3주차 연구일지

-Wi-Fi 공격기법

MITM(Man-In-The-Middle Attack)

- 공격자가 두 개의 통신 주체(사용자,AP) 사이에 개입하여 데이터를 가로채거나 변조하는 공격 방식이다.
- 공격자는 통신 중에 전송되는 데이터를 수정하여 악성코드를 삽입하거나, 사용자의 의도하지 않은 행동을 하도록 유도할 수 있다.
- 공격 유형으로는 DNS Spoofing, Session Hijacking, ARP Spoofing, Phishing AP등이 있다.

-공격 동작

1. 예시로 Client 와 Server가 메시지를 교환 하려고 한다.
2. 메시지 교환을 위해 Server가 Client에게 공개키(Public Key)를 요청한다.
3. Client가 Server에게 공개키를 보내려할때 공격자가 공격유형을 통해 끼어들어 Client의 공개키를 Server 대신 받는다.
4. 공격자는 Server에게 자신의 공개키를 보내 Server가 Client의 공개키로 속여 Server의 비밀키(Private Key)를 받는다.
5. 공격자는 Client에게 공격자의 비밀키를 보내 자신이 Server라고 속여 Client와 Server사이의 메시지들을 자신에게 오도록 만든다.

-보안방법

- WPA 3와 같은 강력한 무선 보안 프로토콜을 사용하여 데이터 암호화하기.
- VPN사용하여 트래픽을 암호화
- 신뢰할 수 있는 AP만 연결하고, SSID가 동일한 AP 주의.
- 정기적으로 소프트웨어 및 펌웨어 업데이트를 통해 보안 취약점을 패치.

-공격 유형

(가) DNS Spoofing

- 공격자가 DNS 요청을 가로채거나 변조하여 사용자가 의도하지 않는 IP 주소로 리다이렉트하는 공격 기법이다

1. 사용자는 웹 브라이주에 www.example.com을 입력하여 DNS에 해당 도메인의 IP 주소를 요청한다.

2. 공격자는 DNS Cache Spoofing/Packet Sniffing/공격자 DNS 서버 설정등의 공격으로 DNS에 해당하는 IP 값을 변조시켜 사용자가 공격자가 원하는 사이트로 접속하도록 만든다.

-보안방법

- DNSSEC(DNS Security Extensions)라는 DNS 응답의 무결성을 검증하는 보안 프로토콜을 사용하여 공격 방지.
- HTTPS를 사용하여 데이터를 암호화되어 전송하여 데이터의 내용을 쉽게 읽을 수 없게 만든다.
- 신뢰할 수 있는 DNS 서버 사용(공용 DNS, Ex) google DNS등)하거나, ISP에서 제공하는 DNS서버 사용.

(나) Phishing AP

- 무선 액세스 포인트(WAP : Wireless Access Point)중 하나로, 공격자가 사용자의 개인 정보 탈취를 위해 설정한 악성 AP다.
- 사용자에게 신뢰할 수 있는 네트워크에 연결하고 있다고 믿게 만들어 공격자가 제어하는 네트워크에 연결하도록 유도한다.

1. 가짜 AP 설정을 위해 실제 무선 네트워크와 유사한 SSID를 가진 무선 AP를 설정한다.
2. 신호강도를 강하게 설정하여 사용자가 쉽게 연결하도록 유도한다.
3. Fishing AP를 통해 실제 인터넷에 연결할 수 있도록 설정하여 사용자가 정상적으로 인터넷을 사용할 수 있도록 하여 사용자의 트래픽을 공격자가 제어하는 AP를 통해 흐르게 만든다.

-보안방법

- SSID를 확인하여 의심스러운 네트워크에 연결하지 않도록 한다.
- VPN사용 및 보안 소프트웨어를 사용.
- HTTPS를 사용하여 데이터를 암호화하여 내용을 쉽게 보지 못하도록 한다.

(다) ARP Spoofing

- ARP란 IP주소를 MAC 주소로 변환하는 프로토콜이다.
- 근거리 통신망(LAN)하에 ARP 메시지를 이용하여 상대방의 데이터 패킷을 중간에 가로채는 공격 기법이다.
- ARP는 인증 과정이 없는 취약점을 이용한 공격이다.

1. A,B가 통신을 위해 ARP 메시지를 전송 하려고 한다.

2. 공격자가 A,B에게 자신의 MAC 주소를 보내어 A,B가 정상적으로 통신하고 있다고 속인다.
3. A,B는 공격자에게 메시지로 공격자는 서로의 메시지를 받은 후 전달하여 메시지를 모두 읽을 수 있다.

공격 과정

1. “arp -a” 명령어로 희생자 PC의 IP, Gateway IP 확인
2. MAC주소 위조를 위해 arpspoof or ettercap 사용
3. arpspoof 사용
   ㄴ> arpspoof -i [인터페이스] -t[희생자 ip] [희생자 gateway address]
4. arp -a로 arp table 확인
5. 희생자 pc가 외부 접속이 가능하도록 패킷을 외부로 전송 포워딩한다(패킷 포워딩) / 명령어 : # fragrouter -B1
6. tcpdump or Wireshark를 이용하여 가로챈 패킷 확인 가능
   ㄴ> tcpdump : tcpdump host 피해자 ip address
   Wireshark : ip.addr == [ip address] -> TCP -> Follow TCP Stream으로 결과값 확인

-보안방법

- 정적(Static) ARP Table 설정, 수동으로 IP-MAC 매핑
  ㄴ> Window : arp -s [ip] [MAC]
  Linux : sudo arp -s [ip] [MAC]
- ARP 감지 시스템(ARPWatch등) 시스템 사용
- 패킷 필터링 적용(DHCP Snooping, Dynamic ARP Inspection)하여 스위치에서 DAI(Dynamic ARP Inspection)활성화 하여 비정상적인 ARP 패킷 필터링
- VPN, HTTPS 사용하여 데이터를 암호화 하기.
- 방화벽 및 IDS/IPS 활용하여 의심스러운 ARP 패킷 탐지

-Wireshark

(1) 패킷 표시

- No : 패킷 번호
- Time : 패킷이 캡쳐된 시간
- Source : 패킷을 보낸 IP주소
- Destination : 패킷을 받은 IP주소
- Protocol : 사용된 프로토콜
- Length : 패킷 크기

- Info : 추가 정보

(2) 패킷 필터링
일반적으로 분석하는 패킷은 HTTP/HTTPS, DNS, TCP/UDP, ICMP, ARP등을 분석한다. 패킷의 양이 방대하므로 필터링 기술을 지원한다.

- ip.addr == xxx.xxx.xxx.xxx : 특정 IP주소만 확인
- tcp,port == xx : 특정 포트 패킷만 확인
- http or dns or icmp… : 해당 패킷만 보기
- tcp contains “example” : “example” 문자열이 포함된 패킷 찾기
- 컬러 필터링(Edit -> Coloring Rules)를 통해 패킷에 대한 규칙을 설정하여 색으로 구분할 수 있다.

(3) 패킷 저장
“File -> Save As”를 통해 저장하면 .pcap확장자를 통해 저장된다.
분석을 위해 tshark, scapy, pyshark등과 함께 사용 가능.

-참고자료
1. FORTINET : https://www.fortinet.com/kr/resources/cyberglossary
2.위키백과 : https://ko.wikipedia.org/wiki/%EC%A4%91%EA%B0%84%EC%9E%90_%EA%B3%B5%EA%B2%A9
3.몰라몰라개복치 : https://mikrkosmos97.tistory.com/105