→ Answer will vary

5. How does long it take fcrackzip to discover the password?

→ Answer will vary depending on platform & actual password used but it will take much longer hours.

6. How long would you recommend a password need to be for it to be secure?

→ Will vary.

PRACTICAL NO. 1(B)

Encrypting and decrypting data using open SSL

1. Did the contents of the message.enc file display correctly? What does it look like?

→ No The file seems broken as just symbols are displayed. The symbols are shown because openssl has generated a binary file

2 Is message.enc displayed correctly now? Explain.

→ Yes While message.enc is encrypted, it is now correctly displayed because it has been converted from binary to text and encoded with Base 64.

3. Can you think of a benefit of having message.enc Base-64 encoded?

→ The encrypted message can now be copied and pasted in an email message for example

4. Was the letter decrypted correctly?

→ Yes, the letter was decrypted correctly.

5. The command used to decrypt also contains a option. Can you explain?

→ Because, message.enc was base 64 encoded after the encryption process took place message.enc must be base 64 decoded from before Openssl can decrypt it.

PRACTICAL NO. 1(c)

Hashing a text file with Openssl and veryfying hashes.

1. Is the new hash different than hash calculated in item (d)? How different?

→ Yes. The new hash is completely different that the previous hash

2 Do the hashes generated with sha256 sum and sha512 sum math the hashes generated in items (f) and (g), respectively? Explain?

→ Yes While different tools are used, they use the same hashing algorithm and input data

3. Was the sample.img downloaded without errors? Explain.

→ Yes. Because both hashes match, the hash calculated before download and the one calculated after it is correct to state that no errors were introduced during download.

PRACTICAL NO. 2(A)

Examining talent and SSH in wireshark

1. Why is SSH preffered over Telnet for remote connections?

→ Answers may vary.

Similar to telnet, SSH is used to access and execute commands on a remote system. However, SSH protocol allows users to communicate with remote system securely by encrypting the communications. This prevents any sensitive information such as usernames and passwords from being captured during the transmission.

PRACTICAL NO. 2(B)

Investing an attack on a windows Host

1. What was the source IP address and port number and destination IP address and port number?

→ Source : 10.0.90.215: 52609
Destination : 10.0.90.9.53

2. What type of protocol and request or response was involved?

→ UDP. Dynamic DNS, Update and response

3. What is the IDS alert and message?

→ Alert UDP $ EXTERNAL_NET any → $ HOME_NET 53, msg: "FT POLICY DNS update from_EXTERNAL net.

4. Do you think this alert was the result of an IDS misconfiguration or a legitmate suspicious communication?

→ This alert may be the result of a misconfiguration in the IDS because the DNS request was a Dynamic DNS update from an internal host to a DNS server on the internal network and not from an external network to the internal network.

5. What is the source and destination IP address?

→ Source: 10.0.90.215:49204

Destination: 209.141.34.8:80

PRACTICAL NO. 2(C)

Investigating a malware exploit

1. What is the time of the first detected NIDS alert in kibana?

→ Jan 27, 2017 - 22:54:43

2. What is the source IP address in the alert?

→ 172.16.4.198

3) What is the destination IP address in alert?

→ 194.87.234.129

4. What is the destination port in the alert? What server is this?

→ 80, HTTP

5. What is the classification of the alert?

→ Trojan activity

6. What is the destination geo country name?

→ Russia

7. What is the malware family for this event?

→ Exploit_kit_RIG

8. What is the severity of the exploit?

→ The signature severity is major

PRACTICAL NO. 3(A)

Demonstrate the use of snort and firewall Rules.

1. The RI shell opens in a terminal window with black text and white background What user is logged into that shell? What is the indicator of this?

→ The root user. This is indicated by the # sign after the prompt

2. What port is used when communicating with the malware web server? What is indicator?

→ Port 6666. The port was specified in the URL after the : separator.

3. Was the file completely downloaded?

→ Yes.

4. Did the IDS generate any alerts related to the file download?

→ Yes.

5. Based on the alert shown above when did the download take place?

→ April 28th around 5pm for example, but the students answer will be different

6. Based on the alert shown above, what was the message recorded by the IDS signature

→ "Malicious server Hit!"

PRACTICAL NO. 3(B)

Demonstrate extract and execute from a PCAP.

1. What are all those symbols shown in the follow TCP stream window? Are they connection noise?

→ The symbols are the contents of the downloaded file Because it is binary file wireshark does not know how to represent it. The displayed symbols are wireshark's best guess at making sense of the binary data while decoding it as text.

2. Using the word fragments displayed by wireshark's follow TCP stream window, can you tell what executable this really is?

→ Scrolling all the way down on that window reveals that this is the microsoft windows cmd.exe.file

3. Why is W32.Nimda.Am.exe the only file in the company?

→ Because the capture was started right before the download and stopped right after No, other traffic was caught while the capture was active.

4. Was the file saved?

→ yes.

PRACTICAL NO.3(C)

Demonstrate a practical for exploring DNS traffic

1. What are the source and destination IP address which network interfaces are these IP addresses associated withe

→ In this example, the source IP address is associated with the NIC on the PC and the destination IP address is associated with the default gateway.

2 What are the source and destination ports? What is the default DNS port number?

→ Source port number - 577729

Destination port number is 53 which is the default DNS port number

3. Can the DNS server do recursive queries?

→ Yes, the DNS can handle recursive queries.

4 How do the results compare to nslookup results?

→ The results in the wireshark should be same as the results from nslookup in the command prompt or terminal

PRACTICAL NO. 4(A)

Using wireshark to examine HTTP and HTTPS traffic

1. List the interfaces and their IP addresses displayed in the ip address output

→ enp0s3 with 10.0.2.15 and lo with 127.0.0.1 (answers for enp0s3 will vary)

2. What two pieces of information are displayed?

→ The uid of admin and passw of Admin

3. What do you notice about the website URL?

→ Answers will vary. The website is using HTTPS, and there is a block.

4. What are the advantages of using HTTPs instead of HTTP?

→ When using HTTPS, the data payload of a message is encrypted and can only be viewed by the devices that are part of the encrypted conversation.

5. Are all websites that use HTTPS considered trustworthy?

→ No, because malicious websites can utilize HTTPS to appear legitimate while still capturing user data and logins.

PRACTICAL NO. 4(B)

Exploring processes, Threads, Handles and windows Registry

1. What happend to the web browser window when the process is killed?

→ The web browser window closes.

2. What happened during the ping process?

→ A child process PING.EXE listed under the cmd.exe during the ping process.

3. Right click the cmd.exe process and select Kill process. What happened to the child process conhost.exe?

→ The child process depends on the parent process. So when the parent process stops, the child process also stops.

4. Examine the details of the thread. What type of information is available in the properties window?

→ Information available includes environment variable, security information, performance information and printable strings.

5. Examine the handles. What are the handles pointing to?

→ The handles are pointing to files, registry keys and threads.

6. When you open the process Explorer, what did you see?

→ The process explorer License agreement dialog box.

PRACTICAL NO. 05

Perform a practical to attack on a mySQL Database by using PCAP file

1. What is the version?

→ MySQL 5.7.12-0

2. What would the modified command of (1 OR 1=1 UNION SELECT NULL column_name FROM INFORMATION_SCHEMA.columns WHERE table_name = #users) do for the attacker?

→ The database would respond with a much shorter output filtered by the union of the word "users".

3. Which user has the password hash ~~of~~? of 8d353d75ae2c3966d7e0d4fcc69216b2

→ 1337

4. What is the plain-text passwords

→ Charley

5. What is the risk of having platform use the SQL language?

→ Web sites are commonly database driven and use the SQL language The severity of a SQL injection attack is up to the attack

6. Browse the internet and perform a several on "prevent SQL·injection attack." What are 2 methods or steps that can be taken to prevent SQL injection attacks.

→

Answers will vary, but should include Filter user input Deploy a web application firewall. Disable unnessesary database features / capabilities monitors SQL statements. Use parameters with store procedure user parameter with dynamic SQL.