

# 2016 Christmas CTF

NMS WriteUP  
team.노드잡익스충  
Nick : Sori

타겟은 어느 도시에 위치한 데이터센터.  
네트워크 담당자 PC에 침투한 해커는 패킷을 획득하였고,  
취약한 설정을 가진 서버를 찾게 되는데...

패킷을 분석하고 취약한 서버를 찾아 키를 획득하라

<https://drive.google.com/open?id=0B74xFxspdAi-dGxObEV4NldvM1U>

데이터 센터에 해커가 침투했다는 시나리오.  
일단 주어진 패킷파일을 Wireshark로 열어보자.

2340	156.8423...	192.168.32.157	174.100.25.20	TCP
2341	156.8445...	192.168.32.157	10.253.41.121	SNMP
2342	156.9020...	192.168.32.157	174.100.25.19	TCP

SNMP라는 수상한 프로토콜을 찾을 수 있었다.

프로토콜을 SNMP로 필터링하여 찾아보자.

2763	190.6782...	52.175.155.146	192.168.32.157	SNMP	78	get-response	1.3.6.1.2
2764	190.6785...	192.168.32.157	52.175.155.146	SNMP	97	get-request	1.3.6.1.2 1.3.6.1.2
2765	190.7241...	52.175.155.146	192.168.32.157	SNMP	97	get-response	1.3.6.1.2 1.3.6.1.2
2766	191.6435...	192.168.32.157	174.100.25.5	SNMP	97	get-request	1.3.6.1.2 1.3.6.1.2

패킷을 분석하니 52.175.155.146이 서버라는 것을 알 수 있었고 무언가를 계속 요청하고 받는 것을 확인할 수 있었다.

여기서 내용을 보자.

```
.PV.'...).^U..E.
.S..@... ..
)5.T...? ..05....
.idcmoni toradmin
.....0.0..
.+.....0 ...+....
```

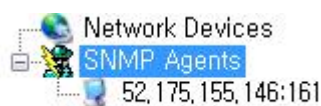
idcmonitor admin이라는 문자열을 확인 할 수 있었다.

우선 SNMP부터 알아보자

간이 망 관리 프로토콜(Simple Network Management Protocol, **SNMP**)은 IP 네트워크상의 장치로부터 정보를 수집 및 관리하며, 또한 정보를 수정하여 장치의 동작을 변경하는 데에 사용되는 인터넷 표준 프로토콜이다.

그렇다고 한다. 따라서, SNMP 접속기를 찾아보자.

**PowerSNMP Free Manager**



띠요요오오옹~ SNMP가 있다!

Agent Configuration

Address: 52.175.155.146 Port: 161 Version: ☒ 1 ☐ 2 ☐ 3

Community: idcmonitoradmin

User Authentication and Privacy (v3)

Name:

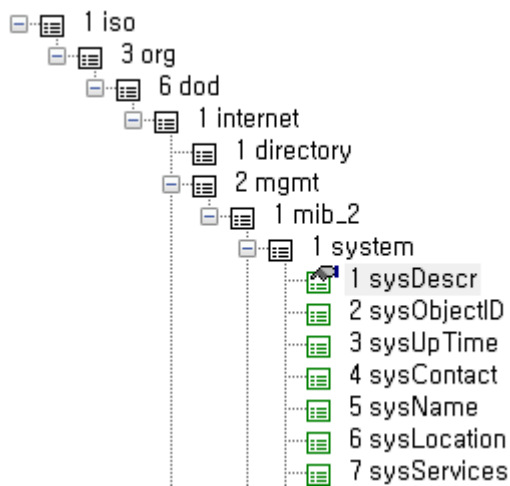
Auth Password:  Auth Protocol: None

Priv Password:  Priv Protocol: None

NOTE: SHA and TripleDes are compliant with FIPS-140 standards.

OK Cancel

이렇게 Agent를 추가해 주고



아까의 13612를 맞추어 쿼리를 보내주면 플래그가 출력되게 된다.

후기. CTF때 풀어놓고 1,2위 모두 NMS풀이가 없기에 써 보았습니다. 데헛★