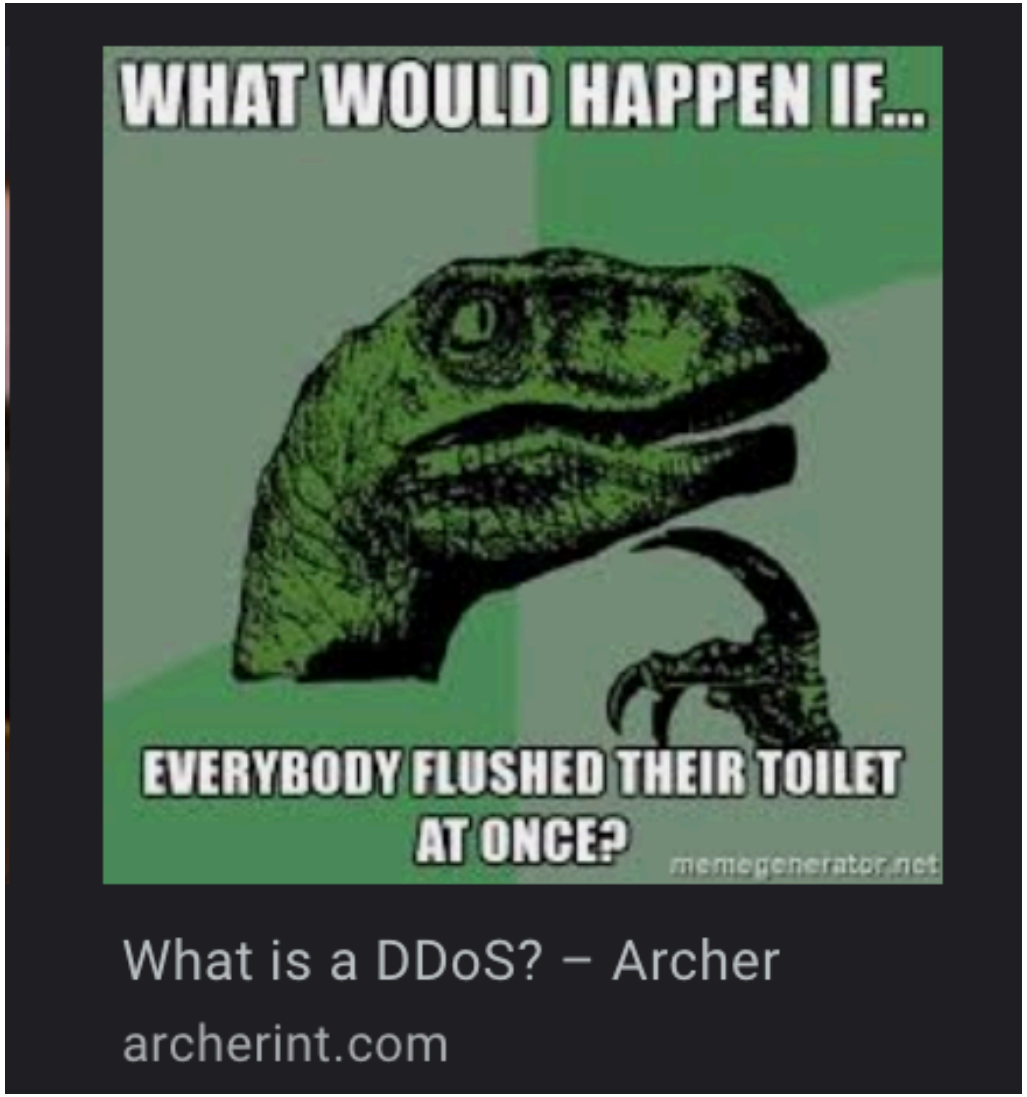
COS30015 – Lab 5

Denial of Service (DoS)

Presented by Jamie Ooi

jooi@swin.edu.au

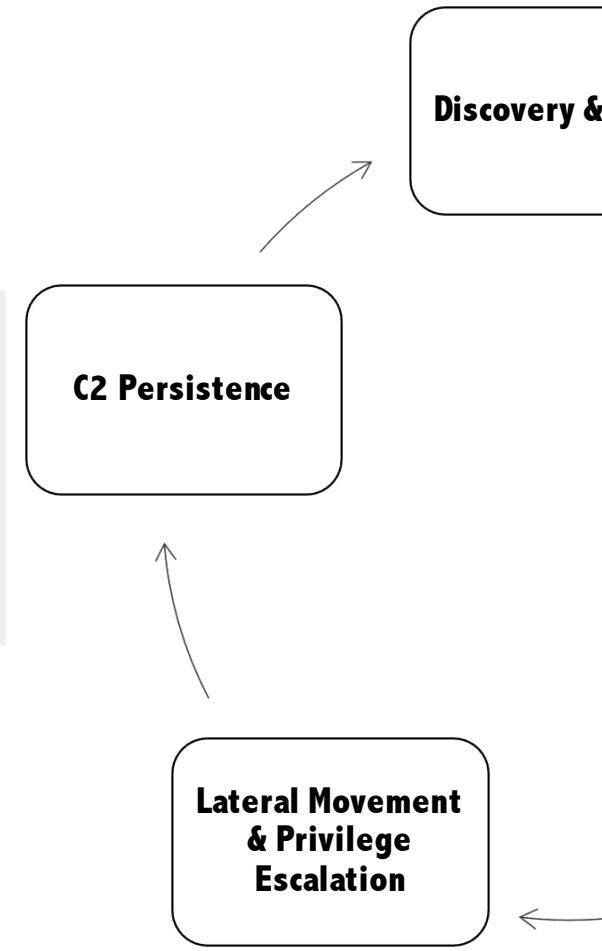
Thursday 1 September, 2022



SWINBURNE UNIVERSITY OF TECHNOLOGY

COS30015 IT Security – Lab 5 Background

Red Team Methodology



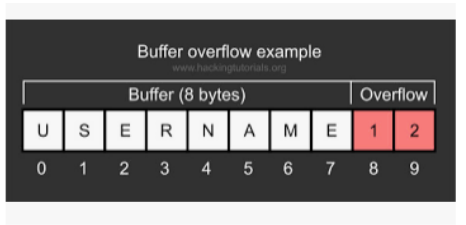
Lab 2 - Fingerprinting

accuracy of facial recognition - BBC News
bbc.com

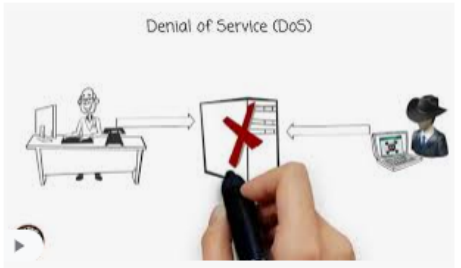
Lab 4 – Malware Implant

What is Malware and How Does It Work?
searchsecurity.techtarget.com

Lab 3 – Buffer Overflow Identification



ıe basics ...



Denial of Service (DoS) - YouTube
youtube.com

Lab 5 – Denial of Service

SWINBURNE UNIVERSITY OF TECHNOLOGY

COS30015 IT Security – Lab 5 Background

User Specified Object Allocation

```
String TotalObjects = request.getParameter("numberofobjects");
int NumOfObjects = Integer.parseInt(TotalObjects);
ComplexObject[] anArray = new ComplexObject[NumOfObjects];  // wrong!
```

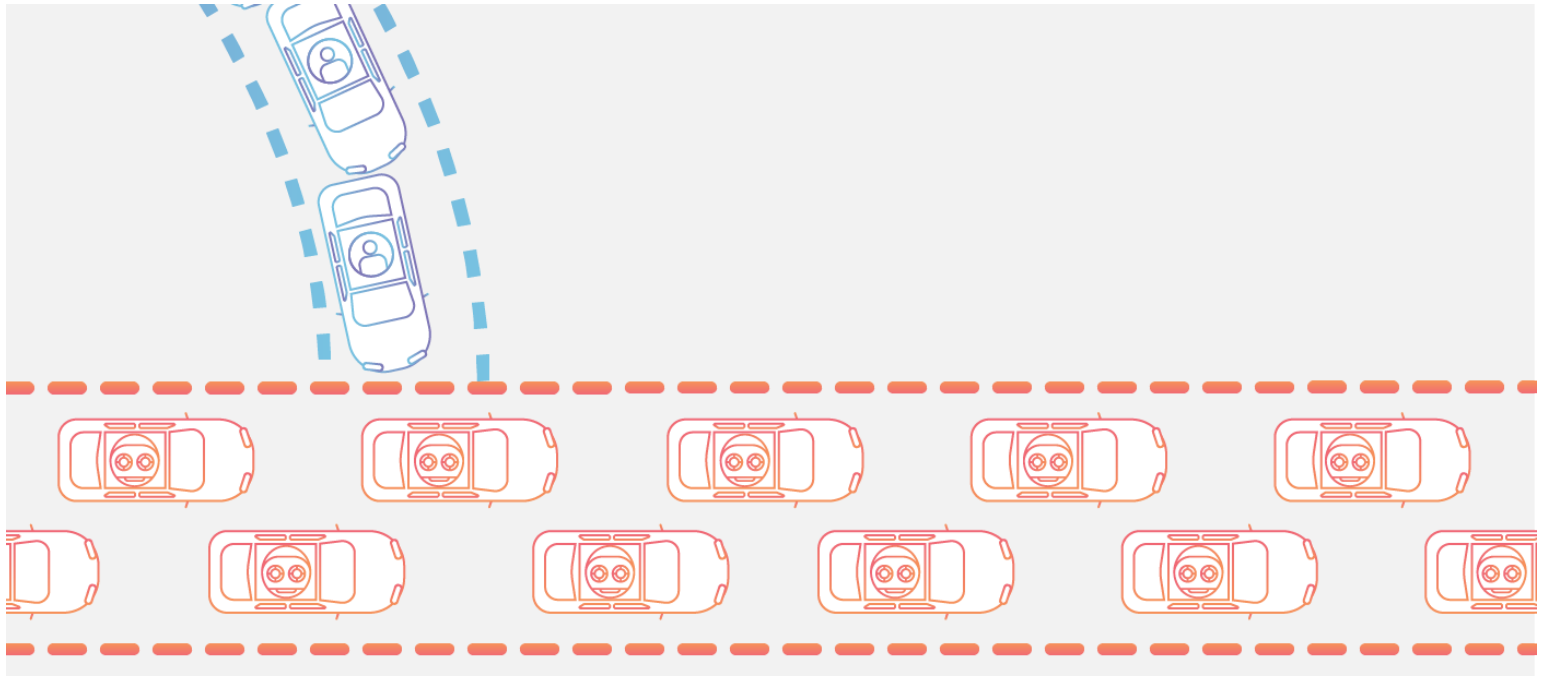
User Input as Loop Counter

```
public class MyServlet extends ActionServlet {
   public void doPost(HttpServletRequest request, HttpServletResponse response)
          throws ServletException, IOException {
          . . .
          String [] values = request.getParameterValues("CheckboxField");
      // Process the data without length check for reasonable range – wrong!
          for ( int i=0; i<values.length; i++) {
                // lots of logic to process the request
          }
```

Reference: https://owasp.org/www-community/attacks/Denial_of_Service

COS30015 IT Security – Lab 5 Background

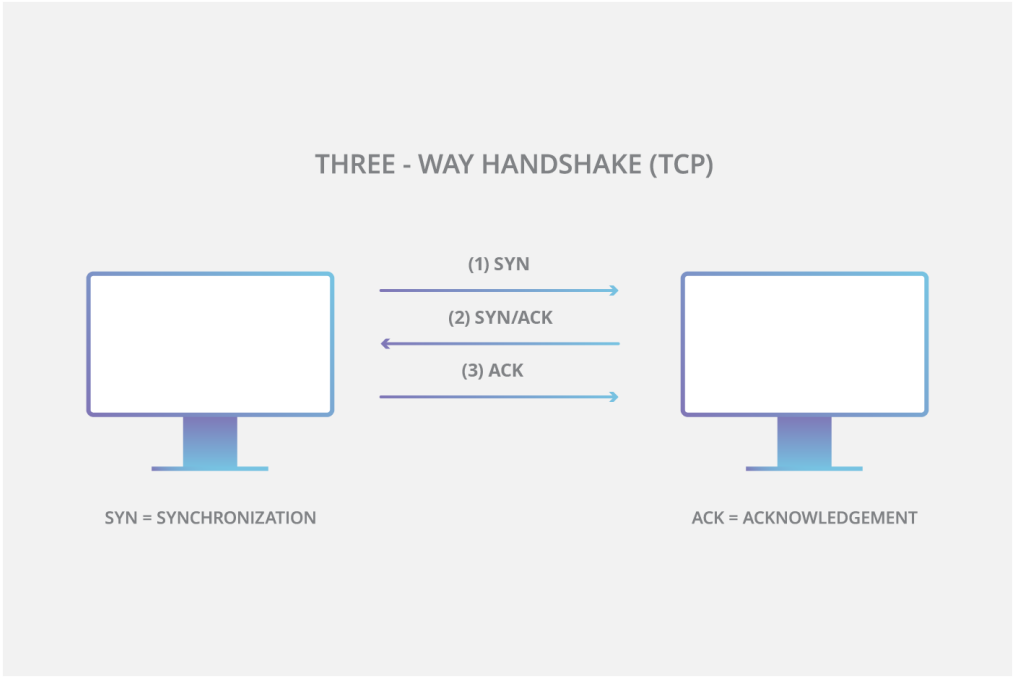
Volumetric Flood



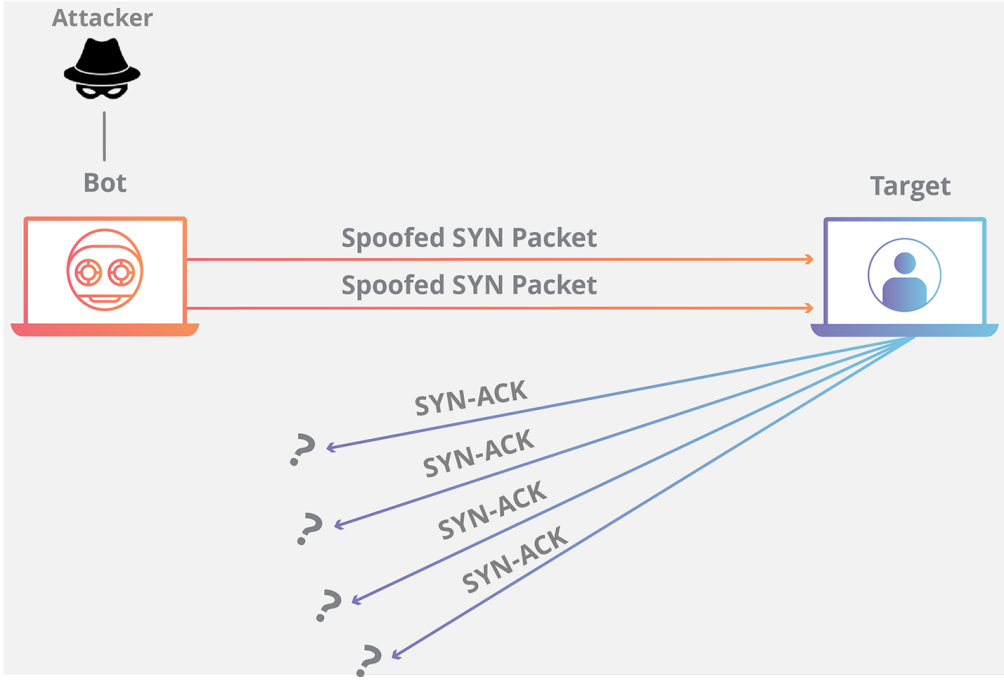
HTTP flood DDoS attack | Cloudflare
cloudflare.com

COS30015 IT Security – Lab 5 Background

SYN Flood



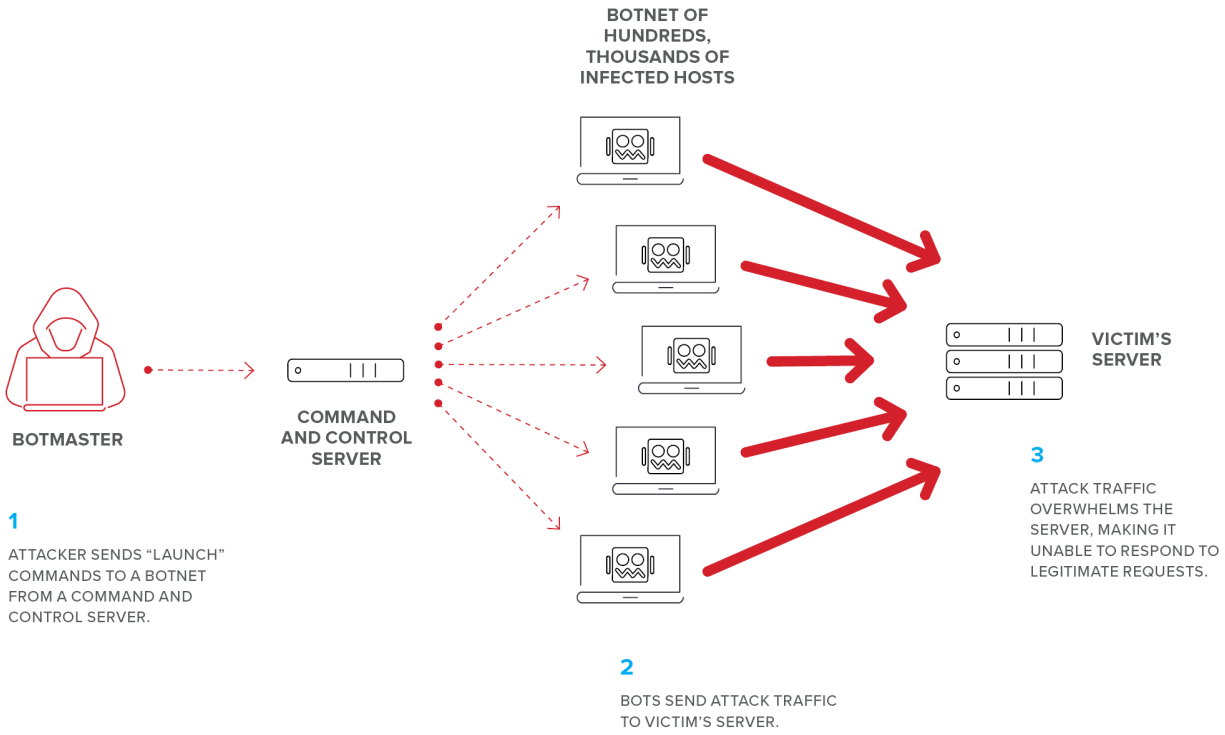
SYN flood DDoS attack | Cloudflare
cloudflare.com



SYN flood DDoS attack | Cloudflare
cloudflare.com

COS30015 IT Security – Lab 5 Background

Distributed Denial of Service (DDoS)



DDoS) Attack ...
f5.com

COS30015 IT Security – Lab 5 Background

Big Attacks

Mirai, 2017

- 620 Gbps
- 600,000 IOT Devices (Including IP Cameras, video recorders, Home routers)

(Source: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/)

Github, 2018

- 1.35 Tbps
- Amplification (Memcached)

(Source: https://github.blog/2018-03-01-ddos-incident-report/)

Google, 2017

- 2.5 Tbps / 167 Mpps
- Amplification (CLDAP, DNS and SMTP)

(Source: https://cloud.google.com/blog/products/identity-security/identifying-and-protecting-against-the-largest-ddos-attacks)

COS30015 IT Security – Lab 4 Background

when my computer is slow - Meme Generato

meme-generator.com

Three Virtual Machines

Kali,

CYSCA2014InABox,

Windows 95

Questions ?

Email: jooi@swin.edu.au
Linkedin: https://www.linkedin.com/in/jamie-ooi-15297b98/

Thursday 1 September, 2022

Reminder:
Assignment 1 is due in 1 week!