RDP 분석 보고서

RED 담당자	정조희
BLUE 담당자	민지 백
진행 상태	완료
마감일	@2023년 8월 29일
최종 편집 일시	@2023년 8월 29일 오후 5:44
최종 편집자	정조희
프로젝트	시나리오 파트별 테스트

시나리오 개요도 7번

1. 취약점 개요

RDP(Remote Desktop Protocol)란 마이크로소프트사가 개발한 사유 프로토콜로, 다른 컴퓨터에 그래픽 사용자 인터페이스를 제공하는 프로토콜이다. 원격 접근 및 제어를 할 수 있도록 도와주는 프로토콜이며 디폴트 포트 설정은 3389으로, 공격자가 피해자 PC에 침투하기 위한 방법으로 사용하였다.

2. 테스트 환경

공격자 PC

OS	6.1.0-kali9-amd64
xfreerdp	2.10.0

피해자 PC

OS	Windows 10 Pro Version 1903 (OS Build 18362.356)
RDP Wrapper	1.6.2

3. 원격 침투 방안

3.1. Bluekeep(CVE-2019-0708) 취약점

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

해당 취약점은 Windows7 까지만 적용되고 Windows 10에서는 취약점이 패치 되었기 때문에 적용이 힘들어 본 시나리오에 사용할 수 없었다.

3.2. VNC

VNC는 원격 접속 프로그램으로 Server와 Viewer로 나뉘어진다. Server는 원격 대상 PC에 Viewer는 원격 접속을 시도할 PC에 설치하여 진행한다. 여러 오픈소스 VNC 프로그램 중 Ultra VNC를 사용하여 테스트해 보았다.

3.2.1. Windows - Windows

Windows 7에 Ultra VNC Viewer를 설치하고 Windows 10에 Ultra VNC Server를 설치해 테스트를 진행하였다.

VNC Server로 사용할 Windows 10에 Ultra VNC Setup.exe 파일을 다운로드 받은 후 cmd 창에서 아래의 명령어를 통해 조용히 설치를 진행한다.

```
UltraVNC_1431_X64_Setup.exe /VERYSILENT /NORESTART
// UltraVNC 자동 설치
```

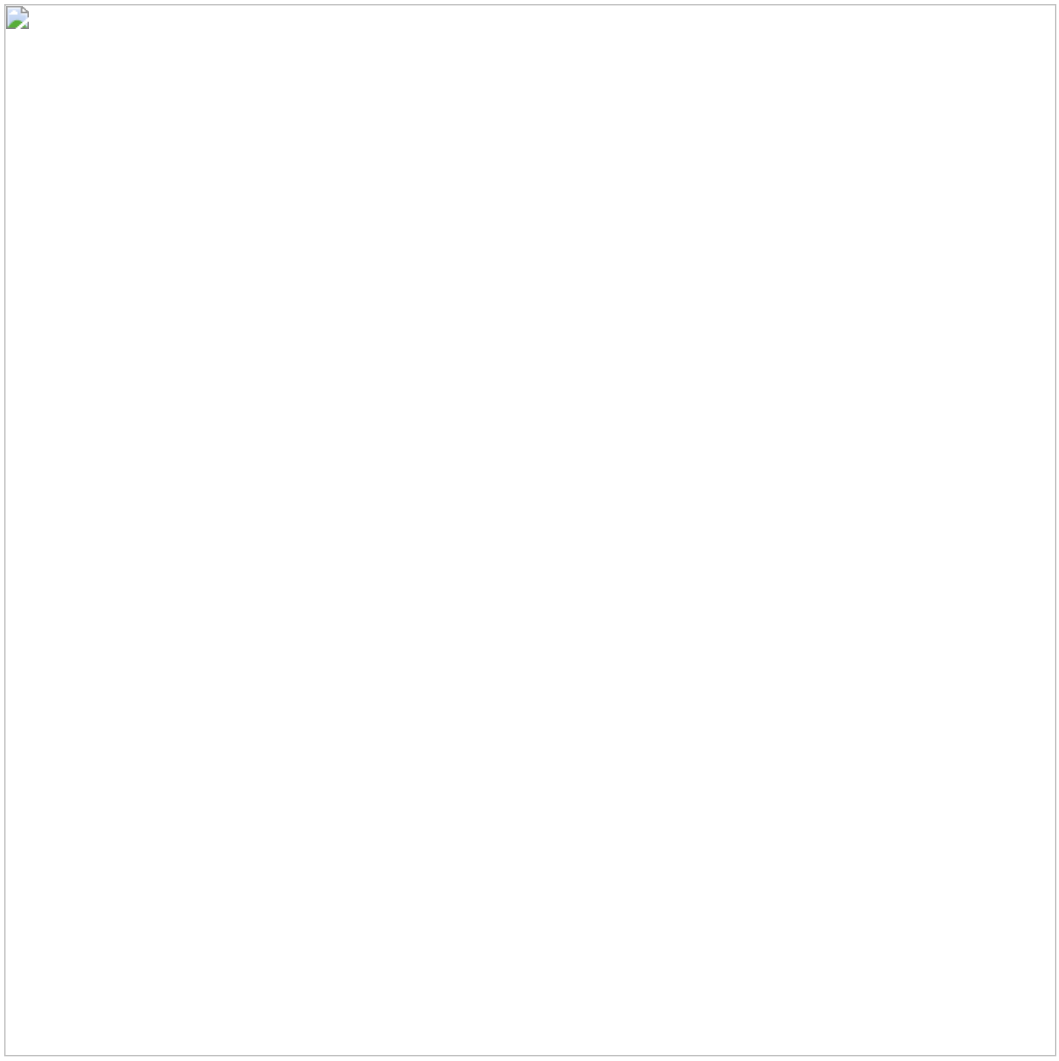
이후, Ultra VNC에 내장되어있는 password 설정 명령어를 사용해 원하는 비밀번호를 설정한 후 VNC를 실행한다.

```
setpasswd.exe [password]
// .ini 파일 password 설정 커맨드
// 관리자 권한 필요

winvnc
// vnc 실행
```

Windows 7에 Ultra VNC Viewer를 설치한 후, cmd에서 아래 명령어를 통해 Windows 10에 원격 접속을 할 수 있다.

```
vncviewer.exe -autoreconnect -connect [IP] -password [password]
```



원격 접속 확인

3.2.2. Kali - Windows

Kali의 Remmnia 플러그인을 이용해 Viewer로 사용하고 Windows 10에 Ultra VNC Server를 설치해 테스트를 진행하였다.

Windows 10에서 Ultra VNC Server를 실행하는 과정까지는 위 3.2.1.과 동일하다.

Kali에서 Remmina의 최신 버전을 아래의 명령어를 통해 설치한다. Remmina를 사용하면 GUI 환경으로 원격 접속을 시도할 수 있다.

```
sudo apt-get update
sudo apt-get -y install remmina
```

Kali에서 원격 접속 대상 PC로 접속하기 위해 Remmina를 실행한 후, 원격 접속 대상 PC의 IP와 설정한 비밀번호를 입력하고 연결을 시도한다.

원격 접속 확인

VNC 프로그램을 사용하면 간편하게 원격 접속 대상 PC에 연결할 수 있으나 VNC를 통해 원격 접속하면 상대방이 내 PC가 원격 접속 되고 있는 중임을 알아차릴 수 있다는 문제가 발생한다. 이 때문에 상대가 모르게 원격 접속할 방법을 더 찾아보기로 하였다.

3.3. RDP

일반적인 윈도우 환경에서는 한 대의 PC에 하나의 RDP 접속만 허용한다. 기존 사용자가 로컬에서 작업 중이거나 다른 사용자가 RDP를 이용해 현재 시스템에 접속하여 사용하고 있을 경우에는 기존 사용자의 인지 없이 RDP 연결이 불가하다. 따라서 Multi Session을 통한 RDP 연결할 방법이 필요하다.

3.3.1. Mimikatz

Mimikatz는 시스템 메모리에서 비밀번호나 자격 증명과 같은 민감한 정보를 추출하는 데 사용되는 도구이다. Mimikatz에는 여러 가지 기능이 내장되어 있는데 이 중 ts::multirdp 명령어를 사용하면 현재 실행 중인 Remote Desktop Service 즉 termsrv.dll을 로드한 svchost.exe에서 해당 DLL의 주소를 구한다. 이후, 특정 바이너리 패턴을 검색하고 정의된 패턴이 존재하면 이를 새로운 바이너리 패턴으로 패치하며, 패치 이후부터는 Multi RDP가 가능하게 해준다.

Mimikatz 설치 후 ts::multirdp 명령 절차를 따라서 시도해봤으나 Windows 7까지만 적용 가능하다는 문제가 있어, 테스트 환경이었던 Windows 10 환경에서는 Multi RDP 접속이 되지 않았다.

3.3.2. RDP Wrapper

RDP Wrapper는 Windows 버전 중 RDP가 지원되지 않는 버전에서 원격 접속을 가능하도록 지원해주는 오픈소스로, 이를 사용하면 RDP 원격 접속 및 Multi Session RDP 접속이 가능하다. 이는 Windows 10 버전에서도 지원 가능하며, Multi Session을 활용하여 원격 접속을 하면 사용자가 원격 제어가 되고 있다는 사실을 감지할 수 없다는 장점이 있어 RDP Wrapper를 사용하였다.

RDP 원격 접속을 사용할 시 사전에 레지스트리 수정이 필요하다. 원격 접속 세션 개수를 제한하는 정책과 원격 접속 사용자에게 1개의 세션만 할당하는 정책을 수정해야 한다. 해당 정책은 **관리자 권한**으로 cmd 실행 시 아래 명령어로 수정이 가능하다. 수정 후에는 정책 강제 업데이트 명령어를 입력하거나 재부팅을 해야 수정한 정책을 적용할 수 있다.

```
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v fSingleSessionPerUser /t REG_DWORD /d 0 /f
  // 1개의 세션만 사용하여 원격 접속하는 정책을 끄는 명령어

REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v MaxInstanceCount /t REG_DWORD /d 999999 /f
  // 멀티 세션 개수 제한을 해제하는 명령어 ( 999999 입력 시 제한 없음 / 개수 제한 두고 싶다면 원하는 숫자 입력 )

gpupdate /force
  // 정책 강제 업데이트
```

관리자 권한으로 cmd 실행 시, 해당 명령어를 통해 원격 접속 정책을 변경할 수 있다.

테스트 환경에서 사용한 Windows Pro 10 1903 버전에서는 RDP Wrapper가 제대로 동작하지 않는 문제가 있다. 작동 여부 확인은 RDP Wrapper 폴더의 RDP Wrapper Configuration 실행파일을 통해 확인할 수 있다.

해당 에러는 RDP Wrapper의 .ini 파일을 수정하는 방법으로 해결할 수 있다. 아래 링크에 있는 배치 파일을 이용하면 더 쉽게 에러를 해결 가능하다.

rdpwrap_ini_updater: support for 10.0.18362.267, 10.0.18362.53, 10.0.18362.1, 10.0.17134.706 ... · Issue #795 · stascorp/rdpwrap

Hi, the batch file rdpwrap_ini_updater add support to rdpwrap.ini for the following new termsrv.dll versions: 10.0.18362.267 10.0.18362.53 (Build 18362.239, 18362.207, 18362.175, 18362.145, 18362.1...

https://github.com/stascorp/rdpwrap/issues/795

RDP Wrapper 설치와 1903 버전 에러 해결 방법은 아래 명령어를 따른다. cmd 실행 시 **관리자 권한**이 필요하다.

```
-------- 관리자 권한 필요 ---------

c:\users\pm\downloads\rdpwrapper\install.bat

c:\users\pm\downloads\rdpwrapper\update.bat

copy "c:\users\pm\downloads\rdpwrapper\*" "c:\program files\rdp wrapper"

"c:\program files\rdp wrapper\re-install.bat"

"c:\program files\rdp wrapper\rdpwrap_ini_updater.bat"
```

RDP Wrapper를 설치하고 나면 Multi Session을 활용한 RDP 원격 접속이 가능하다.

remmina에서 원격 접속 대상 pc ip, id, pw 입력 후 접속하여 Multi Session 접속 확인

4. 대응 방안

4.1. 로컬 계정 정보 변경

사용하는 계정 이름을 변경하거나 비활성화하여 공격자로부터 계정 접근을 제한해야 한다. 또한, 비밀번호 정책은 공격자가 유추하기 어려운 특수문자, 대/소문자, 숫자 조합으로 10자리 이상을 권고한다.

4.2. 원격 데스크톱 접근 보안 강화

공격자는 원격 데스크톱 프로토콜을 이용하여 피해 시스템에 접근할 수 있다. 공격자가 원격으로 서버에 접근할 경우 일반 사용자처럼 작업을 수행할 수 있다. 따라서 인가된 사용자만 접근이 가능하도록 화이트리스트 정책을 권고한다. 또한 원격 데스크톱 접근 시 다중 인증 방식(MFA)를 통해 서버 접속에 제한을 두거나 기능을 비활성화 하는 것을 권고한다.

4.3. 사용하지 않는 포트 비활성화

SSH(22), TELNET(23), 원격 데스크톱(3389) 등 사용하지 않는 서비스들이 외부에서 접근 가능할 경우 초기 공격 대상이 될 수 있으며, 이미 공격자가 서버에 침투하였을 경우에는 내부 확산으로 이어질 가능성이 매우 높다. 때문에, 사용하지 않는 서비스와 관련된 포트는 비활성화 및 제거하는 것을 권고한다.

5. RDP 선정 이유

RDP는 Windows 10 Pro에 자체적으로 내장되어 있는 기능이기 때문에 별도의 설치나 설정이 필요하지 않다. 또한 GUI 환경으로 사용이 가능하기 때문에 편의성이 보장된다. VNC를 통해 원격 접속을 하면 하나의 세션으로만 접속이 가능하지만, RDP를 사용하면 Mimikatz, RDP Wrapper 등의 도구를 통해 Multi Session으로 원격 접속이 가능하다. 공격 도중 공격 대상이 자신의 PC에 이상이 있음을 알아차리게 되면 공격자가 최종 공격 목표에 도달하기 힘들 확률이 높아지기 때문에 피해자의 인식 없이 해당 PC에 접속하는 것이 중요하다. 따라서, Multi Session을 지원하는 RDP를 사용하여 원격 침투를 진행하였다.