준비물

1. **윈도우 유저**
    A. 은신술 도구
        i. 토르 설치
            1. https://www.torproject.org/download/download-easy.html.en
        ii. Browsec 크롬 확장 설치
            A. https://chrome.google.com/webstore/detail/browsec-vpn-free-and-unli/omghfjlpggmjjaagoclmmobgdodcjboh?hl=en
    B. 분신술 도구
        i. TMAC 다운로드
            1. https://technitium.com/download/tmac/TMACv6.0.7_Setup.zip
2. **MAC 유저**
    A. 은신술 도구
        i. kronymous 크롬 확장 설치
            1. https://chrome.google.com/webstore/detail/kronymous-access-internet/dfdhngcahhplaibahkkjhdklhihbaikl?utm_source=chrome-app-launcher-info-dialog
        ii. Proxy SwitchyOmega 크롬 확장 설치
            1. https://chrome.google.com/webstore/detail/proxy-switchyomega/padekgcemlokbadohgkifijomclgjgif
    B. 분신술 도구
        i. macchanger 설치
            1. https://github.com/shilch/macchanger#installation

진행

은신술

1. IP 가 그대로 보여진다는 것 인지시키기
    A. 하지만 무턱대고 IP 를 아무거나 바꿔버리면 TCP 3 way handshake 자체가 성립 안됨
    B. HTTP 연결은 TCP 위에서 이루어지니 당연히 HTTP 연결도 안 됨
    C. 왜냐면 보낼 수는 있지만 서버가 답장을 못해주기 때문.
        i. 사실 이 방식으로 서버가 다른 사람에게 패킷을 보내게 할 수도 있음(보통 DoS 에 사용)
    D. **[실습]** ghostogether.club 접속하게 해서 사람들의 IP 주소가 그대로 보여지는 것 보여주기
        i. tcpdump 명령어와 lnav 명령어로
2. IP 를 숨겨보자
    A. 일반 IP 프록시 (Google 검색 - Proxy List)
        i. 근데 Proxy list 에서 나온 IP 로 프록시 타보니까 IP 변장이 안되더라.
        ii. 그럼 이건 그냥 넘어가고
    B. Socks 프록시 (토르 서킷)
        i. [방법 1] 토르 패키지를 설치하고 Tor.exe 를 실행한 후 9050 포트로 프록시 타기 지정하는 방법이 있고
        ii. [방법 2] Kronymous 확장과 OmegaSwitch 확장의 조합으로 9999 포트로 프록시 타는 방법이 있고
            1. 프록시 타는 건 시스템 설정해서 해도 되고 OmegaSwitch 에서 해도 됨.

iii. 윈도우에서는 [방법1], [방법2] 둘 다 해도 되고 Unix-like 에서는 [방법 1] 이 firefox 에서는 잘 되고 chrome 에서는 약간 불안정하네. Unix-like 는 그냥 [방법 2] 로 해야 할 것 같다.

iv. 세팅 다 한 후에 ghostogether.club 접속하게 해서 IP 바뀌는 것 보여주고

C. VPN (Browsec)

i. Browsec 확장 설치한 후 ghostogether.club 접속하게 해서 IP 바뀌는 것 보여주면 되고

분신술

1. MAC 과 쿠키를 내 것이 아닌 다른 사람의 것 혹은 가상의 것으로 변장해보자
   A. 이때는 로컬 서버 하나 열어서 거기에 접속하는 것 보여주고
   B. tcpdump 로 MAC 주소가 보여지는 것 확인시켜 주고..
2. MAC 을 변조해보자
   A. **[실습]** 내 컴퓨터에서 서버 하나 열어서 사람들의 MAC 주소가 그대로 보여지는 것 보여주기
   B. TMAC 과 macchanger 로 MAC 주소 변조 해보기.
   C. A 의 주소를 0.2 이라고 하고 B 의 주소를 0.3 이라고 하고 내 컴퓨터에서 열어둔 서버를 0.5 라고 했을 때 A 가 자신의 아이피를 0.3 으로 변조해서 내 서버로 보냈을 때 서버가 B 에게 답장하는 것도 보여주면 재밌을 듯
3. 쿠키를 변조해보자 (버프 슈트)
   A. 크롬에서 접속하게 하고 쿠키값을 파이어폭스에 접속할 때
   B. 버프 슈트로 프록시 탄 후에
   C. 근데 이거 트리거가 좀 애매해서 불안정하다
   D. 그럼 이거 넘어가고

메모

1. 내 노트북에 서버 열어서 들어오게 한 다음 " sudo tcpdump –i wlo1 –enNt 'port 3000 and dst host 192.168.0.4(내 아이피)' 명령어로 패킷이 들어오는 걸 보여주게 함
2. " sudo iftop –i wlo1 –f 'port 3000 and dst host 192.168.0.4 " 로 사람들이 접속하면서 연결이 되는 것을 메모해가면서 보여줌.
3. 각자의 컴퓨터에서 ipconfig, ifconfig 로 자신의 아이피를 알려주라 한 후 각자의 IP 를 메모장에 IP – 이름과 매핑시키면서 메모해둠.

사실 IP 스푸핑을 하면 제대로된 답장을 받지 못하기 때문에 HTTP 통신은 불가능. 하지만 LAN 에 있는 어떤 컴퓨터의 ARP 스푸핑을 떄려서 패킷 릴레이를 하게 한 다음 그 컴퓨터 IP 로 스푸핑을 하면 통신 가능함.

TMAC 으로 맥주소 바꾸니까 연결 안 끊기고 잘 된다. 장치관리자에서 맥주소를 00000000000 으로 바꾸니까 연결 자체가 끊어졌다. 하지만 TMAC 은 되더라.

BrowSec 확장 키는 것만으로 일단 IP 가 변조되긴 하네. 얘네들 프록시 서버로 릴레이 시켜주나봐.

그니까 BrowSec 은 단순한 프록시 접속이고, SwitchyOmega 확장으로 프록시 설정을 간편하게 하고 Kronymous 로 토르 프록시를 탈 수 있음.

IP 는 변조 되는데, MAC 은 안 바뀜. TMAC 으로 바꿔도 NIC 에서 안 바뀌는 듯. TMAC 으로 MAC 을 바꿔도 서버 로그에서는 MAC 이 안바뀌는 이유를 NIC 자체 원리를 이해해야 알 수 있을 듯 함.

자기 IP 와 MAC 주소를 변경해서 서버에 접속하게 해보기.

- IP 변경 --> TCP 연결 성립 안됨

- IP 변경 대신 프록시 --> 로컬 서버 접속 안됨
- 프록시 --> ghostogether.club 에 접속하게 해서 IP 가 잘 변경 되었나 확인해야 함.
- 결론 : IP 변경은 로컬 서버로 테스트 할 수 없음 (ARP 스푸핑 연계로 가능하긴 함)
- MAC 변경 --> TCP 연결 성립 오케이
- MAC 변경 --> 로컬 서버에서 테스트 시켜줌

IP 변경 시 TCP 연결이 성립되지 않기 때문에 불가능하지만 ARP 스푸핑을 통한 LAN 내부의 컴퓨터 IP 를 위조함으로써 패킷 릴레이를 시켜주는 것으로 IP 변경 후 HTTP 연결 가능하게 할 수 있음.

1. 내 컴퓨터 0.2 피해자 컴퓨터 0.3 게이트웨이 0.1 이라고 하고, 서버 20.20 이라고 하자.
2. ARP 스푸핑을 떄린다. (1) 피해자(0.3) 에게 내 컴퓨터(0.2) 가 게이트웨이 라고 우기고, 게이트웨이(0.1) 에게 내 컴퓨터(0.2) 가 0.3 이라고 우긴다.
    A. 이때 게이트웨이는 0.3 에게 갈 패킷을 0.2 에게 보내고 0.3 도 0.1 에게 보낼 패킷을 0.2 에게 보낸다.
    B. 따라서 내 컴퓨터에서 라우팅 기능을 킨 다음 (리눅스랑 윈도우 둘 다 라우팅 서비스 가능함 방법은 좀 다르지만) 패킷을 릴레이 시켜준다.
3. 그럼 이때 나는 내 컴퓨터의 IP 를 0.3 으로 변조시킨 후 서버에 패킷을 보낸다.
4. 서버는 0.3 에게 반환하겠지만 0.3 으로 갈 패킷은 ARP 스푸핑으로 인해 내 컴퓨터(0.2) 에게로 온다.

IP 추적? MAC 추적?
