SANGFOR

Is Red Team a Hero or Villain?

David Chan | Systems Engineer Director

中华人民共和国
网络安全法

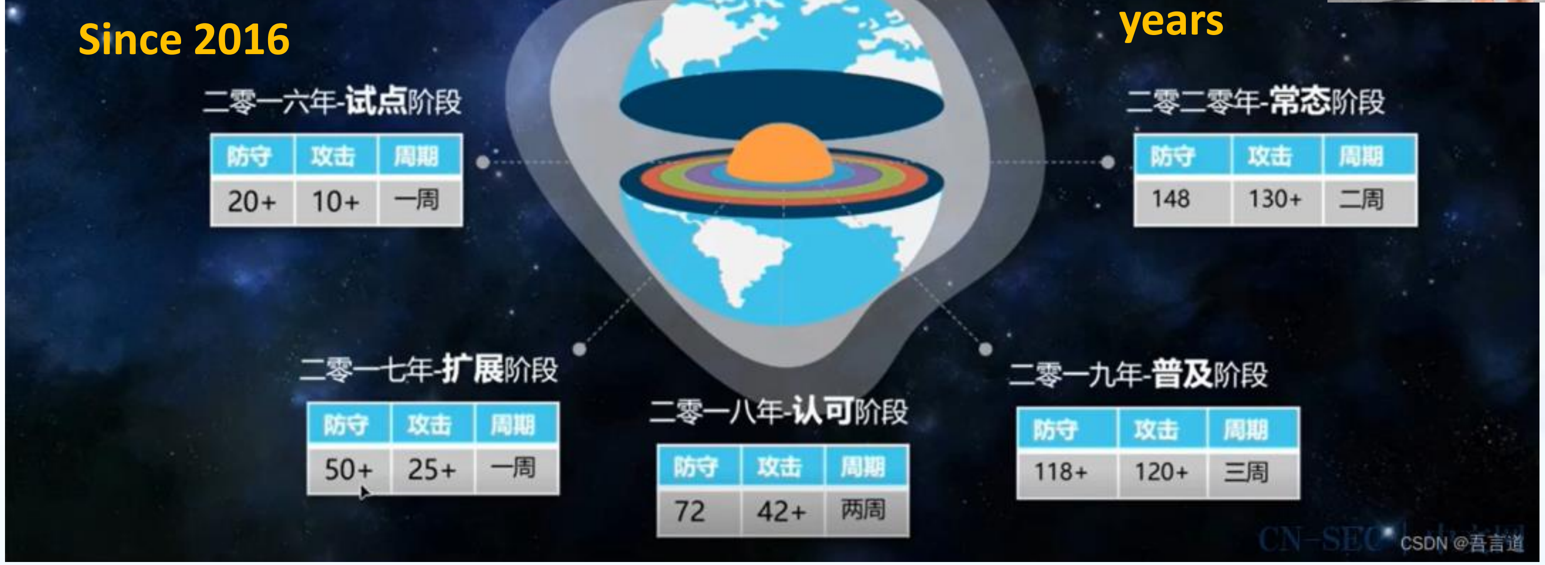
含草案说明

中国法制出版社

護網行動/护网行动/HW

Sangfor as National Team for Red Team Exercise

國家隊
(Red Team)



Since 2016

In the past 6 years

二零一六年-试点阶段

防守	攻击	周期
20+	10+	一周

二零一七年-扩展阶段

防守	攻击	周期
50+	25+	一周

二零一八年-认可阶段

防守	攻击	周期
72	42+	两周

二零一九年-普及阶段

防守	攻击	周期
118+	120+	三周

二零二零年-常态阶段

防守	攻击	周期
148	130+	二周

DSE 模擬考試 - 唔考, 唔知分數高

- Examination Procedure
- Examination Atmosphere
- Answering Question Technique

2021-2022
數據數學新高中文憑試
中六（必修部份）模擬考試服務
2020-DSE
MATH CP
PAPER 1
HONG KONG EXAMINATIONS AND ASSESSMENT AUTHORITY
HONG KONG DIPLOMA OF SECONDARY EDUCATION EXAMINATION 2014
Please stick the barcode label here
Candidate Number

模擬網絡攻擊 (Red Team)

無受攻擊, 唔知防守好

Terrorist (T) Side Takes an Aggressive Stance

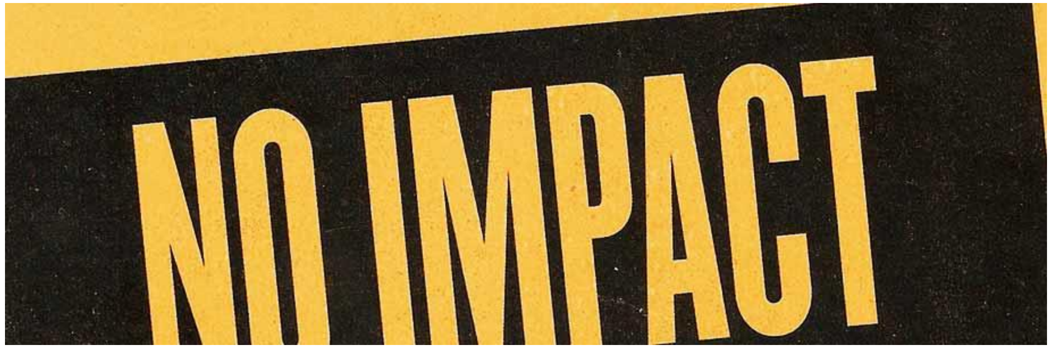
Red Team

- Real hacker attack tactics
- Dig Out Vulnerabilities
- Attack on those vulnerabilities

Counter Terrorist (CT) Side Takes of Defending

Blue Team

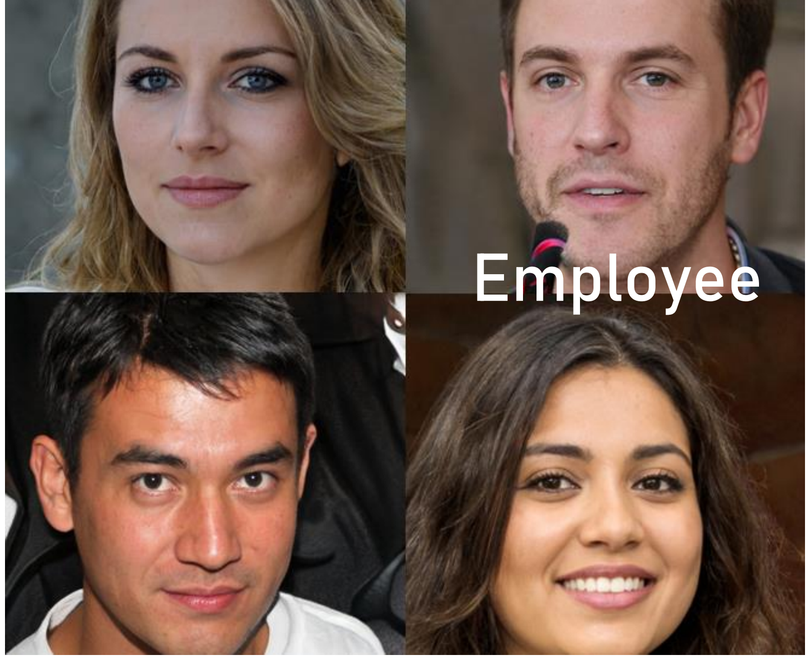
- Defence
- Capture The Flag



- **NO** service interruption
- **NO** information stealing

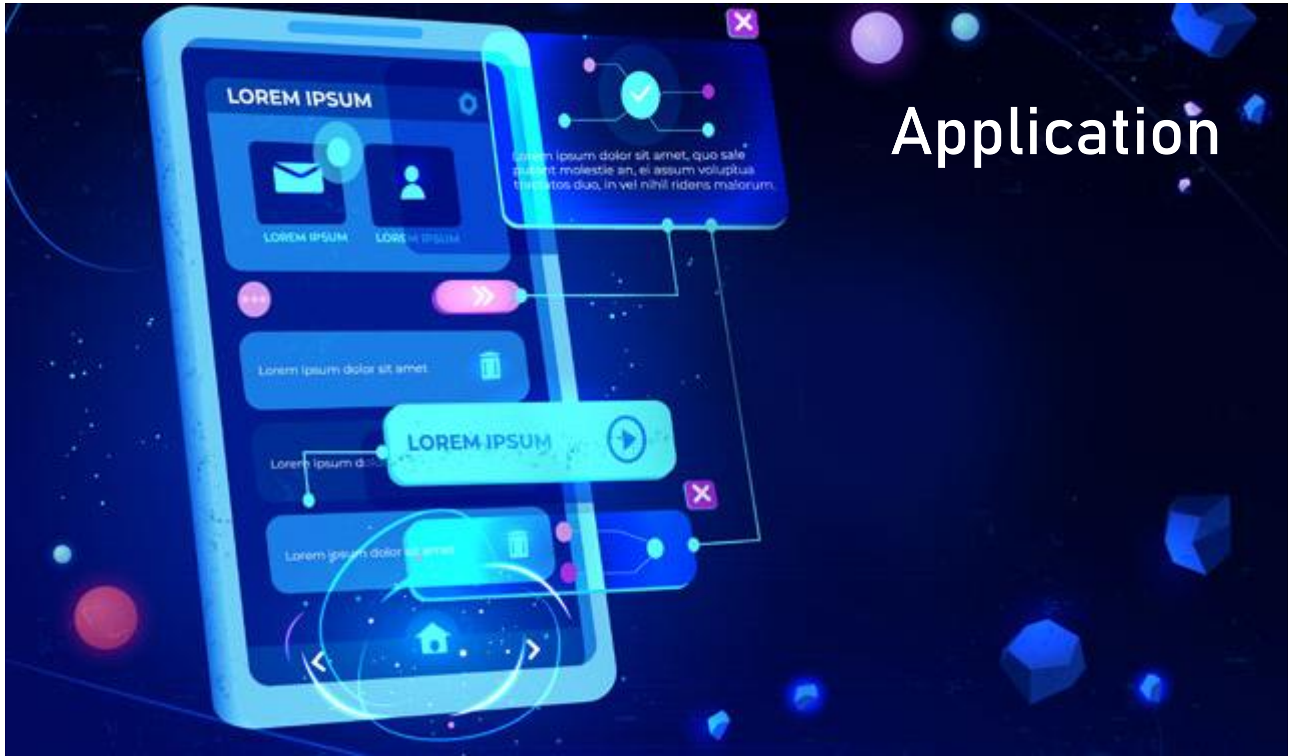
- **ONLY** senior management knows
- **NO** operation team realize

Why?



Employee

Network



Application

Physical Security

Tailgating

- Pretend janitor
- Pretend air conditioner technician

Anonymous USB

Leave a malicious USB

- Once plugged in, connect back to Red Team Server
- A very typical tactics by auditor

Employee

SANGFOR

Social Engineering

SANGFOR

Social Engineering

Shoulder Surfing

- Personal preference
- Company internal chat

Patch Vulnerabilities in Remote Acce
Remote Storage Now

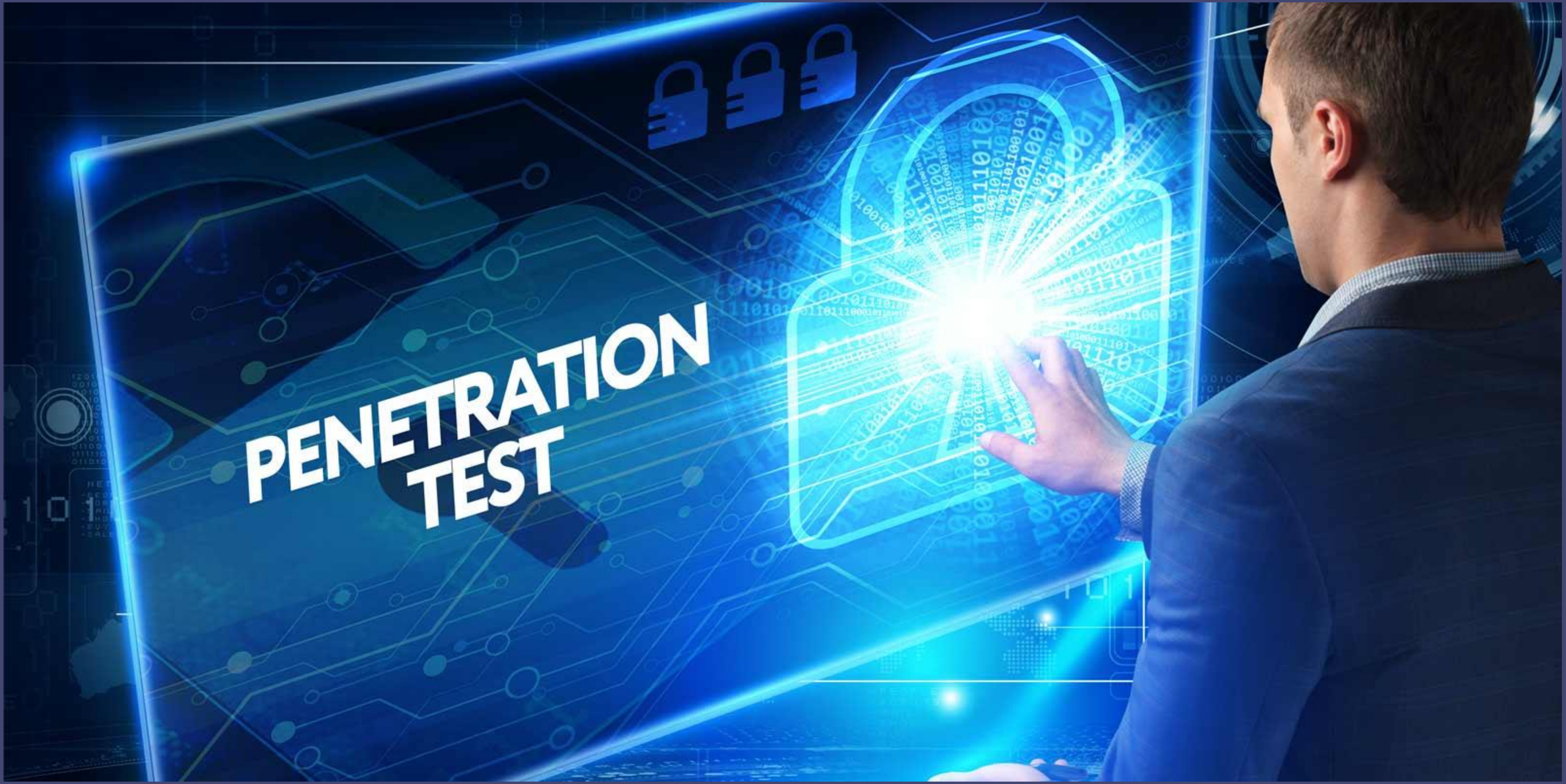
Release Date: 1 Sep 2021 | 8989 Views

HKCERT
Hong Kong Computer
Emergency Response Team
Coordination Centre
香港電腦保安事故協調中心

Network

Application

What Is The Difference?

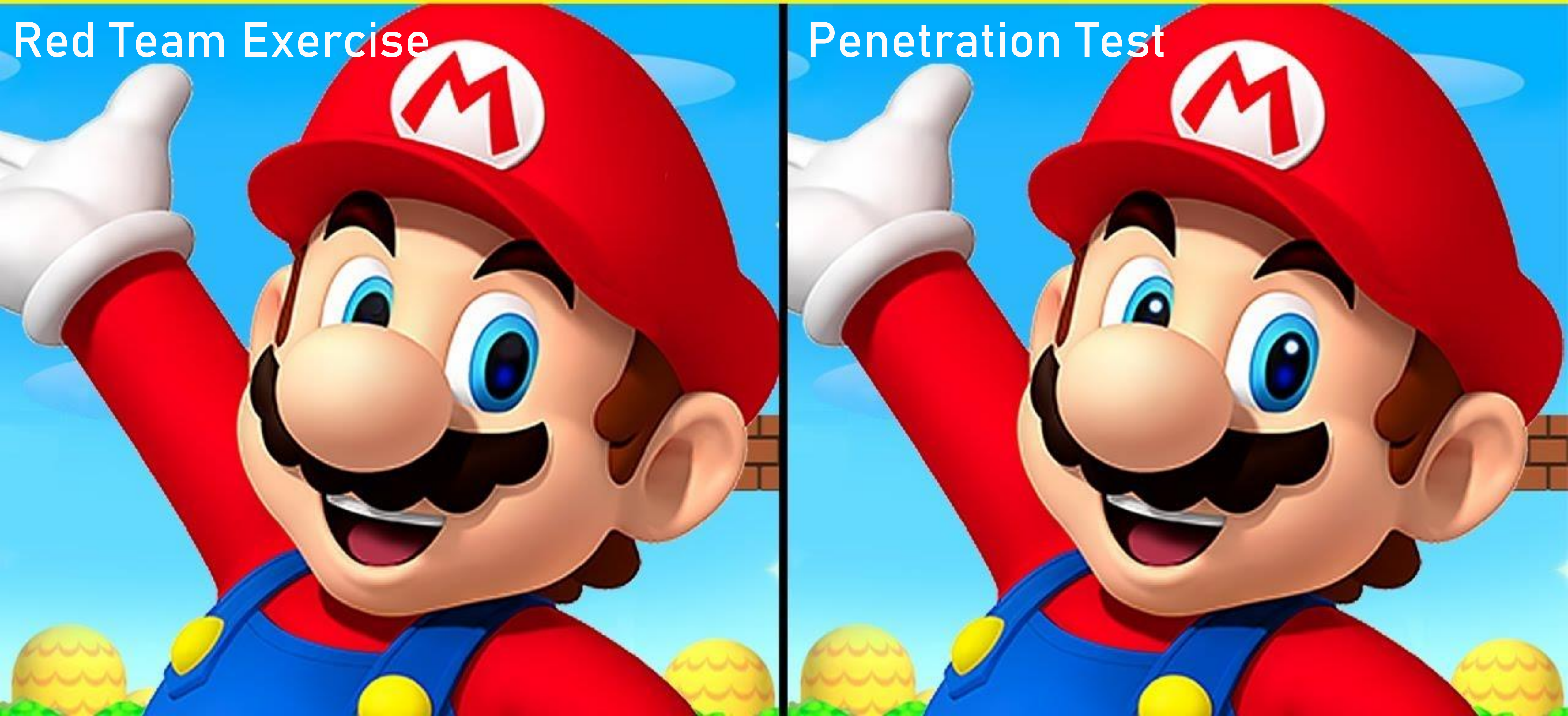


Similarity

Similar but not the same

Digging out known vulnerability

FIND THE DIFFERENCE

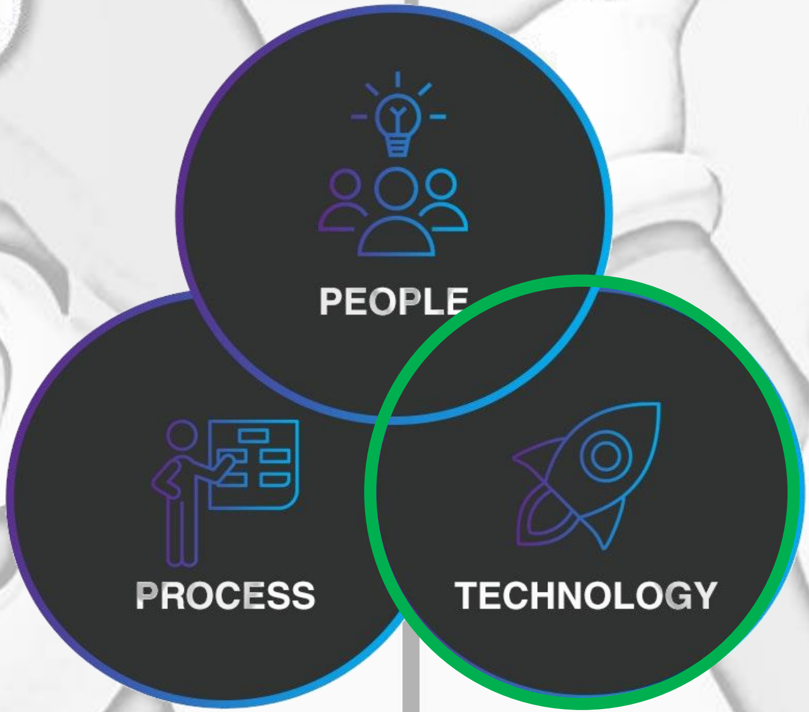


Red Team Exercise

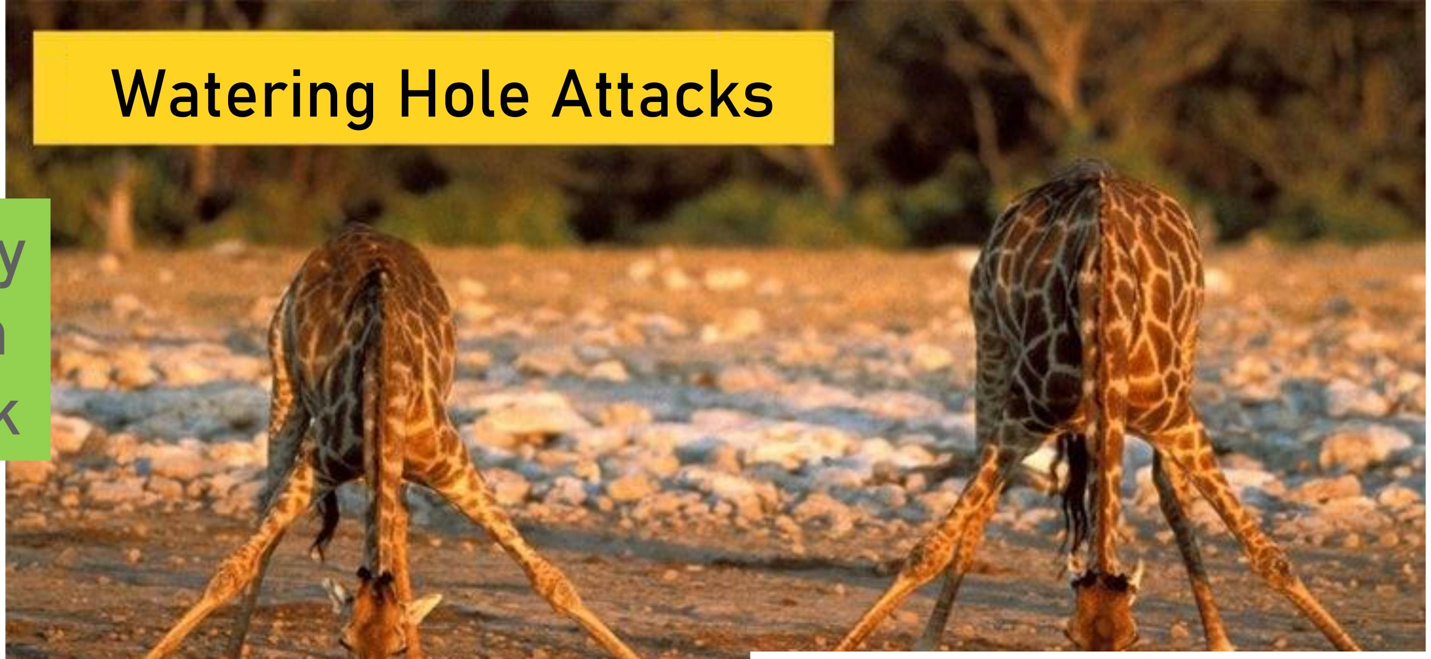
Penetration Test

FIND THE DIFFERENCE

Emergency Response Plan



Supply Chain Attack



Watering Hole Attacks

Vulnerability in Website Builder Exposes 700,000 sites

August 5, 2020 / in Security /

Red Team Exercise 5-Stages

1 Reconnaissance

2 Initial Access

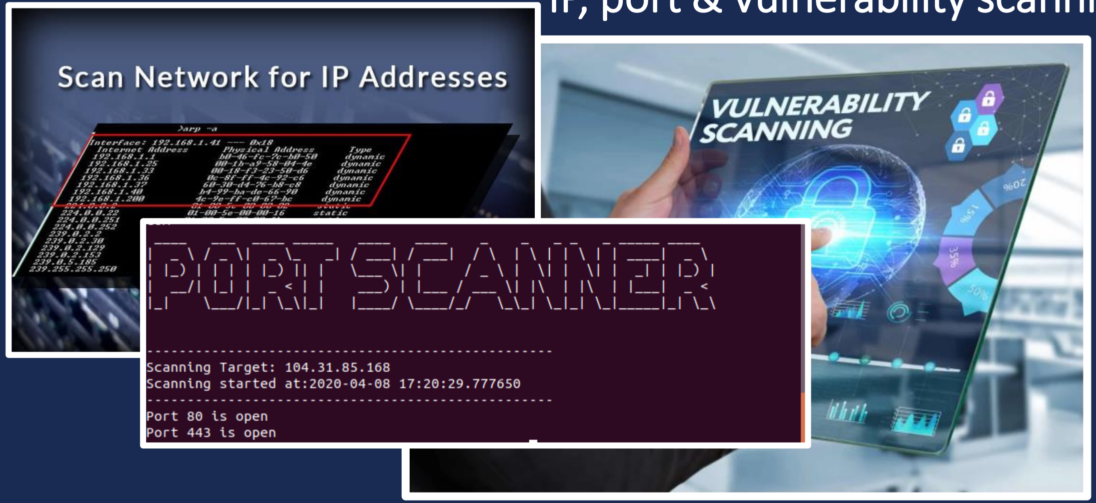
3 Lateral Movement

4 Exploit

5 Report

Reconnaissance

IP, port & vulnerability scanning



Scan Network for IP Addresses

```
>arp -a
Interface: 192.168.1.41 --- 0x18
  Internet Address      Physical Address      Type
  192.168.1.1           b0-46-fc-7c-b0-50     dynamic
  192.168.1.25          00-1b-a9-58-04-4e     dynamic
  192.168.1.33          00-18-f3-23-50-d6     dynamic
  192.168.1.36          0c-8f-ff-4c-92-c6     dynamic
  192.168.1.37          60-30-d4-76-b8-c8     dynamic
  192.168.1.40          b4-99-ba-de-66-90     dynamic
  192.168.1.200         4c-9e-ff-c0-67-bc     dynamic
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251
  224.0.0.252
  239.0.2.2
  239.0.2.30
  239.0.2.129
  239.0.2.153
  239.0.5.185
  239.255.255.250
```

```
PORT SCANNER

--------------------------------------------------
Scanning Target: 104.31.85.168
Scanning started at:2020-04-08 17:20:29.777650
--------------------------------------------------
Port 80 is open
Port 443 is open
```

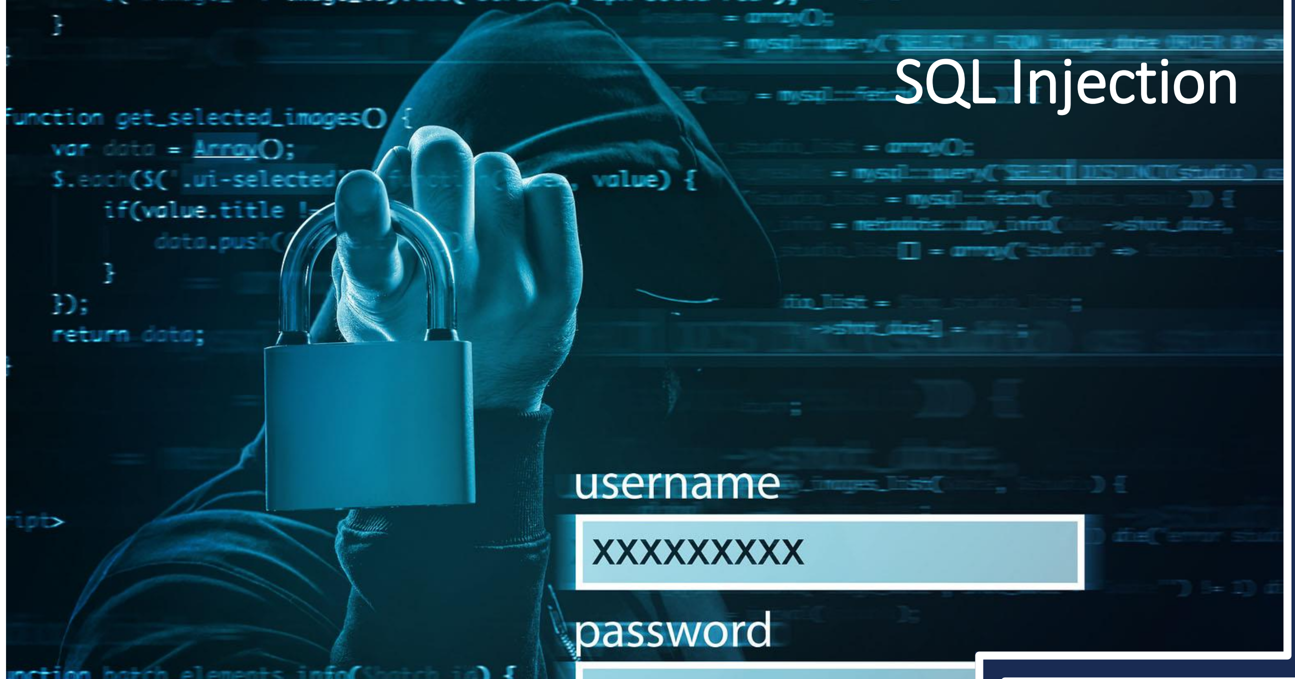
Mobile Apps Reverse Engineering

Sensitive Information

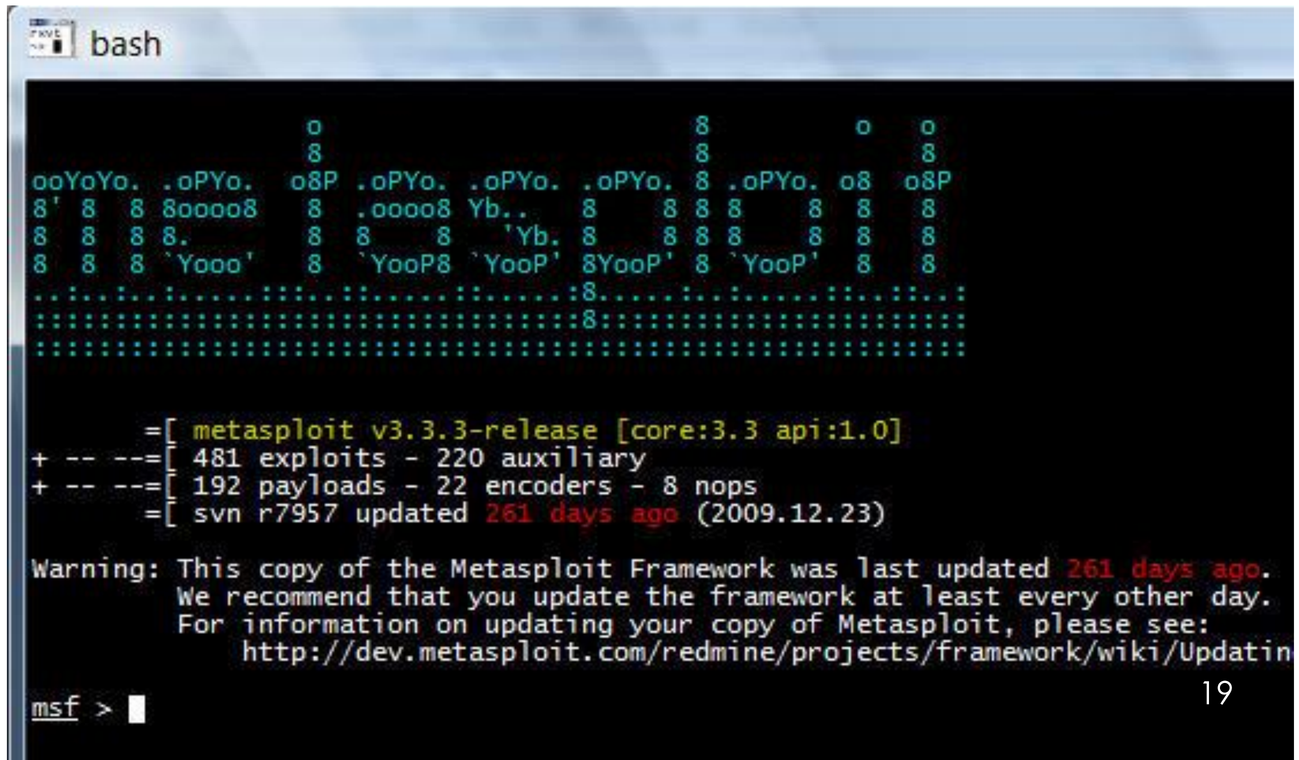
GitHub Repositories Leak Thousands of Secrets, Study Shows

Jessica Sirkin | 4/11/19

Share This!



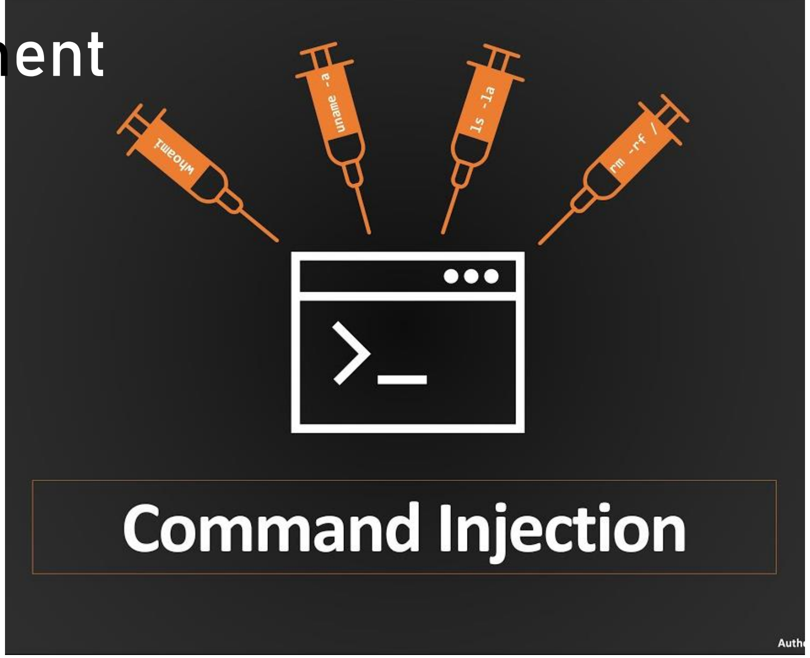
Initial Access



```
                o                       8         o   o
                8                       8             8
ooYoYo. .oPYo.  o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8  o8P
8' 8  8 8oooo8   8  .oooo8 Yb..   8    8 8 8    8  8   8
8  8  8 8.       8  8    8   'Yb. 8    8 8 8    8  8   8
8  8  8 `Yooo'   8  `YooP8 `YooP' 8YooP' 8 `YooP'  8   8
..:..:..:.....:::..:.....::.....::8.....:..:.....::..:::..:
::::::::::::::::::::::::::::::::::8:::::::::::::::::::::::::
::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::


       =[ metasploit v3.3.3-release [core:3.3 api:1.0]
+ -- --=[ 481 exploits - 220 auxiliary
+ -- --=[ 192 payloads - 22 encoders - 8 nops
       =[ svn r7957 updated 261 days ago (2009.12.23)

Warning: This copy of the Metasploit Framework was last updated 261 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             http://dev.metasploit.com/redmine/projects/framework/wiki/Updatin

msf > █
```

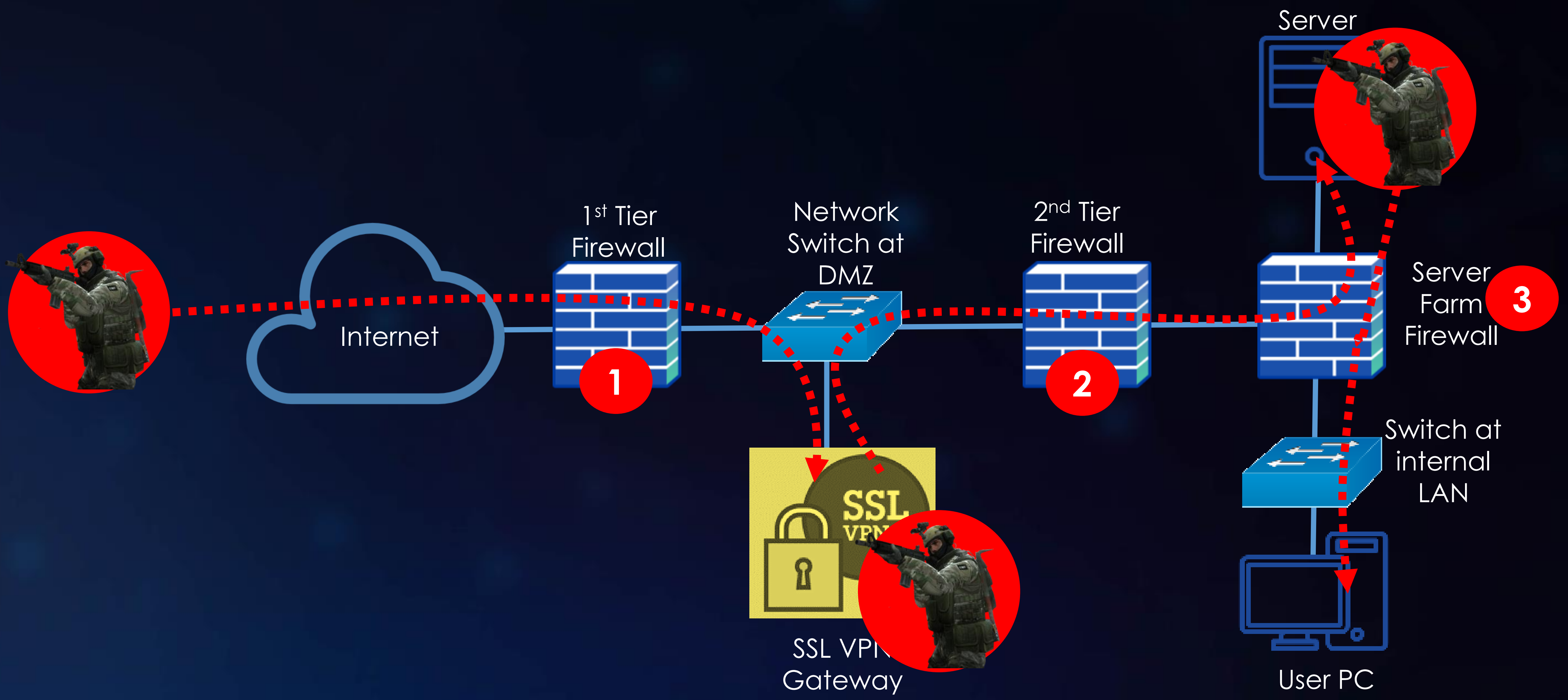
Lateral Movement & Exploit

SQL Injection



This is an
example!

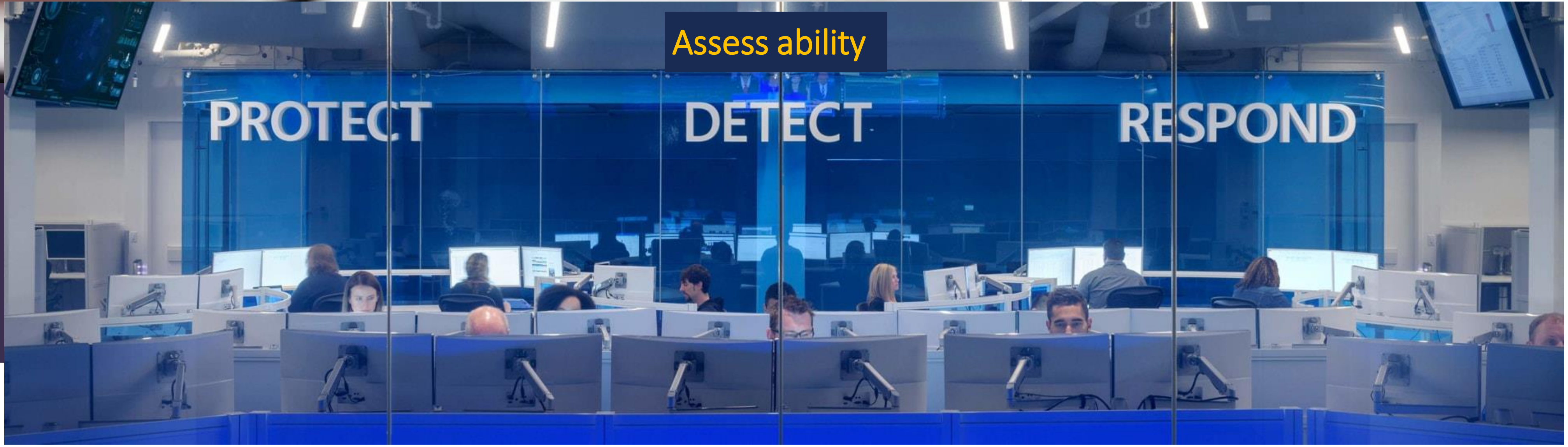
Red Team Example



Benefits of Red Team

Identifies the risk of key business information assets

Real attacks under a controlled manner.
No impact



Assess ability

地球嘅Cyber Security
就交俾你哋班後生啦!