COS30015 – Lab 4

C2 Persistence

Presented by Jamie Ooi

Thursday 25 August, 2022

COS30015 IT Security – Lab 4 Background

Red Team

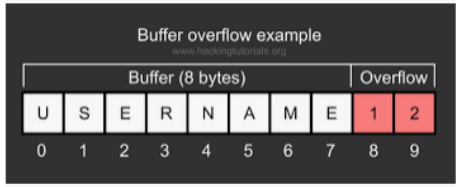
Lab 2 - Fingerprinting

accuracy of facial recognition - BBC News
bbc.com

Discovery & Recon

Analysis

Lab 3 – Buffer Overflow Identification



Buffer overflow explained: The basics ...
hackingtutorials.org

Exploitation

Lateral Movement & Privilege Escalation

C2 Persistence

Lab 4 – Malware Implant

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

COS30015 IT Security – Lab 4 Background

Command and Control (C2) Persistence

To establish persistent (forever, kinda) access on your target

- Methods of delivery: phishing, USB drop, browser drive by, untrusted downloads, file upload
- Some examples of maintaining persistent access:
  - Kerberoasting Golden Ticket
  - Anti-virus Evasion
  - Reverse Shell
  - Privilege Escalation to Domain Administrator

Lab 4 – Malware Implant

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

COS30015 IT Security – Lab 4 Background

Stuxnet

Ooh a free usb drive - Piece of Candy ...
memegenerator.net

- Discovered in 2010, was dormant / active since 2005
- Targeted SCADA systems
- Delivered via an infected USB drive – breached the "*air gap*"
- Identified because it accidentally infected an engineer's computer
- Infects a computer and then scans the network for specific Siemens software
- Tweaked the frequency of the centrifuges at specified time of the day, so that parts were being thrown out

COS30015 IT Security – Lab 4 Background

when my computer is slow - Meme Generato

meme-generator.com

Three Virtual Machines

RedHat Linux 7.3,

WindowsXP Control,

Windows XP

Questions ?

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

Thursday 25 August, 2022

Reminder:
Assignment 1 is due in 2 weeks!