

데프콘 미리보기 1일차

Attack Basics

<https://tlk.io/hspace1357>

Who am I

- 문형일 (mhibio)
- Defcon 2021 - pbXsg
- Defcon 2023/2024 - Hypeboy
- Handles
 - @mhibio
 - @mhibio_ptw

2024	Defcon 32 CTF (Team.Hypeboy)
2023	Defcon 31 CTF (Team.Hypeboy)
2023	Pwn2Own Toronto (Team.STEALIEN)
2022	코드게이트 대학생부 2등 (Team.해군해난구조전대)
2020	Seccon 1등 (한글사랑)
2021	Whitehat Contest 2등
2020	Whitehat 콘테스트 3등

뭘 배우나요 ?

- 1일차 / 2일차

- [GDB / IDA / MCP / AI] Basics
- 취약점 탐색 Basics
- Exploit Basics
- 취약점 탐색 Advanced
- Exploit Advanced
- 2023/2024 데프콘 문제 연습해보기
- Packet Reply

- 3일차 / 4일차

- 야라 룰로 backdoor 탐지.
- IDA MCP 연결 후 분석해서 backdoor + 취약점 탐지.
- 바이너리 패치 + diffing.
- backdoor planting
- wireshark: packet 분석 후 exploit root cause 탐지.
- pcap 읽고 exploit payload 있는 packet 잡기 + replay
- wireshark 1-day를 통해서 DoS 유발

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

Defcon

- 2박 3일에 걸친 CTF.
- 점수 분야는 **Attack / Defence / King of the hill / LiveCTF**
- 4가지 점수를 모두합쳐서 최종 스코어링
- 패치내용 (**패치된 인스턴스**), 공격내용 (**Exploit Packet**) 을 제공해줌.
 - 다른팀이 우리 Patch를 가져다 쓸 수도, => 백도어
 - 우리팀이 다른팀 **Exploit Code**를 가져다 쓸 수도 있음. => **Packet Reply**

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

Defcon

- 대회시간 : 현지시간 **10시 ~ 17시**
 - 10시 ~ 17시는 실시간 이슈를 핸들링하는것이 중요.
 - **Packet Reply**
 - 취약점 패치 등
 - 매 **Tick**마다 **Exploit**전송
 - 새벽 : 바이너리 분석하고, 새로운 **Exploit**을 개발하고, 대회시작하면 전송할 준비하기.

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

점수 집계

- **1tick : 5분, 3tick 15분.** 모든 점수 측정은 1틱마다
- **공격**
 - 다른 팀에 **Exploit**을 성공해서 **Flag**를 가져오면 점수 제공 **+1**
 - **5분동안 12팀중에 7팀의 플래그를 가져오면 +7 점**
- **방어**
 - 이번 **Tick**에 플래그가 유출되지 않으면 **+1**
 - **5분동안 우리 인스턴스를 대상으로 12팀중에 5팀이 플래그를 가져갔으면 $12-5 = 7$ 점**
- **King of the hill**
 - 알고리즘, 스피드, 창의력을 포괄한 **Challenge**를 풀이.
 - **EX)** 작년에는 **AI Prompting**을 활용하여 배틀쉽을 조종하는 게임을 진행.
- **LiveCTF**
 - 팀 대표가 특정분야의 문제를 1대1로 겨뤄 빨리 푸는 사람이 살아남는 토너먼트 (점수 차등 지급, 점수 엄청 큼)

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

역할 배분

• 공격

- 취약점 분석, **Exploit** 제작
- 공격 자동 스크립트 : 1틱마다 자동으로 **Exploit**을 전송하고, **flag**를 가져와서 인증하는 서비스

• 패치

- 식별된 취약점에 따라 패치, 분석방해 : 와이어샤크 **DOS** (우리팀 패킷 뜯으면 **Hang**)
- 백도어 : 누가 우리팀 패치가 유용해 보여서 가져가서 적용하면? : **Exploit** 하지 않아도 자동으로 **flag** 획득

• 패킷

- 유의미한 패킷 (**^flag\{[A-Za-z0-9_-]+\}**\$) 를 가져간 공격 패킷 식별
- 해당 패킷을 **Reply** (필요에 따라 가공)

• **KOTH / SpeedRun** = 논외

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

역할 배분

1/2 일차

3/4 일차

• 공격

- 취약점 분석, Exploit 제작
- 공격 자동 스크립트 : 1틱마다 자동으로 Exploit을 전송하고, flag를 가져와서 인증하는 서비스

• 패치

- 식별된 취약점에 따라 패치, 분석방해 : 와이어샤크 DOS (우리팀 패킷 뜯으면 Hang)
- 백도어 : 누가 우리팀 패치가 유용해 보여서 가져가서 적용하면? : Exploit 하지 않아도 자동으로 flag 획득

• 패킷

- 유의미한 패킷 (`^flag\{[A-Za-z0-9_-]+\}$`) 를 가져간 공격 패킷 식별
- 해당 패킷을 Reply (필요에 따라 가공)

- KOTH / SpeedRun = 논외

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

Rule

- 기존 규칙
 - 바이너리는 시간순서대로 **Open**.
 - 일정시간 지나면 바이너리 **Retire** 발생. (더이상 **Exploit** 불가).
 - **Patch**정보 및 **Packet**정보는 3틱(15분)마다 공개
 - 즉, **Packet Reply**같은 경우 3틱 다음부터 가능
 - 엄청난 **Exploit**을 제작 하였다 하더라도, 3틱 뒤에서부터는 누군가가 **Reply**할 가능성 존재.
 - 예전에는 이를 방지하기 위해서 **Stealth Port** (패킷 공개 **X**) 제공했었지만 현재는 **X**

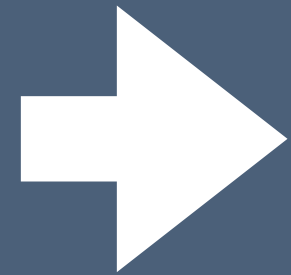
데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

대회시작전에 알아야할 정보 들

- 2박 3일에 걸친 해킹 대회
- 대회시작 2,3일전에 “**Rule book**” 제공
 - 꼭 읽어봐야할 정보들이 많음.
 - 패치 배포 어떻게 진행되는지, 인스턴스 관리는 어떻게 되는 지, 스텔스 포트 등등
 - 특히 **패치 배포에 따라 여러 전략이 생기기** 때문에.
 - EX) 도커 이미지를 통으로 우리가 올릴 수 있으면 커널레벨, 라이브러리 같은곳에 백도어 심기도 쉬워짐.
 - EX) 바이너리 패치만 제공되면 매우어려워짐
- 팀 12~16개
 - 각 팀은 내부망 IP 할당 받음 (보통 순위대로)

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

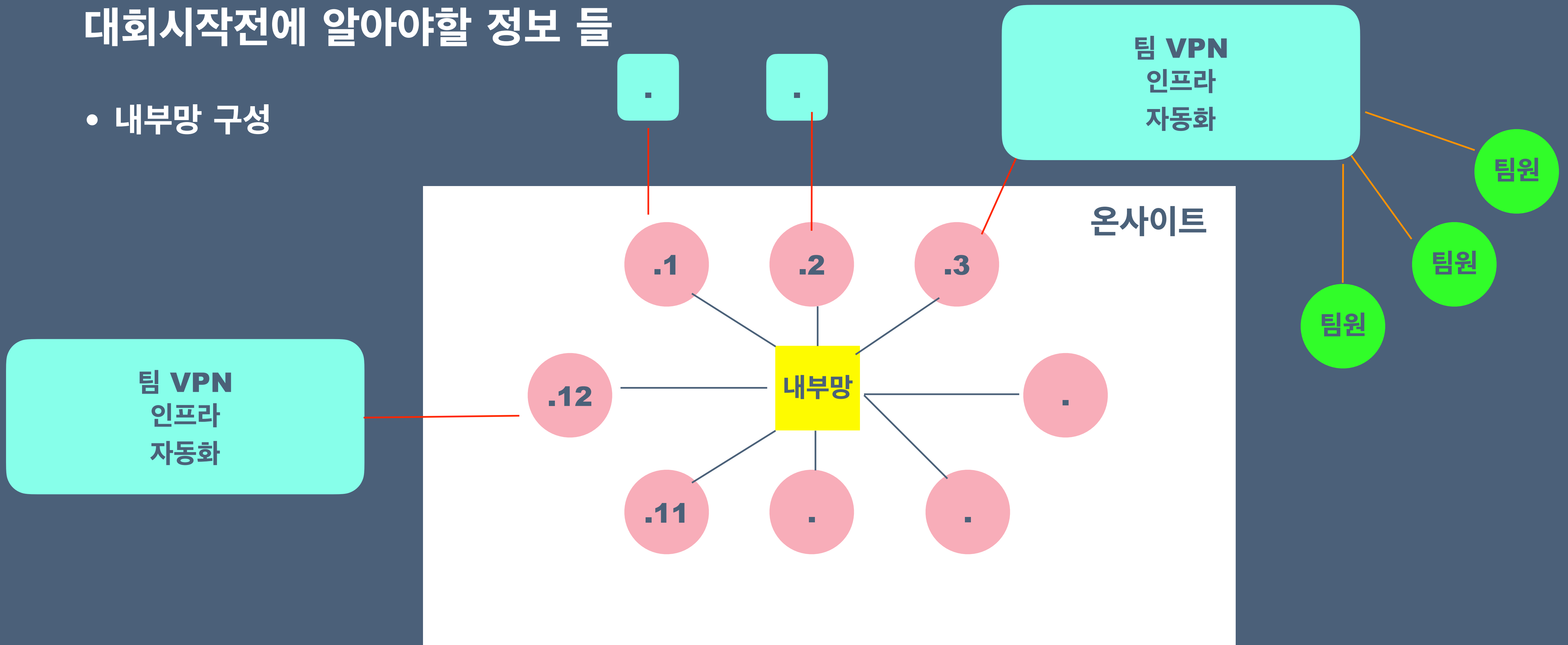
일반적인 준비전략 - 팀단위 준비해야할것

- **Auto Exploit Sender** : 기존에 작성한 **Exploit**을 5분마다 자동으로 전송 / 인증 해주는 인프라
 - **Packet 분석기** : 제공받은 **pcap**을 자동으로 분석, **Suspicious** 한 패킷들 별도 분리해서 팀원이 확인
 - **Patch 전략 준비**
 - 바이너리 패치
 - 시스템 패치
 - **Mitigation** 적용
 - **백도어 준비**
 - 바이너리 백도어
 - 시스템 백도어
- 
- 보통 팀단위에서 개발 후 팀원들에게 배포

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

대회시작전에 알아야할 정보 들

- 내부망 구성



데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

일반적인 준비전략 - 개인이 준비해야할것

- **Wireshark**
- **GDB**
- **IDA**
- **Python** 잘다루기
- **Exploit** 개발 경험
- 취약점 탐지 경험

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

요약

- 제공되는 룰북은 꼭 읽어보자
- 새로운 **Exploit** 코드를 발견하면 바로 날릴 수 있을정도로 빠르고 유연하게

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

대회당일 우리들의 전략.

- 현황

- **Exploit**경험이 적다보니 실전에서 엄청난 크기의 바이너리를 상대로 취약점 발굴 및 **Exploit**하는것에 어려움이 있을것.
- 적절한 기술에 인적자원이 필요한 곳에 지원을 하는 것이 좋아보임.
- 적절한 기술 = 바이너리 분석
- 인적자원이 필요 = 패킷 분석 및 **Exploit** 증명

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

대회당일 우리들의 전략.

- 패킷 분석 그거 그럼 자동화가 다 해주는거 아니가요 ?
 - 아래는 거의 모든팀이 사용하는 전략들.
- **Fake Flag**를 고의로 패킷에 심는 경우.
- **Flag**를 암호화 하여 빼오는 경우.
- => 단순 **flag regex** 로 빼오기가 어려움
- => **Suscpicious** 한 패킷 분류 & 무슨 작업하는지, 어디를 공격하려고 시도한건지 분석

데프콘이 뭔가요 - 대회시작전에 알아야할 정보들

대회당일 우리들의 전략.

- 하나 혹은 두세개의 문제들에 대해서 (하루에 하나씩 이해하면 좋음!) 바이너리에 대한 이해를 수행하고,
- 대회 러닝 타임
 - 패킷 분석팀에서 전달받은 / 혹은 우리가 추출한 패킷으로부터 해당 패킷이 **Exploit**에 성공한 패킷인지 아닌지 구분. (자동화 되어있을 가능성 높음)
 - 자동화 인프라에서 잡지 못하는 (flag는 추출되지 않았지만, sus한 행위를 수행하는 code)
 - 우리 인프라에서 작동하는 **Exploit** 으로 포팅.
 - 취약점을 빠르게 분석해서 패치팀에게 전달.
- 대회 퍼즈 타임
 - 바이너리를 분석하여 취약점을 찾거나 & **Exploit** 제작
 - 기존의 취약점을 이해하거나
 - 패치 포인트를 찾거나.
 - 밤샘 효율이 좋지 않을것으로 보이기 때문에 체력관리 추천. (단 바이너리 이해정도까지는 노력해보죠 !)

본격강의시작 - Attack Basics

GDB, IDA, MCP, AI

본격강의시작 - Attack Basics

취약점 찾기 & Exploit 개발

본격강의시작 - Attack Basics

2024 데프콘 톨아보기 1