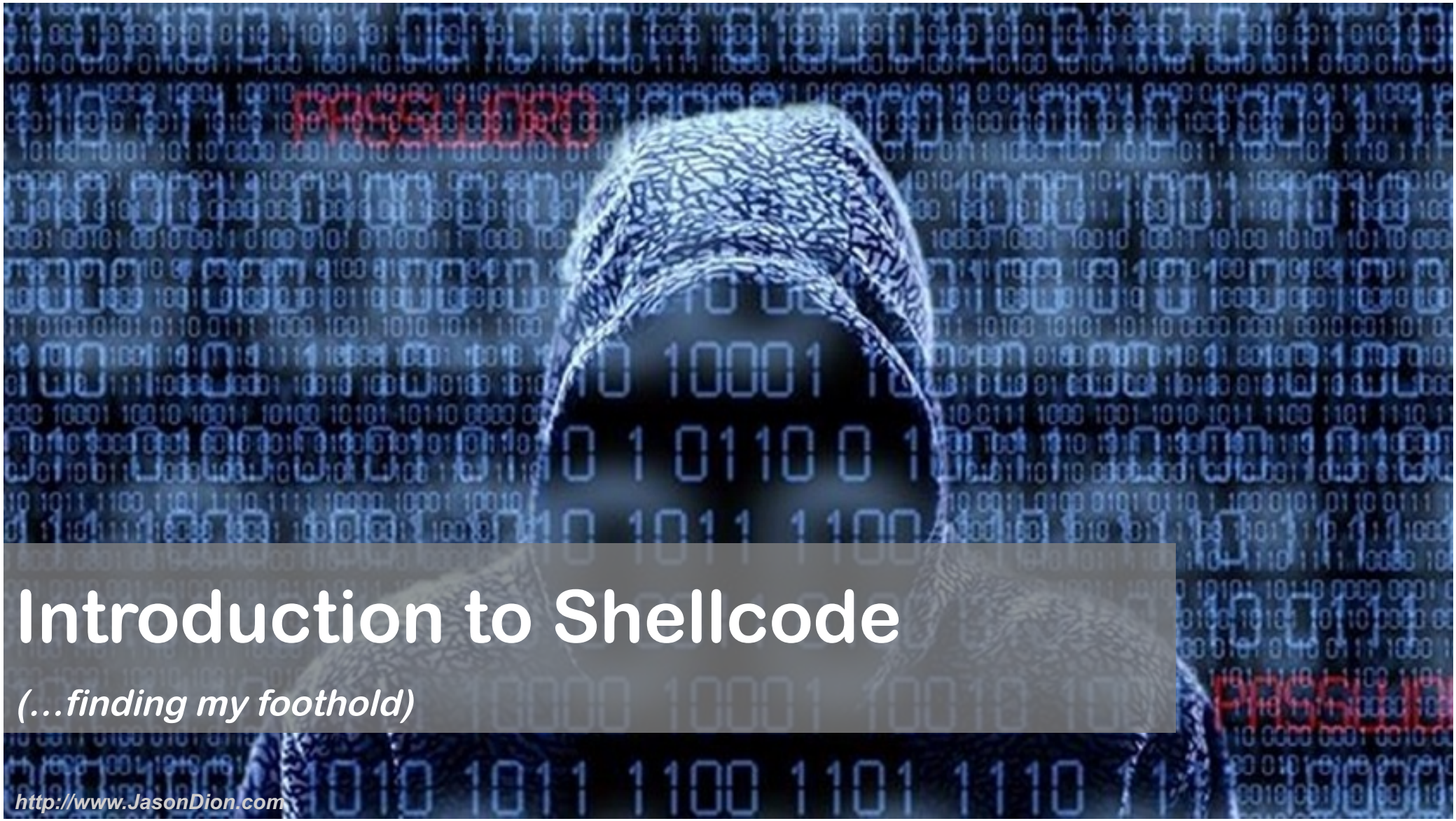


Introduction to Shellcode

(…finding my foothold)

http://www.JasonDion.com

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

What is Shellcode?

- Small piece of code used as payload in exploitation of a software vulnerability
- Easily reused in other exploits

What does Shellcode do?

- Typically starts a command shell from which the attacker can use for interactive command execution

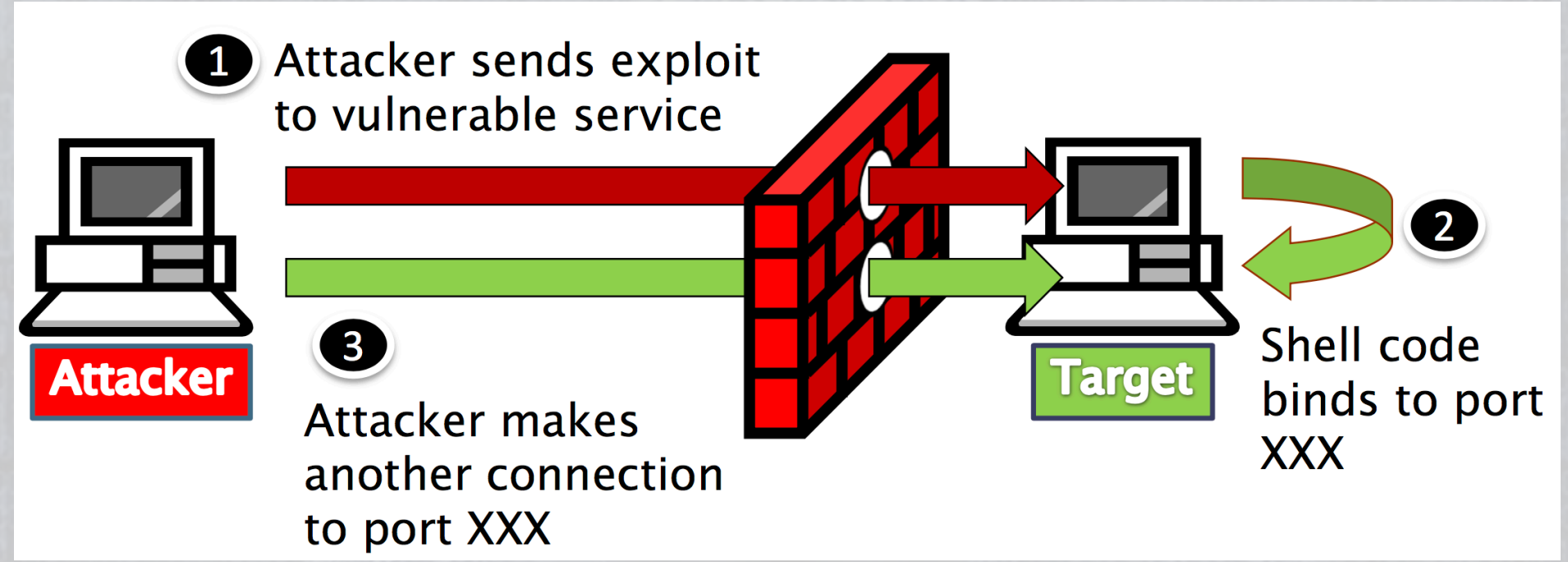
How to make Shellcode?

- Commonly written in machine code
- But, any piece of code that performs a similar task can be called shellcode

Examples of Shellcode

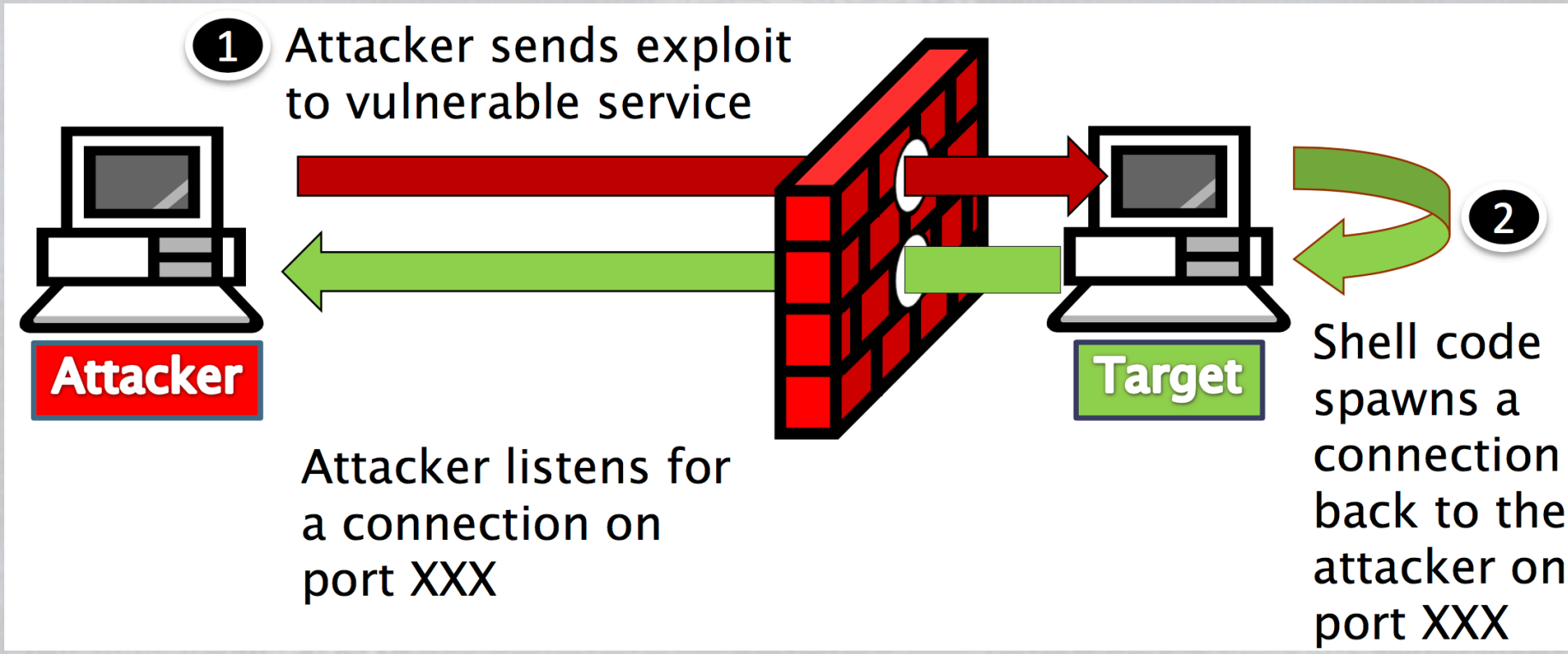
- Bind Shell
- Reverse Shell
  - We will use this in the lab!

How Bind Shells Works



Requires additional open ports on the firewall for this to work

How Reverse Shells Works



Once vulnerable service is exploited, the target machines contacts us!

What are staged payloads?

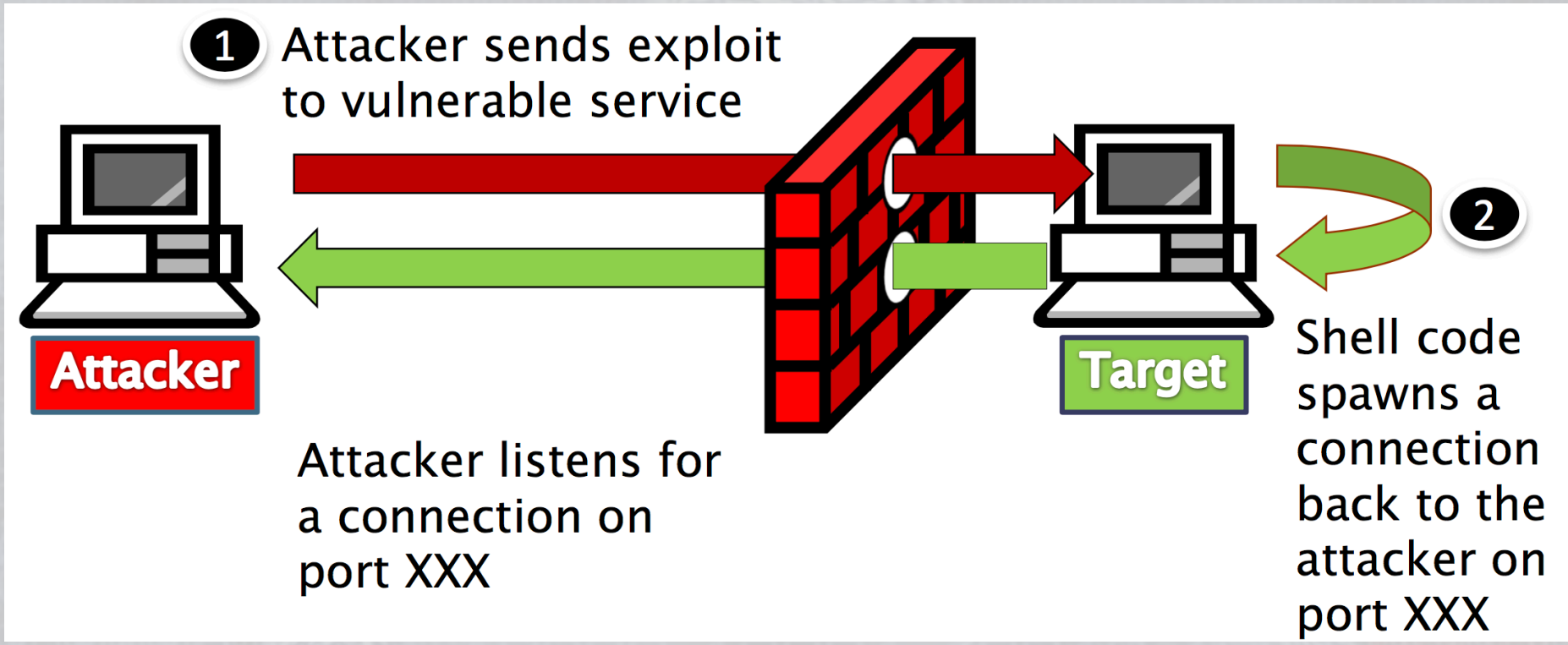
- If shellcode is too large to pass at once, the shellcode could be broken into smaller stages.

- Helps keep attack quieter

How staged payloads work

- Stage 1
  - Attacker passes small piece of shellcode to the target
- Stage 2
  - Shellcode reaches back to grab larger piece of code

Reverse Shell in our Lab



Windows/shell/reverse_tcp is a "staged" payload

Attacker's Methodology

Performing Reconnaissance

Scanning and Enumeration

Gaining Access

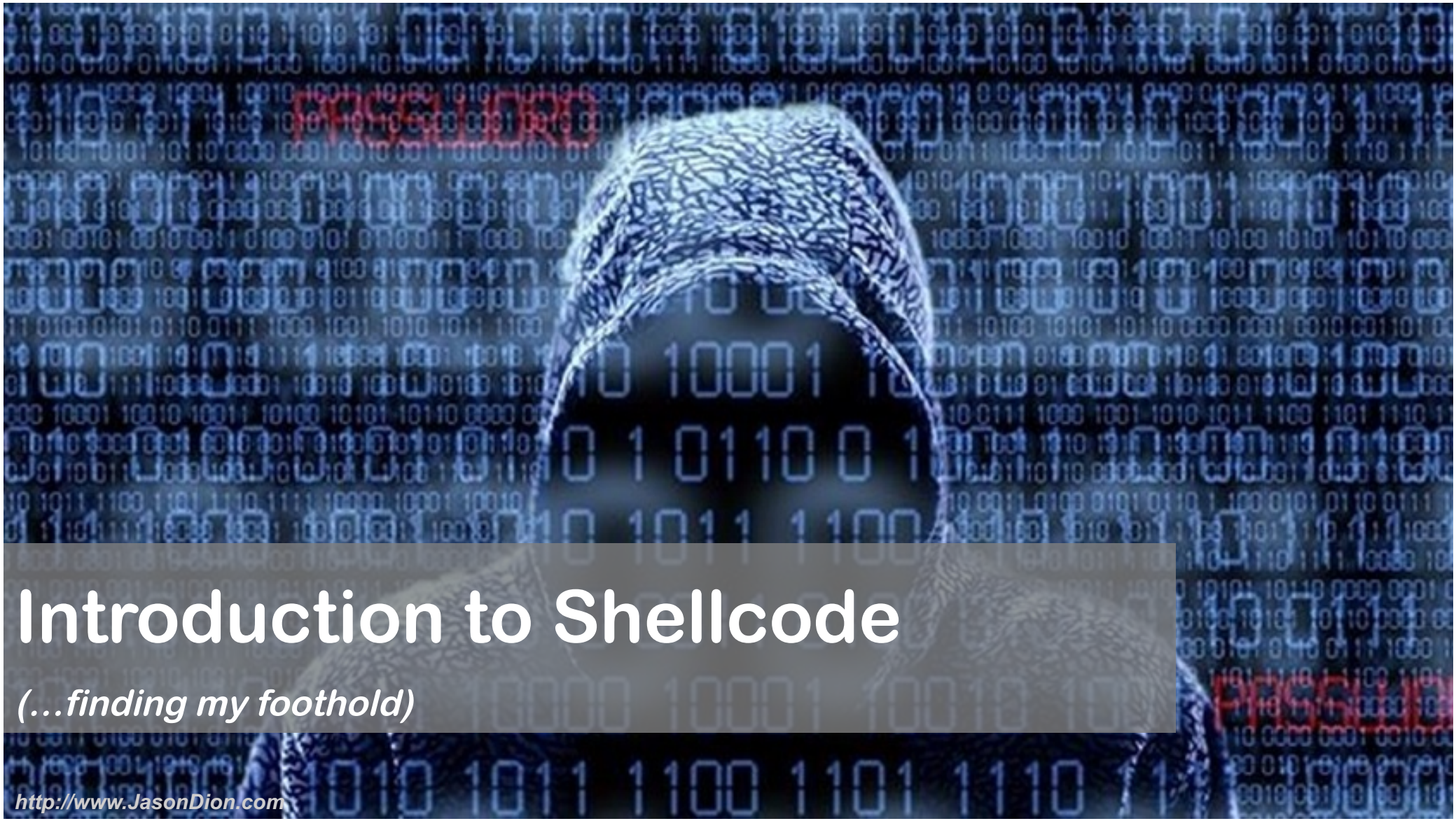
Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level



Introduction to Shellcode

(…finding my foothold)

http://www.JasonDion.com