27: Lab 27: Detecting and responding to malware

Security+ (Exam SY0-701)

Solve ×

Congratulations, you passed!

Duration: 37 minutes, 7 seconds

☑ From the "Mitre Att&ck Matrix" section of the Zeus.x86 analysis report, what attack technique groups (i.e., columns) does this malware demonstrate? (Select all that apply) *Score: 1*

- ☑ Credential Access
- ☐ Privilege Escalation
- ☑ Command and Control
- ☐ Lateral Movement

Congratulations, you have answered the question correctly.

☑ When was this EICAR URL first seen in the wild? *Score: 1*

- ○ 2006-05-22 12:42:02 UTC
- ○ 2023-02-08 20:20:58 UTC
- ○ 2016-09-15 12:34:56 UTC
- ◉ 2010-08-11 15:12:06 UTC

Congratulations, you have answered the question correctly.

☑ On what tab of the VirusTotal analysis report will you find information about execution parents and bundled files? *Score: 1*

- ○ DETECTION
- ○ DETAILS
- ◉ RELATIONS
- ○ BEHAVIOR
- ○ COMMUNITY

Congratulations, you have answered the question correctly.

☑ What are the benefits of using a sandbox-based malware analysis tool? *Score: 1*

- ○ Quick analysis of suspicious files
- ○ Analysis performed separate from production systems
- ○ Automated evaluation of detonated code
- ○ Detailed information about evaluated samples
- ◉ All of the above

Congratulations, you have answered the question correctly.

What are the options to submit code samples to Joe Sandbox Cloud for analysis? (Select all that apply) *Score: 1*

- [ ] USB drive
- [x] Direct upload
- [x] URL
- [ ] Hash
- [x] Download and execute
- [x] Command line

Solve

Congratulations, you have answered the question correctly.

What types of submissions are supported by VirusTotal? *Score: 1*

- ( ) File upload
- ( ) URL retrieval
- ( ) Hash submission
- ( ) IP address
- ( ) Domain name
- (•) All of the above

Congratulations, you have answered the question correctly.

The EICAR test file (or string) is malicious code. *Score: 1*

- (•) False
- ( ) True

Congratulations, you have answered the question correctly.

When using an online malware scanning service uploading a file and using a hash of a suspicious file both provide confidentiality protection of sensitive information. *Score: 1*

- (•) False
- ( ) True

Congratulations, you have answered the question correctly.