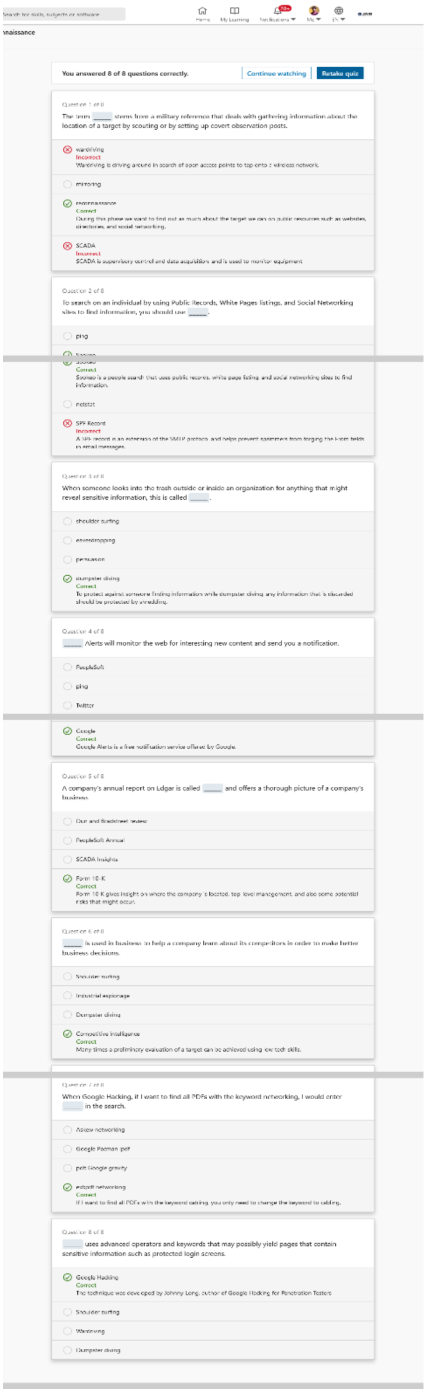
Introduction to the Course

In this course, we took a look at high and low-tech tools to scout our target. We first begun with a reconnaissance overview and then we saw how to use competitive intelligence. We examined search engines and look at Google hacking. We took a look at social media and the importance of tracking online reputation. We looked at email and website footprinting and how to mirror and monitor websites. We investigated email and email headers and we saw the power of open-source intelligence tools. We took a look at some of the reconnaissance tools that include footprinting network and examining ways to see how DNS can help us in our search. We looked at tools such as ping, tracert, nslookup, and dig. And then we looked at countermeasures for footprinting and reconnaissance and then pen testing reports which should be done at the end of every exercise. This course is part of the Ethical Hacking series.

Learning objectives

- Using competitive intelligence
- Hacking with search engines
- Using email for footprinting
- Getting social
- Mirroring websites
- Using Ping, Tracert, nslookup, and dig
- Taking footprinting countermeasures
- Pen testing for footprinting

Screenshots



You answered 8 of 8 questions correctly.

Question 1 of 8

The term _____ stems from a military reference that deals with gathering information about the location of a target by scouting or by setting up covert observation posts.

✗ wardriving
Incorrect
Wardriving is driving around in search of open access points to tap onto a wireless network.

○ mirroring

✓ reconnaissance
Correct
During this phase we want to find out as much about the target we can on public resources such as websites, directories, and social networking.

✗ SCADA
Incorrect
SCADA is supervisory control and data acquisition and is used to monitor equipment

Question 2 of 8

To search on an individual by using Public Records, White Pages listings, and Social Networking sites to find information, you should use _____.

○ ping

✓ Spokeo
Correct
Spokeo is a people search that uses public records, white page listing, and social networking sites to find information.

○ netstat

✗ SPF Record
Incorrect
A SPF record is an extension of the SMTP protocol and helps prevent spammers from forging the From fields in email messages.

Question 3 of 8

When someone looks into the trash outside or inside an organization for anything that might reveal sensitive information, this is called _____.

○ shoulder surfing

○ eavesdropping

○ persuasion

✓ dumpster diving
Correct
To protect against someone finding information while dumpster diving, any information that is discarded should be protected by shredding.

Question 4 of 8

_____ Alerts will monitor the web for interesting new content and send you a notification.

○ PeopleSoft

○ ping

○ Twitter

✓ Google
Correct
Google Alerts is a free notification service offered by Google.

Question 5 of 8

A company's annual report on Edgar is called _____ and offers a thorough picture of a company's business.

○ Dun and Bradstreet review

○ PeopleSoft Annual

○ SCADA Insights

✓ Form 10-K
Correct
Form 10 K gives insight on where the company 's located, top level management, and also some potential risks that might occur.

Question 6 of 8

_____ is used in business to help a company learn about its competitors in order to make better business decisions.

○ Shoulder surfing

○ Industrial espionage

○ Dumpster diving

✓ Competitive intelligence
Correct
Many times a preliminary evaluation of a target can be achieved using low tech skills.

Question 7 of 8

When Google Hacking, if I want to find all PDFs with the keyword networking, I would enter _____ in the search.

○ Askew networking

○ Google Pacman :pdf

○ pdf: Google gravity

✓ ext:pdf networking
Correct
If I want to find all PDFs with the keyword cabling, you only need to change the keyword to cabling.

Question 8 of 8

_____ uses advanced operators and keywords that may possibly yield pages that contain sensitive information such as protected login screens.

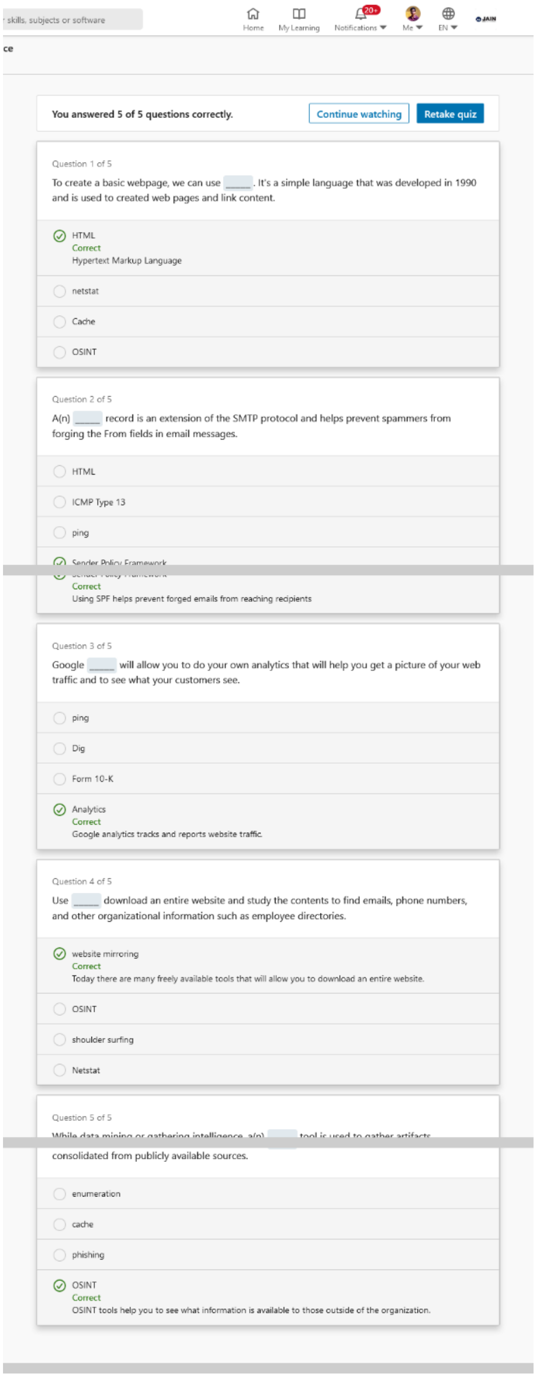
✓ Google Hacking
Correct
The technique was developed by Johnny Long, author of Google Hacking for Penetration Testers

○ Shoulder surfing

○ Wardriving

○ Dumpster diving

Figure: Section 01 – Reconnaince Overview



You answered 5 of 5 questions correctly.

Question 1 of 5

To create a basic webpage, we can use _____. It's a simple language that was developed in 1990 and is used to created web pages and link content.

✓ HTML
Correct
Hypertext Markup Language

○ netstat

○ Cache

○ OSINT

Question 2 of 5

A(n) _____ record is an extension of the SMTP protocol and helps prevent spammers from forging the From fields in email messages.

○ HTML

○ ICMP Type 13

○ ping

✓ Sender Policy Framework
Correct
Using SPF helps prevent forged emails from reaching recipients

Question 3 of 5

Google _____ will allow you to do your own analytics that will help you get a picture of your web traffic and to see what your customers see.

○ ping

○ Dig

○ Form 10-K

✓ Analytics
Correct
Google analytics tracks and reports website traffic.

Question 4 of 5

Use _____ download an entire website and study the contents to find emails, phone numbers, and other organizational information such as employee directories.

✓ website mirroring
Correct
Today there are many freely available tools that will allow you to download an entire website.

○ OSINT

○ shoulder surfing

○ Netstat

Question 5 of 5

While data mining or gathering intelligence, a(n) _____ tool is used to gather artifacts consolidated from publicly available sources.

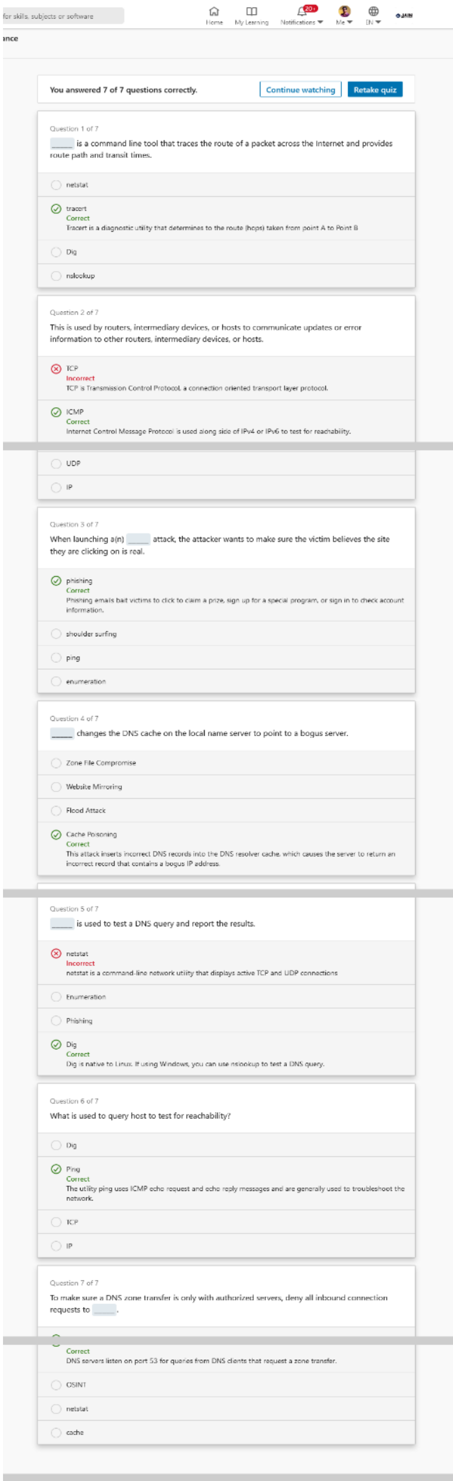
○ enumeration

○ cache

○ phishing

✓ OSINT
Correct
OSINT tools help you to see what information is available to those outside of the organization.

Figure: Section 02- Using email.& websites



You answered 7 of 7 questions correctly. Continue watching Retake quiz

Question 1 of 7

_____ is a command line tool that traces the route of a packet across the Internet and provides route path and transit times.

○ netstat

✓ tracert
Correct
Tracert is a diagnostic utility that determines to the route (hops) taken from point A to Point B

○ Dig

○ nslookup

Question 2 of 7

This is used by routers, intermediary devices, or hosts to communicate updates or error information to other routers, intermediary devices, or hosts.

⊗ TCP
Incorrect
TCP is Transmission Control Protocol, a connection oriented transport layer protocol.

✓ ICMP
Correct
Internet Control Message Protocol is used along side of IPv4 or IPv6 to test for reachability.

○ UDP

○ IP

Question 3 of 7

When launching a(n) _____ attack, the attacker wants to make sure the victim believes the site they are clicking on is real.

✓ phishing
Correct
Phishing emails bait victims to click to claim a prize, sign up for a special program, or sign in to check account information.

○ shoulder surfing

○ ping

○ enumeration

Question 4 of 7

_____ changes the DNS cache on the local name server to point to a bogus server.

○ Zone File Compromise

○ Website Mirroring

○ Flood Attack

✓ Cache Poisoning
Correct
This attack inserts incorrect DNS records into the DNS resolver cache, which causes the server to return an incorrect record that contains a bogus IP address.

Question 5 of 7

_____ is used to test a DNS query and report the results.

⊗ netstat
Incorrect
netstat is a command-line network utility that displays active TCP and UDP connections

○ Enumeration

○ Phishing

✓ Dig
Correct
Dig is native to Linux. If using Windows, you can use nslookup to test a DNS query.

Question 6 of 7

What is used to query host to test for reachability?

○ Dig

✓ Ping
Correct
The utility ping uses ICMP echo request and echo reply messages and are generally used to troubleshoot the network.

○ TCP

○ IP

Question 7 of 7

To make sure a DNS zone transfer is only with authorized servers, deny all inbound connection requests to _____.

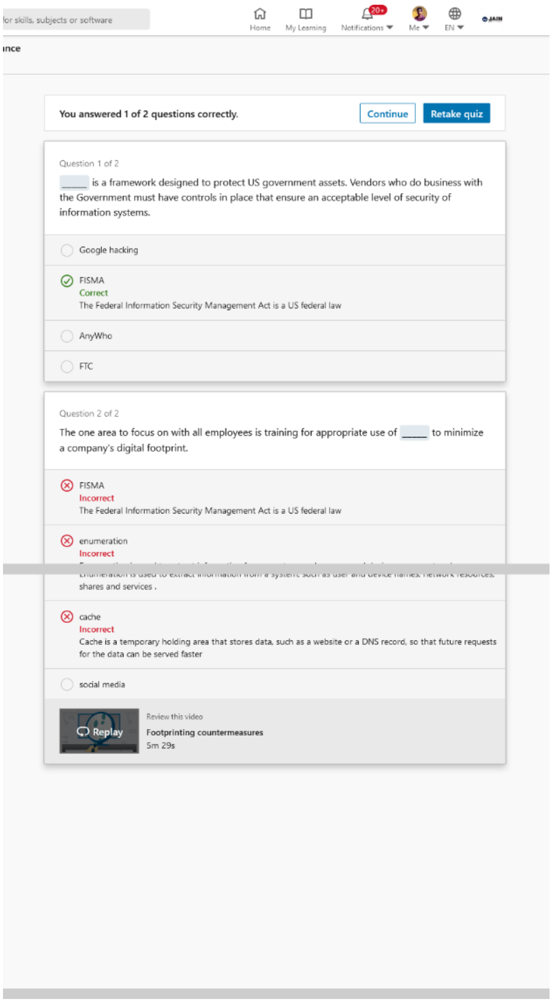
Correct
DNS servers listen on port 53 for queries from DNS clients that request a zone transfer.

○ OSINT

○ netstat

○ cache

Figure: Section 03 – Dicvovering Reconnsaince Tools



You answered 1 of 2 questions correctly. Continue Retake quiz

Question 1 of 2

_____ is a framework designed to protect US government assets. Vendors who do business with the Government must have controls in place that ensure an acceptable level of security of information systems.

○ Google hacking

✓ FISMA
Correct
The Federal Information Security Management Act is a US federal law

○ AnyWho

○ FTC

Question 2 of 2

The one area to focus on with all employees is training for appropriate use of _____ to minimize a company's digital footprint.

⊗ FISMA
Incorrect
The Federal Information Security Management Act is a US federal law

⊗ enumeration
Incorrect
Enumeration is used to extract information from a system, such as user and device names, network resources, shares and services .

⊗ cache
Incorrect
Cache is a temporary holding area that stores data, such as a website or a DNS record, so that future requests for the data can be served faster

○ social media

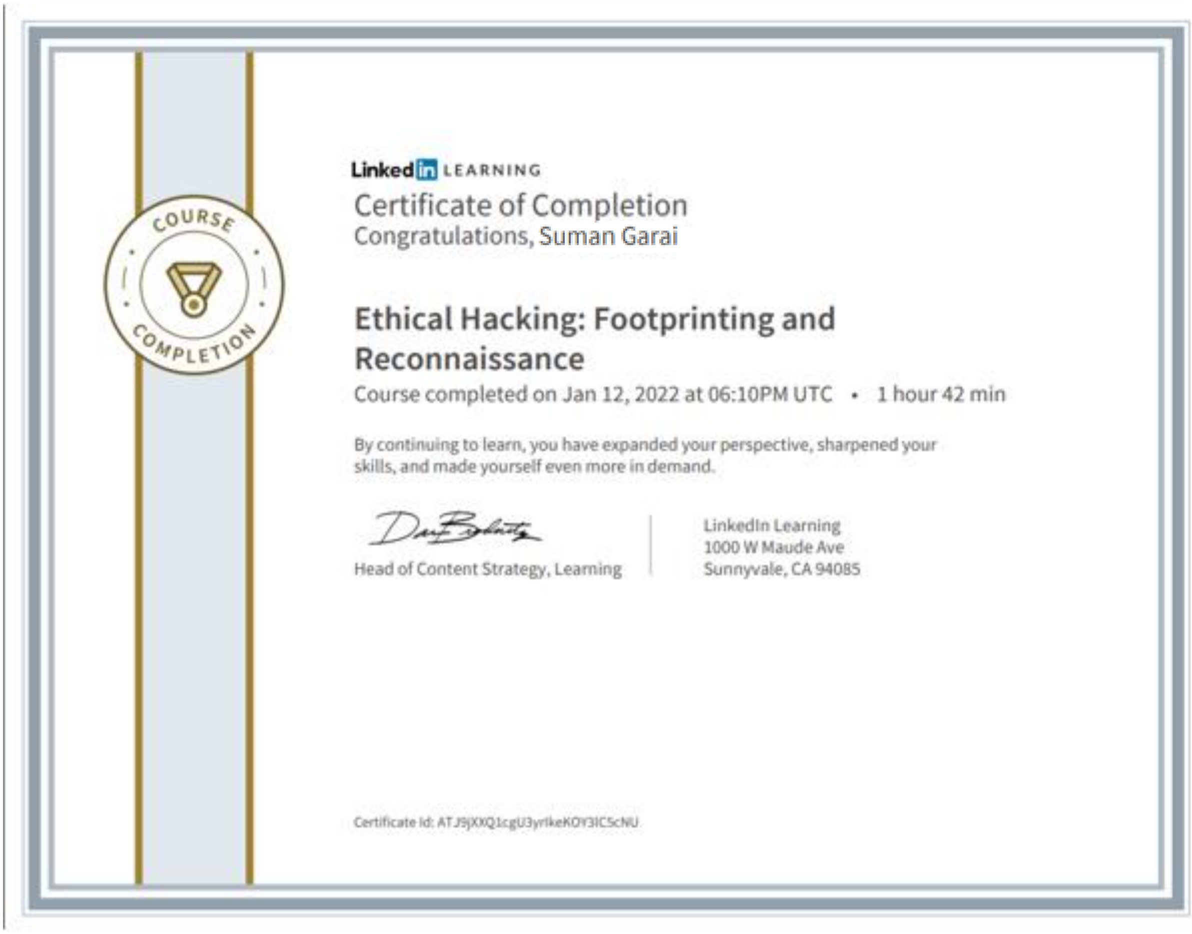
Replay
Review this video
Footprinting countermeasures
5m 29s

Figure: Section 04- Conclusion

Conclusion

I got provided an overview on footprinting and reconnaissance. We took a look at search engines and the power of Google hacking. We looked at social media and the importance of tracking your online reputation. We learnt about tools like Google Hacking Databases, AnyWho, Spokeo. We took a look at websites and email footprinting and how to mirror and monitor websites and looked closer at investigating email and seeing the story that email headers will tell us. We then looked at some of the reconnaissance tools to help us in our investigation, the competitive intelligence, OSINT tools like Maltego & Shodan, and how to footprint networks. We looked at utilities, such as ping, tracert, nslookup, and dig. Then we studied ways to prevent and then document our efforts. We looked at countermeasures for footprinting and reconnaissance, and then ways to compile penetration tests and the resultant reports.

Certificate



Linked in LEARNING

Certificate of Completion

Congratulations, Suman Garai

Ethical Hacking: Footprinting and Reconnaissance

Course completed on Jan 12, 2022 at 06:10PM UTC • 1 hour 42 min

By continuing to learn, you have expanded your perspective, sharpened your skills, and made yourself even more in demand.

Head of Content Strategy, Learning

LinkedIn Learning
1000 W Maude Ave
Sunnyvale, CA 94085

Certificate Id: ATJ9jXXQ1cgU3yrlkeKOY3IC5cNU