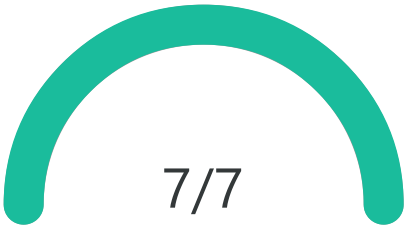
16: Lab 16 - Assisted - Working with threat feeds
Security+ (Exam SY0-701)



Congratulations, you passed!

Duration: 18 minutes, 26 seconds

☑ On the selected AlienVault Pulse page related to Mirai, what is one of the types of indicators? *Score: 1*

- ○ Host system
- ○ Victim ID
- ◉ FileHash
- ○ Registrar

Congratulations, you have answered the question correctly.

☑ Which of the following is **NOT** an option in the list of Filters for exploits on The Exploit Database? *Score: 1*

- ○ Authentication Bypass / Credentials Bypass
- ○ Code Injection
- ○ Deserialization
- ◉ Evil Twin / Rogue Access Point
- ○ Heap Overflow

Congratulations, you have answered the question correctly.

☑ What is the goal of researching and understanding IoCs? *Score: 1*

- ○ Improving response efficiency
- ○ Reducing resolution costs
- ◉ Detecting attempted and successful violations
- ○ Improving ROSI of IAM

Congratulations, you have answered the question correctly.

☑ What types of entities provide threat intelligence feeds? (Select all that apply) *Score: 1*

- ☑ Government agencies
- ☑ Commercial organizations
- ☐ Dark web groups

- [x] Open-source community groups

Congratulations, you have answered the question correctly.

What indicators are used to locate IoC entries on the AlienVault site? (Select all that apply) *Score: 1*

- [x] Domain
- [ ] MAC
- [x] URL
- [x] IPv4 or IPv6
- [x] Hostname
- [ ] OS type
- [x] FileHash

Congratulations, you have answered the question correctly.

What is unique about Exploit Database compared to most other exploit information sites and services? *Score: 1*

- ( ) Indication of the types of targets
- (•) Access to the source code of exploits
- ( ) List new and zero-day exploits
- ( ) Inclusion of exploits for hardware

Congratulations, you have answered the question correctly.

What is a Google dork? *Score: 1*

- ( ) A person who does not understand how to use keywords to search for content on Google
- ( ) A listing of symbols used to alter search functions when used in Google searches
- ( ) A type of hacker to performs OSINT using only Google searches
- (•) A search expression which may use advanced operators to discover security issues of indexed websites through a Google search

Congratulations, you have answered the question correctly.