|  |
| --- |
|  |
| Capstone Experience  Summer 2025- IST 894  **Dr. Mike Bartolacci** |
| **Lab 4: Common Attack Types and Recon and Footprinting** |

|  |  |
| --- | --- |
| Mike Carver | 6/29/25 |

Contents

[General Context 3](#_Toc201842245)

[Technical Context 3](#_Toc201842246)

[Screenshots 5](#_Toc201842247)

[Common Attack Types 5](#_Toc201842248)

[Recon and Footprinting 7](#_Toc201842249)

[References 8](#_Toc201842250)

# General Context

This lab covered a cyber range, Common Attack Types, and a course, Recon and Footprinting. The cyber range used software to test and demonstrate how injection attacks occur. These attacks occur when a vulnerability allows for code to be added or executed to use the system in an unintended way (Lenaerts-Bergmans, 2024). For example, coding can be added to a password field that allows an SQL Injection to bypass a password for an account.

The course covers the Recon stage of the Cyber Kill Chain (Hospelhorn, 2016). The Cyber Kill Chain is an eight-phase process of a cybersecurity attack. This phase focuses on the initial intelligence gathering on a network. There are several free tools that can be used to actively or passively scan networks or websites for information.

This course also focuses on Open-Source Intelligence. This type of intelligence is where information that is open to the public is used. This could be common known IP addresses for specific companies. This can also involve looking for people who work in certain departments to send phishing emails to.

# Technical Context

This lab went over a cyber range, Common Attack Types, and a course, Recon and Footprinting. The cyber range covered several injection types. The first type examined was HTML Injections. These can be categorized by reflected injections and stored injections. Reflected injections are not permanently stored on a server and use URLs to trick users into executing the malicious code (Imperva, 2019). The lab used a first and last name field to demonstrate this. Using the HTML for bold, we were able to bold the first name. This can then be used to gain information about the system or anything attached to it via HTML code. Stored injections, or persistent injections, are permanently stored on servers (Imperva, 2019). This allows attackers to affect many users without any work other than the original exploit. The example in this lab was inserting a link in a blog post. This then allows the malicious code to blend in with blog posts and potentially bypass any vetting the site may have.

This cyber range also covered OS Command Injection and SQL Injection. OS Command Injection, or Shell Injection, is an attack that targets the OS that is running the program (PortSwigger, n.d.). This lab used a DNS lookup field to test these. We were able to run two commands to find the user information and ping a specific IP address from the OS of the DNS server. This could allow us to potentially add users and escalate privileges on the host machine or potentially use it to gain more intelligence or entry to the larger network. The last section of this lab used SQL Injection. SQL is used in database management. We were able to see the entire list of movies with the classic ‘ or ‘1’=’1’ SQL command.

The first video in the Recon and Footprinting course focuses on tools to be used for recon. One of the most useful is Maltego. Maltego is an investigation tool that can be used to gain information from sites on the internet (Maltego, n.d.). The instructor uses this tool later in the course to crawl the Infosec website and find all emails associated with the domain. The second video in the course focuses on OS Int applications. By using Google, the instructor was able to gain access to unsecured cameras. With the use of a website specializing in Google queries, the instructor also gained access to an account username and password open to the internet to see. This could allow anyone able to find the file to gain access to the site through the portal.

# Screenshots

## Common Attack Types

A screenshot of a computer

AI-generated content may be incorrect.

Figure 1: Image of Cyber Academy.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 2: Image of successful HTML Injection on a name field.

A computer screen shot of a computer

AI-generated content may be incorrect.

Figure 3: Image of successful HTML Injection on a blog.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 4: Image of successful injection for names on a DNS lookup field.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 5: Image of successful injection of a ping command on a DNS lookup field.

A screenshot of a computer

AI-generated content may be incorrect.

Figure 6: Image of successful SQL injection.

## Recon and Footprinting

A certificate of completion

AI-generated content may be incorrect.

Figure 7: Image of the certificate for the Recon and Footprinting course.

# References

Hospelhorn, S. (2016, June 20). *What is The Cyber Kill Chain and How to Use it Effectively | Varonis*. Www.varonis.com. https://www.varonis.com/blog/cyber-kill-chain

Imperva. (2019). *HTML Injection | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/html-injection/

Lenaerts-Bergmans, B. (2024, May 3). *What Is an Injection Attack?* Crowdstrike.com. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/injection-attack/

Maltego. (n.d.). Homepage. Www.maltego.com. Retrieved June 26, 2025, from https://www.maltego.com/

PortSwigger. (n.d.). *What is OS command injection, and how to prevent it?* Portswigger.net. Retrieved June 26, 2025, from https://portswigger.net/web-security/os-command-injection