1. 인터넷과 보안

먼저, 인터넷이 인기가 없었으면, 지금처럼 보안이 중요하지 않았을 것이다.
인터넷과 보안은 너무나 밀접한 관계에 있다.

◈ 인터넷 프로토콜

HTTP, FTP, SMTP, Telnet	응용층	HTTPS, SFTP, S/MIME SSH, Kerberos, SET
TCP, UDP	전송층	SSL / TLS
IP	네트워크층	IPSec
이더넷, 토큰링	데이터링크층	L2TP(Layer2 Tunneling Protocol)
	물리층	
[보안 기능이 없는 프로토콜]	[인터넷]	[보안 기능이 있는 프로토콜]

- 인터넷은 개방시스템이다.
- 인터넷은 지구 전체의 컴퓨터 네트워크 시스템이다.
- 인터넷 프로토콜은 처음 개발되면서 보안 기능이 포함되지 않았다.
- 인터넷 인기가 높아지면서 보안의 필요성은 매우 중요하게 되었고
- 해서, 보안 관련 프로토콜이 개발되었다.

- 위에 소개된 **보안 기능이 있는 프로토콜**들은 보안에서 매우 중요한 프로토콜들이다.
- 중요하다는 것은 현재 보안 시험에 많이 출제되고 있다는 것이다.
- 인터넷 각 층에서 사용되는 보안 프로토콜이 무엇인지? 우선 정리해야 한다.
- 앞으로 하나씩 상세하게 설명할 것이다.

Polybius 암호 - "혼돈과 확산" 이해

- Polybius 암호는 고대 그리스 시민 "Polybius"가 제안한 암호이다.
- Polybius 암호는 다음 변환표를 이용하여 영문자를 수로 암호화 한다.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i / j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

변환표

- Polybius 암호에서 송수신측은 동일한 변환표를 이용해야 한다.

[예제] "pass"를 암호화 하면

---

① 위의 변환표에 의거하여 각 문자를 숫자로 변환하면 (대치암호)

p = 35, a = 11, s = 43, s = 43
↓
35 11 43 43

- 각 문자를 숫자로 대치하면, 혼돈(confusion)의 특성을 가지게 된다.
- **혼돈**의 사전적 의미는 "마구 뒤섞여 있어 갈피를 잡을 수 없는 상태"이다.

② 변환된 각 수를 세로로 쓰고, 가로로 읽는다. (전치암호)

3	1	4	4
5	1	3	3

→ **가로로 차례로 읽음 : 31 44 51 33**

- 각 수를 세로로 쓰고, 가로로 읽으면, 확산(diffusion)의 특성도 가지게 된다.
- **확산**은 물리적으로 농도가 다른 물질이 시간이 지나면서 **혼합**되는 의미를 가진다.

기출문제 분석

1. TCP에 대한 설명으로 옳지 않은 것은? [2022년 국가 9급]

① 비연결 지향 프로토콜이다.
② 3-Way Handshaking을 통해 서비스를 연결 설정한다.
③ 포트번호를 이용하여 서비스들을 구별하여 제공할 수 있다.
④ SYN Flooding 공격은 TCP 취약점에 대한 공격이다.

♤ TCP

• **비연결** 지향 프로토콜이다.(×) → TCP는 **연결** 지향 프로토콜이다.

정답 : ①

2. 다음의 OSI 7계층과 이에 대응하는 계층에서 동작하는 〈보기〉의 보안 프로토콜을 바르게 연결한 것은? [2017년 지방 9급]

ㄱ. 2계층　　ㄴ. 3계층　　ㄷ. 4계층

-----<보기>----------

A. SSL/TLS　　B. L2TP　　C. IPSec

	ㄱ	ㄴ	ㄷ
①	A	B	C
②	A	C	B
③	B	C	A
④	B	A	C

♤ OSI 7계층과 이에 대응하는 보안 프로토콜

• 2계층 : L2TP(Layer 2 Tunneling Protocol)
• 3계층 : IPSec
• 4계층 : SSL/TLS → SSL/TLS는 전송층과 응용층 사이에서 동작한다.

정답 : ③

3. TCP/IP 프로토콜 계층과 각 계층에서 구현되는 보안 기술의 연결로 옳은 것은? [2015년 국회 9급]

① 응용층 - Kerberos
② 전송층 - IPSec
③ 네트워크층 - TLS
④ 데이터링크층 - SSL
⑤ 물리층 - SET

♤ **보안 기술 연결**

---

② IPSec - 네트워크층
③ TLS - 응용층과 전송층 사이에서 웹 보안을 담당한다.
④ SSL - 응용층과 전송층 사이에서 웹 보안을 담당한다.
⑤ SET - 응용층

정답 : ①

4. 네트워크 각 계층별 보안 프로토콜로 옳지 않은 것은? [2014년 국가 9급]

① 네트워크층(network layer) : IPSec
② 네트워크층(network layer) : SFTP
③ 응용층(application layer) : SSH
④ 응용층(application layer) : S/MIME

♤ **보안 프로토콜**

• IPSec : 네트워크층
• SSH, S/MIME, SFTP : 응용층

◈ **SSH(Secure Shell)**

• SSH는 원격으로 다른 호스트에 접근하는 것을 보호하기 위해 설계되었다.
• SSH는 불안전한 네트워크에서 안전하게 통신할 수 있는 기능을 지원한다.
• SSH는 기존의 Telnet, rlogin 등을 대체하기 위해 설계되었다.
• SSH는 사용자(클라이언트)와 서버를 인증한다.(공개키 암호)

정답 : ②

5. 다음 중 OSI 7계층 모델에서 동작하는 계층이 다른 것은? [2019년 지방 9급]

① L2TP ② SYN 플러딩
③ PPTP ④ ARP 스푸핑

♤ **OSI 7계층**

- 2계층 : L2TP, PPTP, ARP 스푸핑
- 4계층 : SYN 플러딩

정답 : ②

6. OSI 7계층 중 2계층 암호화 프로토콜로 짝지어진 것은? [2020년 국회 9급]

① PPTP – SSL
② PPTP – IPSec
③ L2TP – IPSec
④ L2TP – SSL
⑤ PPTP – L2TP

♤ **2계층 암호화 프로토콜**

OSI 계층	터널링 프로토콜
2계층	• L2F(layer 2 Forwarding) • L2TP(Layer 2 Tunneling Protocol) • PPTP(Point-to-Point Tunneling Protocol)
3계층	• IPSec(Internet Protocol Security) → IPSec는 VPN 터널링의 업계 표준이다. → IPSec는 강력한 인증과 암호화가 3계층에서 실시된다. • VTP(Virtual Tunneling Protocol) • ATMP(Ascend Tunnel Management Protocol)
5계층	• SOCKS V5 • SOCKS V5의 터널 서비스는 Session-by-Session 구조이다. → SSL/TLS를 결합하여 사용 가능하다. → 2, 3층 터널링 프로토콜에 비해 뛰어난 접근제어 기능 제공 → Extranet VPN에 적합

- 터널링(tunneling)은 VPN 구성의 핵심요소 중 하나이다.

정답 : ⑤

7. SSL 프로토콜에 대한 설명으로 옳지 않은 것은? [2018년 지방 9급]

① 전송층과 네트워크층 사이에서 동작한다.
② 인증, 기밀성, 무결성 서비스를 제공한다.
③ Handshake Protocol은 보안 속성 협상을 담당한다.
④ Record Protocol은 메시지 압축 및 암호화를 담당한다.

♤ **SSL 프로토콜**

- **전송층**과 **네트워크층** 사이에서 동작한다.**(×)**
  → SSL은 **전송층**과 **응용층** 사이에서 동작한다.
- 주의할 것은 "SSL은 전송층에서 동작한다." 라고도 출제된다.

정답 : ①