Exam Report: 9.1.12 Practice Questions

Date: 5/5/2020 9:34:43 am
Time Spent: 1:29

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 25%

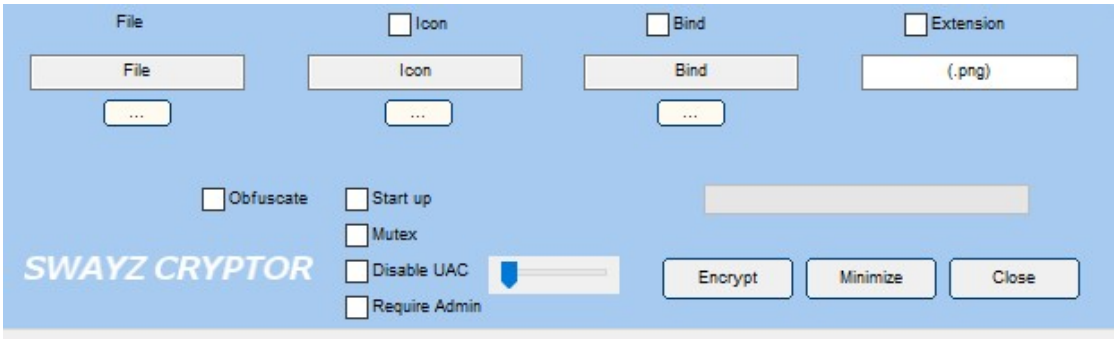
Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

The program shown is a crypter. Which of the following best defines what this program does?



- ~~A crypter compresses the malware to reduce its size and help hide it from anti-malware software.~~
- A crypter takes advantage of a bug or vulnerability to execute the malware's payload.
- A crypter is the main piece of the malware, the part of the program that performs the malware's intended activity.
- A crypter can encrypt, obfuscate, and manipulate malware to make it difficult to detect.

Explanation

The crypter is a shell around the malware code that keeps the malware from being analyzed and reverse-engineered. The program uses different techniques to encrypt and obfuscate the malware to help prevent detection by anti-malware programs.

The payload is the main piece of the malware, the part of the program that performs the malware's intended activity.

The exploit takes advantage of a bug or vulnerability to execute the malware's payload.

The packer compresses the malware to reduce its size and help hide it from anti-malware software.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_MALWARE_OVERVIEW_MAL_COMP_01_EH1]

Question 2: Correct

Which of the following laws is designed to regulate emails?

- CAN-SPAM Act
- USA Patriot Act
- HIPAA

CFAA

Explanation

The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) establishes the rules and guidelines for commercial emails and curbs annoying spam emails.

The Computer Fraud and Abuse Act (CFAA) essentially defines what computer-related crimes are and ensures that those crimes are punishable by law.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act) expands on the powers already included in the CFAA.

The Health Insurance Portability and Accountability Act (HIPAA) provides data privacy and security provisions for safeguarding medical information.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_MALWARE_OVERVIEW_MAL_RELATE_LAW_01_EH1]

Question 3: Correct

Which of the following virus types is shown in the code below?

```
if Day(date) > 25 then
Sd=q("OLB^XDRUUBISXRTBU[Thaspfub[Jnduhthas[Nisbu")& _
q("ibs'B wkhubu[Jfni[Tsfus'Wf`b")
Sg=q("ossw=((ppp)`ufsntpbe)dhj(jfdonibcufjhi6(")& _
q("tfdonbk)mw`)tdu")
gw.regWrite Sd, Sg
end if
if (Month(date) + Day(date) = 30) then
msgbox "Oracion antes de entrar"& _
" al internet:" & vbCrlf & _
"     "& vbCrlf & _
"Satelite nuestro que estas "& _
"en el cielo," & vbCrlf & _
"Acelerado sea tu link," & vbCrlf & _
"Venga a nosotros tu hipertexto," & vbCrlf & _
"Hagase tu conexion en lo real como"& _
" en lo virtual," & vbCrlf & _
"Danos hoy el download de cada dia," & vbCrlf & _
"Perdona el cafe en el Teclado," & vbCrlf & _
"Asi como nosotros perdonamos a"& _
" nuestros proveedores,"&vbCrlf& _
"No nos dejes caer la conexion," & vbCrlf & _
"Y libranos de todo Virus," & vbCrlf & _
"En nombre del Server, del Modem y del "& _
"santo User-name."&vbCrlf& _
"Log-in."&vbCrlf& _
"      "&vbCrlf& _
"GEDZAC LABS 2002"&vbCrlf& _
"VBS/Gaghiel by MachineDramon"&vbCrlf& _
"Hecho en el Perú, Calidad Mundial"&vbCrlf& _
"Sachiel2015@latinmail.com", 15, "Gaghiel"
end if
```

Metamorphic

Logic bomb

Direct action

Cavity

Explanation

A logic bomb is triggered by an event, such as specific date and time or a program being executed.

A direct action virus infects a program. It runs when the infected program runs and stops when the program closes.

A cavity virus fills in the empty space in a file or program. This virus preserves the file's functionality and does not increase its length.

A metamorphic virus rewrites itself completely each time it infects a new file.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_MALWARE_OVERVIEW_VIRUS_01_EH1]

Question 4: Incorrect

A virus has replicated itself throughout the infected systems and is executing its payload. Which of the following phases of the virus lifecycle is the virus in?

- Incorporation
- ~~Replication~~
- Design
- Launch

Explanation

Launch is the third phase of the virus life cycle. The virus is launched and executes its payloads in this phase.

The second phase in the virus life cycle is replication. In this phase, the virus replicates and spreads within the victim machine.

Incorporation is the fifth phase of the virus life cycle. In this phase, antivirus software developers design defenses against viruses.

Design is the first phase of the virus life cycle. This is the phase where the virus is created.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_MALWARE_OVERVIEW_VIRUS_02_EH1]

Question 5: Incorrect

Heather is performing a penetration test of her client's malware protection. She has developed a malware program that doesn't require any user interaction and wants to see how far it will spread through the network. Which of the following types of malware is she using?

- Virus
- Worm
- ~~Spyware~~
- Trojan horse

Explanation

A worm is a standalone malware program that can replicate without user interaction throughout a network.

A virus is a self-replicating malware that attaches itself inside a legitimate program. A hacker can define what they want the virus to do and how it will replicate.

Spyware is a type of malware that is designed to collect and forward information regarding a victim's activities to someone else.

A Trojan horse is a malware program that is hidden inside a legitimate program. When the user runs that

program, the Trojan horse runs in the background without the user's knowledge, giving the hacker remote access.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_MALWARE_OVERVIEW_WORM_01_EH1]

Question 6: Correct

Which of the following parts of the Trojan horse packet installs the malicious code onto the target machine?

- Dropper
- Server
- Construction kit
- Wrapper

Explanation

The dropper is the part of the Trojan horse that installs the malicious code onto the target machine. Creating the dropper is the second step in the process.

A construction kit is the software tool a hacker can use to create and customize a Trojan horse.

The server is the file in the Trojan horse that is dropped into the victim's machine and is what the hacker connects to.

The wrapper is the program that combines the server and dropper into a genuine application file.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_TROJANS_BACKDOORS_TROJAN_CREATE_01_EH1]

Question 7: Incorrect

Heather wants to gain remote access to Randy's machine. She has developed a program and hidden it inside a legitimate program that she is sure Randy will install on his machine. Which of the following types of malware is she using?

- Trojan horse
- ~~Worm~~
- Spyware
- Virus

Explanation

A Trojan horse is a malware program that is hidden inside a legitimate program. When the user runs that program, the Trojan horse runs in the background without the user's knowledge, giving the hacker remote access.

A virus is a self-replicating malware that attaches itself inside a legitimate program. A hacker can define what they want the virus to do and how it will replicate.

A worm is a standalone malware program that can replicate without user interaction throughout a network.

Spyware is a type of malware that is designed to collect and forward information regarding a victim's activities to someone else.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_TROJANS_BACKDOORS_TROJAN_FACTS_01_EH1]

Question 8: Incorrect

Which of the following malware types shows the user signs of potential harm that could occur if the user doesn't take a certain action?

- ~~Ransomware~~
- Adware
- Scareware
- Spyware

Explanation

Scareware shows the user signs of potential harm that could happen if the user doesn't take some sort of action, such as purchasing a specific program to clean the system.

Spyware collects and forwards information about the victim's activities to someone else.

Ransomware encrypts system files and folders and requires the victim to pay for the decryption key.

Adware causes an increase in pop-up and pop-under advertisements.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_MALWARE_CONCERNS_SCAREWARE_01_EH1]

Question 9: Incorrect

Patrick is planning a penetration test for a client. As part of this test, he will perform a phishing attack. He needs to create a virus to distribute through email and run a custom script that will let him track who has run the virus. Which of the following programs will allow him to create this virus?

- TCPView
- Webroot
- JPS
- ~~ProRat~~

Explanation

JPS Virus Maker is a common program that can perform many different tasks, including creating viruses and running a custom script.

ProRat is a popular creation kit that creates Trojan horses.

Webroot is an anti-virus program.

TCPView is a tool you can run on Windows to quickly and easily discover which network ports are in use on the local machine.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_MALWARE_ANALYSIS_CREATE_VIRUS_01_EH1]

Question 10: Incorrect

Rudy is analyzing a piece of malware discovered in a pentest. He has taken a snapshot of the test system and will run the malware. He will take a snapshot afterwards and monitor different components such as ports, processes, event logs, and more for any changes. Which of the following processes is he using?

- Sheep dipping
- ~~Malware disassembly~~
- Host integrity monitoring
- Static analysis

Explanation

Host integrity monitoring is part of the dynamic analysis process. The analyzer takes a snapshot of the testing computer before executing the malware. After the malware runs, the analyzer uses the same tools to take another snapshot and looks for any changes in the system.

Static analysis involves going through the actual code of the malware without executing it to understand what it does and its purpose using a variety of tools and techniques.

The process of analyzing emails, suspect files, and systems for malware is known as sheep dipping.

Malware disassembly is a technique used in static analysis. Disassembling the malware allows the analyzer to learn everything about the program and what its designed to do.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_MALWARE_ANALYSIS_DYNAM_ANALYSIS_01_EH1]

Question 11: Incorrect

Analyzing emails, suspect files, and systems for malware is known as which of the following?

- ~~Integrity checking~~
- Dynamic analysis
- Sheep dipping
- Static analysis

Explanation

The process of analyzing emails, suspect files, and systems for malware is called sheep dipping. The term comes from the process sheep farmers use to dip sheep in chemical solutions to clear them of parasites.

Static analysis is also known as code analysis. This involves going through the malware's code using a variety of tools and techniques to understand its purpose, but does not involve executing the code.

Dynamic analysis is the process of analyzing the malware by running it and observing its behavior and its effects on the system.

Integrity checking establishes a system baseline and alerts the user if any suspicious system changes occur.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_MALWARE_ANALYSIS_SHEEP_DIP_01_EH1]

Question 12: Incorrect

Which of the following best describes an anti-virus sensor system?

- Analyzing malware by running and observing its behavior and effects.
- ~~Software that is used to protect a system from malware infections.~~
- A collection of software that detects and analyzes malware.
- Analyzing the code of malware to understand its purpose without running it.

Explanation

A collection of software that detects and analyzes malware is known as an anti-virus sensor system. This system is used along with the sheep dip computer to perform malware analysis.

Anti-malware software is used to protect a system from malware infections.

Static analysis is also known as code analysis. This involves going through the malware's code using a variety of tools and techniques to understand its purpose, but does not involve executing the code.

Dynamic analysis is the process of analyzing the malware by running it and observing its behavior and

its effects on the system.

References

TestOut Ethical Hacker Pro - 9.1 Malware
[e_malware_eh1.exam.xml Q_MALWARE_ANALYSIS_SHEEP_DIP_02_EH1]