**ARP 스푸핑**

|  |  |
| --- | --- |
| 과 목 | 시스템보안 |
| 담 당 교 수 | 송유진 |
| 조 원 | 김진우, 김태환 |
| 제출일자 | 2018년 10월 31일 |

1. 스푸핑이란?

* 스푸핑의 사전적인 의미는 '속이다'이다.
* 스푸핑은 MAC 주소, IP 주소, 포트 등 네트워크와 관련된 모든 것과 관련이 있다.
* 스푸핑은 속임을 이용한 모든 공격을 칭한다.

1. ARP 스푸핑이란?

* LAN에서 ARP 메시지를 이용하여 상대방의 데이터 패킷을 중간에서 가로채는 중간자 공격기법이다.

1. ARP 동작 과정
2. 송신자는 ARP Table에서 수신자의 MAC 주소를 확인한다.
3. 수신자 MAC 주소에 대한 정보가 존재하지 않는다면 송신자의 IP 주소를 포함한 ARP Request 메시지를 생성하여 네트워크 상에 Broadcasting한다.
4. 수신자는 Broadcasting 된 메시지에서 IP 주소 일치를 확인하고 ARP Reply 메시지를 생성하여 송신자에게 전송한다.
5. 송신자는 ARP Reply 패킷을 받고 목적지 ip 주소와 물리주소를 ARP table에 기록한다.
6. 테이블에 기록 이후부터 이러한 과정 없이 테이블을 참조하여 바로 데이터를 전달한다.
7. ARP의 취약점

* ARP 동작과정에서 Reply 패킷으로 받은 MAC 주소가 진짜인지 아닌지 검증하는 시스템이 없다.

1. ARP 스푸핑 동작 과정
2. 공격자가 victim에게 gateway의 ip 주소와 공격자의 MAC 주소가 담긴 패킷을 지속적으로 전송한다.
3. victim은 ARP table에 gateway의 ip 주소와 공격자의 MAC 주소를 저장한다.
4. victim은 공격자를 gateway로 생각하여 공격자의 mac 주소로 데이터를 전송한다.
5. (추가사항) 공격자는 victim에게 받은 데이터를 포워딩해준다.
6. ARP 스푸핑에 대한 대응책
7. ARP 테이블이 변경되지 않도록 arp -s [IP 주소] [MAC 주소] 명령으로 MAC 주소 값을 고정시킨다.
8. 네트워크 장비에 서로 다른 ip에 동일한 MAC 주소가 매핑되어있는지 확인
9. 패킷 감지 프로그램을 사용하여 ARP 신호를 보내는 패킷 확인
10. ARP 스푸핑인 ARP 프로토콜 자체의 문제로 근본적인 대책은 없음.
11. ARP 스푸핑 툴
    1. TCP dump

* 주어진 조건식을 만족하는 패킷들의 헤더를 출력해주는 프로그램
* 명령어 형식 : tcpdump [options] [expression] [host]
  1. Fake
* 명령어 형식 : send\_arp [T1 IP] [공격자 MAC] [T2 IP] [T2 MAC]
* T2의 MAC Table에 T1의 IP에 대응하는 MAC 주소를 공격자 MAC 주소라고 알린다.
* ARP는 일정 시간마다 갱신되기 때문에 지속적으로 사용해야함.
  1. Fragrouter
* 스푸핑 과정에 있어서 받은 패킷을 릴레이 해주기 위한 툴이다.
* 명령어 형식 : fragrouter -B1
* B1 옵션은 Nomal IP Forwarding을 의미한다.

8. 출처

* https://ko.wikipedia.org/wiki/%EC%8A%A4%ED%91%B8%ED%95%91
* <https://ko.wikipedia.org/wiki/ARP_%EC%8A%A4%ED%91%B8%ED%95%91>
* https://m.blog.naver.com/PostView.nhn?blogId=ryuroy&logNo=130153765154&proxyReferer=https%3A%2F%2Fwww.google.co.kr%2F
* http://blog.plura.io/?p=7247
* <http://www.loelab.com/tcpdump-%EC%82%AC%EC%9A%A9%EB%B2%95/>
* http://tisiphone.tistory.com/270