**Question N1 Which open source program is recommended to create a snapshot of theWindows registry? Describe the flow of the process.**

Regshot.

Create a 1st shot.

Do some changes.

Create a 2nd shot.

Click on compare button to compare both the shots.

**Question N2 Explain which type of computer forensics method is appropriate to use at thescene of a cyber incident? Name some other types of expertise.**

Live forensics – This process involve gathering volatile data of the operating system such as processes, open files, network etc.

Network forensics, Mobile forensics, digital forensics.

**Question N3 Explain at which stage of incident response the system is isolated to preventthe spread of malicious code in the computer network?**

Containment stage

In containment stage the operating system is isolated to prevent the spread of any kind of malicious program.

**Question N4 Explain what the volatility tool is used for and what capabilities it has.**

Volatility tool is used for analysing data from the memory to gather more details about malicious programs or other artifacts.

Memory Analysis, malware detection, supports multiple OS’s, anti-forensics technique.

**Question N5 Describe what issues should be addressed in a malicious code analysis executive summary report?**

1. Executive Summary

2. Identification

3. Capabilities

4. Dependencies

5. Static Analysis

6. Dynamic Analysis

7. Supporting Data

8. Conclusion

**Question N6 Name and describe a tool through which it is possible to determine the IPaddress of a malicious domain and give an example of a complete command.**

nslookup a command line tool used for retrieving info about domain names, ip-addresses.

Supported on windows. Mac and linux

nslookup google.com

**Question N7 Explain the so-called Ransomware action steps from a technical point of view. Name some famous Ransomware and provide information about them.**

1. Detection and Isolation: Identify ransomware and isolate affected systems.
2. Incident Response Team Activation: Activate a team to manage the response effort.
3. Containment: Limit ransomware impact and prevent further spread.
4. Analysis and Threat Assessment: Understand ransomware behaviour and assess the damage.
5. Recovery and Restoration: Restore systems from clean backups or explore recovery options.
6. Malware Removal and System Hardening: Remove ransomware and strengthen system security.
7. Investigation and Forensic Analysis: Determine the attack's cause and gather evidence.
8. Communication and Reporting: Inform stakeholders and prepare incident reports.
9. Enhancing Security Controls: Learn from the incident and improve security measures.

WannaCry: It exploited a vulnerability in the Windows operating system and encrypted files, demanding a ransom in Bitcoin.

NotPetya: It disguised itself as the Petya ransomware but was later revealed to be a destructive wiper malware disguised as ransomware.

**Question N8 Describe the hashing process and explain its purpose.**

Hashing process involves applying hash values to a file or data. These hash values couldbe in md5, md2, sh265/512 etc.

Its purpose is to uniquely identify a file. Such as checking if the file we downloaded is not modified during the download process and is in fact the file that we need.

**Question N9 Explain what is called a virtual environment and list the known virtualizationtools.**

The process of using multiple operating systems such as Linux, mac, windows on a single operating system is called virtualization. These operating systems are installed as if it were running on its own separate system. Some of the most used tools are VMWare, VirtualBox, Hyper-V, KVM.

**Question N10 What are DLL type files used for and what is their role in terms of maliciouscode?**

DLL are reusable code and data that multiple programs can access and use simultaneously.

In terms of malicious code:

Code Injection, DLL Hijacking, DLL Spoofing, DLL Preloading.

Question N11 Describe the working principle of the given encrypted programming code.~amp;lt;script type=~amp;quot;text/javascript~amp;quot;~amp;gt; function check() { var \_0x4347x2 = ~amp;#39;PaSsW0rD!~amp;#39;; var \_0x4347x3 = document[~amp;#39;getElementById~amp;#39;](~amp;#39;JSka~amp;#39;)[~amp;#39;value~amp;#39;]; \_0x4347x2 === \_0x4347x3 ? alert(~amp;#39;Passed~amp;#39;) : alert(~amp;#39;Failed~amp;#39;) }~amp;lt;/script~amp;gt;

**Question N12 Describe the principle of operation of the given encrypted code and present itsdecrypted version. RHJhd2luZyBvbiBteSBmaW5lIGNvbW1hbmQgb2YgbGFuZ3VhZ2UsIEkgc2FpZCBub3RoaW5nLg==**

The text is encrypted in base64 format.

Drawing on my fine command of language, I said nothing.

**Question N13 Describe the principle of operation of the given encrypted code and present its decrypted version. Jevgvat nobhg zhfvp vf yvxr qnapvat nobhg nepuvgrpgher**

The text uses and algorithm called shift/Caesar cipher to encrypt the text. Shift cipher basically takes in a number and shifts each letter based on the number.

Writing about music is like dancing about architecture.

**Question N14 Describe the principle of operation of the given encrypted code and present itsdecrypted version. 01110000 01101001 01101110 01100111 00100000 00110001 00111001 0011001000101110 00110001 00110110 00111000 00101110 00110001 00101110 0011000100110010 00110011**

The text is in binary format. Each group of numbers are ASCII characters. It can be decrypted using some online binary to text decoder.

ping 19.168.1.23

Question N15 Describe the principle of operation of the given encrypted programming code andget the password encoded in it.var\_0xea0e=[~amp;quot;\x76\x61\x6C\x75\x65~amp;quot;,~amp;quot;\x69\x6E\x70\x75\x74\x53\x74\x72~amp;quot;,~amp;quot;\x67\x65\x74\x45\x6C\x65\x6D\x65\x6E\x74\x42\x79\x49\x64~amp;quot;,~amp;quot;\x64\x47\x56\x73\x62\x47\x31\x6C\x62\x57\x39\x79\x5A\x51\x3D\x3D~amp;quot;,~amp;quot;\x50\x61\x73\x73\x65\x64~amp;quot;,~amp;quot;\x46\x61\x69\x6C\x65\x64~amp;quot;];function check(){var\_0x8ecbx2=document[\_0xea0e[2]](\_0xea0e[1])[\_0xea0e[0]];var

The password is in hex decimal format which when decrypted is in base64 format. The check () function uses the inbuilt method called atob() to convert the base64 string into normal text and then compares it with the input of the user.

Password: tellmemore

Q1 list the malicious code types and their function ?

Viruses: Self-replicating programs that infect and modify files.

Worms: Self-propagating programs that spread through networks.

Trojans: Malicious software disguised as legitimate programs.

Ransomware: Encrypts files and demands a ransom for decryption.

Spyware: Collects and transmits user information without consent.

Adware: Displays unwanted advertisements.

Rootkits: Conceals malicious activity to maintain control.

Botnets: Networks of compromised devices used for attacks.

Keyloggers: Records keystrokes to capture sensitive information.

Backdoors: Provides unauthorized access to systems.

Q2 what is dynamic analysis of malicious code?

Dynamic analysis is when we are running and executing the malicious code and analysing the behaviour of it and what it does in a target system.

Q3 list and explain what steps should be taken to detect malicious code on infected system ?

Run antivirus and anti-malware scans.

Monitor for abnormal behavior.

Analyze network traffic.

Inspect files and memory.

Match against known signatures and indicators of compromise.

Use heuristic and behavioral analysis.

Execute in sandboxes or emulation.

Analyze system logs.

Stay updated with threat intelligence.

Implement continuous monitoring.

Q4 list the Dll files and their function which are often used by malicious code ?

It’s a file within a programme that can’t be run independently in other words , DLL files are used in software applications to store reusable code.

DLL files can also be leveraged by malicious actors to carry out their activities: such as DLL Side-Loading – Dll\_Hijacking and Dll injection.

Q5 what is the use of regshot in malicious code analysis ?

Regshot is being used to compare the system after some changes and modification by the time when there was no change. The functionality is like we are making first shot before changes and then second shot after changes then at the end we are pressing button compare in order to compare between these two shots.

Q6 why number of cybercrimes is growing?

The number of cybercrimes is growing due to increasing digital connectivity, profitability for criminals, availability of tools, lack of cybersecurity awareness, evolving attack techniques, international reach, and underreporting/detection.

Q7 what is static analysis of malicious code ?

Static analysis is when we are trying to find and analyze malicious software by looking at the source code without running and executing it.

Q8 how can malicious code be hashed and generated MD5 hash ?

To generate an MD5 hash of malicious code, use an MD5 hashing tool or library to process the code and obtain a unique alphanumeric hash value. However, MD5 is considered weak and not recommended for secure purposes.