OSINT for ICS/OT Course

Review Questions

Written by Mike Holcomb

Contents

NOTE: Some questions in this document were written at a specific point in time and might no longer be valid in the future.

Time stands still for no one.

Part 1: Course Introduction

There are no review questions for this part of the course.

Part 2: Getting Started with OSINT

1. Which of the following is not considered a type of intelligence?
    a. OSINT
    b. HUMINT
    c. ICSINT
    d. SIGINT

2. OSINT indirectly maps to which phases of the penetration testing methodology?
    a. Reconnaissance
    b. Scanning & enumeration
    c. Exploitation
    d. Post-exploitation

3. When starting a new engagement, what will be your most likely starting point?
    a. The LinkedIn profile of the target company's CEO
    b. The LinkedIn profile of the target company's CIO
    c. The target company's main website
    d. A Google search on the target company's financials

4. Which of the following is not a common way for attackers to gain access to an ICS/OT network?
    a. From the IT back office/enterprise network
    b. Physically brought in by "transitory cyber assets"
    c. Vía legitímate remote access capabilities
    d. Through control systems that are not exposed to the Internet

5. Which of the following is not considered a phase of the OSINT process?
    a. Planning

b. Collection
c. Analysis
d. Attribution

6. Which of the following can be used when performing OSINT to mask the true identity of an analyst?
    a. Sock puppet
    b. Packet sniffer
    c. Reverse proxy
    d. PLC and/or HMI

7. Which phase of the OSINT process includes determining the scope of the OSINT engagement?
    a. Planning
    b. Collection
    c. Processing
    d. Reporting and dissemination

8. Which phase of the OSINT process includes examining data to identify patterns and trends?
    a. Planning
    b. Collection
    c. Analysis
    d. Processing

9. The creator of which app was just arrested in France after major OPSEC fails by his traveling companion?
    a. Switch
    b. Telegram
    c. Signal
    d. Twitter/X

10. Which of the following tools could be used to help in OSINT investigations such as creating fake account profiles and writing sample OSINT reports?
    a. ChatGPT
    b. Facebook
    c. OneNote
    d. Obsidian

Part 3: Social Media

1. Which of the following platforms has over 1 billion users and is considered the social media platform for business?
    a. Facebook
    b. Instagram
    c. TikTok
    d. LinkedIn

2. Select the most accurate answer. Employees can post sensitive information on social media, including:
    a. Their employee badge
    b. Sensitive documents
    c. Information on the hardware and software their company uses
    d. Anything and everything

3. Which of the following would not be considered an internal threat?
    a. Employees with access to sensitive information
    b. A competitor in the same market
    c. Disgruntled team members
    d. Careless employees

4. Which of the following social media platforms is considered the largest search engine in the world after Google?
    a. Facebook
    b. TikTok
    c. YouTube
    d. LinkedIn

5. Which of the following “newgroup readers” is known for having PLC technicians and engineers post pictures of sensitive hardware and software?
    a. TikTok
    b. YouTube
    c. Reddit
    d. LinkedIn

6. Which of the following open source utilities can be used to determine if a profile name is used on dozens of different social media platforms?

a. Sherlock
b. Holmes
c. Investigator
d. SocialMediaPI

7. Which of the following would normally be considered an external threat?
    a. Hacktivists
    b. Disgruntled team members
    c. State adversaries
    d. Competitors

8. User profiles on which social media platform can be examined and used to often find which types of hardware and software are found at that user's company?
    a. Facebook
    b. Instagram
    c. TikTok
    d. LinkedIn

9. Which of the following is not included on a person's LinkedIn profile?
    a. Resume
    b. Banner
    c. Certifications
    d. Connections
10. When performing OSINT, which of the following would be considered illegal if you do not have authorization?
    a. Determining an employee's personal interests
    b. Finding when a company's CEO will be on vacation
    c. Asking a user of the platform for sensitive company information
    d. Discovering which hardware and software platforms are in use at a company

Part 4: Email Addresses, Usernames and Passwords

1. Email addresses are normally used by adversaries to launch all of the following except which?
    a. Phishing
    b. Privilege escalation
    c. Password spraying
    d. Credential stuffing

2. Which of the following tools can be used to quickly create an email scraper?
    a. ChatGPT
    b. Metasploit
    c. Sherlock
    d. Haveibeenpwned

3. Once a few email addresses for a target company have been discovered, an analyst could determine the company's email what?
    a. SPF record
    b. Subdomain
    c. MX record
    d. Format

4. Which of the following web platforms provides search capabilities including the options for Discover, Domain Search, Email Finder, Email Verifier and Signals?
    a. sherlock.io
    b. hunter.io
    c. shodan.io
    d. cybersearch.io

5. Which of the sites can be used to determine if a known email address is associated with a public breach?
    a. haveibeenhacked.com
    b. ohwowthatsucks.com
    c. haveibeenpwned.com
    d. dontclickme.com

6. Which of the following is a "collected" database of all data associated with known breaches as of January 2019?
    a. Collection #1
    b. Big Data #1
    c. Go Dawgs #1
    d. Dehashed #1
7. Which of the following Microsoft Windows services reveals usernames via a GUI on Shodan?
    a. SMB
    b. SSH
    c. IIS

    d. RDP
8. Which of the following would be considered the most secure pattern for creating user account names?
    a. mike
    b. m.holcomb
    c. mike.holcomb
    d. mh482971

9. Which of the following sites is a cost effective way to look up passwords associated with known breaches?
    a. Shodan
    b. Censys
    c. Dehashed
    d. Encrypted

10. Approximately what percentage of OT environments demonstrate users having the same password for both the IT and OT networks?
    a. 0%
    b. 25%
    c. 50%
    d. 75%

Part 5: Domain Names, IP Addresses & Autonomous System Numbers (ASNs)

1. The Google search of "site:netflix.com -www.netflix.com -help.netflix.com" can be used for which of the following?
    a. Subdomain enumeration
    b. Password spraying
    c. User account enumeration
    d. Credential stuffing

2. Which of the following tools is great for determining information related to a particular IP address or domain name?
    a. MX Tool Shed
    b. DNSlytics
    c. DNSdumpster
    d. Dehashed

3. Which of the following records can be reviewed for sensitive information such as the email addresses and phone numbers of IT employees at a target company?
    a. A record
    b. MX record
    c. WHOAMI
    d. WHOIS

4. Which of the following is an effective tool for easily finding subdomains and individual assets for a domain name?
    a. MX Tool Shed
    b. DNSlytics
    c. DNSdumpster
    d. Dehashed

5. Which one of the following DNS records is mostly like to expose sensitive information?
    a. A record
    b. MX record
    c. PTR record
    d. TXT record

6. Which of the following Project Discovery tools is effective at finding subdomains for a particular top-level domain?
    a. subfinder
    b. submarine
    c. GoSubmarine
    d. SpiderFoot

7. Which of the following tools was created by Steve Micallef in 2012 and is considered the “shotgun approach” of OSINT?
    a. Dehashed
    b. SpiderFoot
    c. GoSubmarine
    d. Hunter

8. Which of the following is considered to be a much more focused version of the tool mentioned in the previous question?
    a. BBOT

b. C3PO
c. Nmap
d. Smap

9. Which of the following Project Discovery tools can be used to determine the IP ranges associated with an ASN?
    a. DNSlytics
    b. DNSdumpster
    c. ASNmap
    d. ASNfinder
10. Which of the following can be used to identify all of the public IP address ranges associated with a (usually large) company?
    a. ASN
    b. DNS
    c. DOS
    d. BRO

Part 6: Traditional Search Engines

1. Which of the following is the name given to specialized Google searches designed to find one specific "type of thing" on the Internet?
    a. Google Dork
    b. Google Geek
    c. Google Meet
    d. Google prohibits this type of functionality

2. Which of the following Google advanced operators could be used to search a particular website for specific information?
    a. site:
    b. insite:
    c. title
    d. intitle

3. The following custom Google search can be used to find which type of ICS/OT asset exposed to the Internet?
    a. RDP
    b. HMI
    c. PLC
    d. Engineering workstation

4. Which of the following NSA projects released on GitHub provided several URLs for finding ICS/OT assets connected to the Internet?
    a. ELITEWOLF
    b. FINITECHOPPER
    c. TOPTIGER
    d. SOARINGEAGLE

5. Which of the following is discovered with Google using the following custom search:

    "/rokform/advancedDiags?pageReq=tcp"

    a. The memory diagnostics page on a Siemens PLC
    b. The TCP connections page on a AB/Rockwell PLC
    c. The CPU utilization on a Unitronics HMI/PLC
    d. The run mode status page on a CLICK PLC

6. Which of the following search engines is more likely to allow you to use specialized searches related to cyber security findings?
    a. YouTube
    b. Bing
    c. DuckDuckGo
    d. Google

7. Which is true about the following custom Google search?

    site:.edu intext:"robotics" inurl:/research

    a. It searches all websites except those ending in .edu
    b. It searches for a URL with the word research in it
    c. It searches for a directory named “research”
    d. It searches for the word “robotics” in the title of the webpage.

8. Which of the following custom Google searches can be used to find “legitimate” webcams (and not those associated with adult entertainment)?
    a. intitle:"Webcam" inurl:WebCam.htm
    b. title:"Webcam" dirl:WebCam.htm
    c. intitle:"Webcam" site:WebCam.htm
    d. site:"Webcam" inurl:WebCam.htm

9. Accessing the ELITEWOLF project file with Siemens signatures, which family type of Siemens asset would be found if using the signature as a Google search?
    a. S7-300
    b. S7-1200
    c. S7-2600
    d. S7-90210

10. Which of the following Google search operators can be used to load a previously saved copy of a website?
    a. proxy:
    b. cache:
    c. cloud:
    d. local:

Part 7: Specialized Search Engines for ICS/OT

1. Using the Open Infrastructure Map (openinframap.org), what is the southern most rated power station on the island of Manhattan (New York City)?
    a. Greensville County
    b. San Onofre
    c. Kinder Morgan Fordham
    d. Woodrow

2. What type of power station is the above?
    a. Nuclear
    b. Solar
    c. Geothermal
    d. Coal

3. Which of the following websites can be used for tracking security vulnerabilities related to ICS/OT?
    a. ICS Advisory Project
    b. OT Tenable Vulnerability Dashboard
    c. Dragos Community Defense Program
    d. ICS/OT VulnExchange

4. Which of the following Shodan searches would look for all potential PLCs running Modbus TCP/IP in the country of China?
    a. port:502 country:”cn”

b. port:102 country:”cn”
c. port:502 co:”cn”
d. port:102 co:”cn”

5. Which of the following ICS/OT protocols runs over TCP 44818?
    a. Modbus
    b. S7
    c. EthernetIP
    d. CODESYS

6. Which of the following usernames is exposed by the asset at 45.64.52.58?
    a. Admin
    b. Administrator
    c. Charles
    d. Xiaofeng

7. Which type of asset is exposed to the Internet purposefully to be attacked so researchers can learn from watching attacker activity?
    a. Remote access host
    b. EDR
    c. NIDS and/or NIPS
    d. Honeypot

8. Which of the following searches would find the string “Programmable Logic Controller” in returned banner information on hosts scanned by Shodan?
    a. Programmable Logic Controller
    b. “Programmable Logic Controller”
    c. ics:Programmable Logic Controller
    d. ics:”Programmable Logic Controller”

9. Which of the following ICS/OT vendors has the most reported vulnerabilities?
    a. Siemens
    b. Rockwell Automation
    c. Schneider Electric
    d. Delta Electronics

10. Which of the following tools can be used from the command line to lookup Shodan information in an Nmap format?

a. Shodan CLI
b. Nmap
c. Smap
d. SmapNG

Part 8: Writing a Successful OSINT Report

There are no review questions for this part of the course.

Answer Key

Part 1: Course Introduction

There are no review questions for this part of the course.

Part 2: Getting Started with OSINT

1. C
2. A
3. C
4. D
5. D
6. A
7. A
8. C
9. B
10. A

Part 3: Social Media

1. D
2. D
3. B
4. C
5. C
6. A
7. B
8. D
9. A
10. C

Part 4: Email Addresses, Usernames and Passwords

1. B
2. A
3. D
4. B
5. C
6. A
7. D
8. D

9. C
10. C

Part 5: Domain Names, IP Addresses & Autonomous System Names (ASN)

1. A
2. B
3. D
4. C
5. D
6. A
7. B
8. A
9. C
10. A

Part 6: Traditional Search Engines

1. A
2. A
3. C
4. A
5. B
6. D
7. C
8. A
9. B
10. B

Part 7: Specialized Search Engines

1. C
2. B
3. A
4. A
5. C
6. B
7. D
8. B
9. A
10. C

Part 8: Writing a Successful OSINT Report

There are no questions for this part.

Thank you for checking out the OSINT for ICS/OT course and the review questions!

If you have any questions, please don't hesitate to reach out to me on LinkedIn (linkedin.com/in/mikeholcomb) or by email (mike@mikeholcomb.com).