

토픽 이름	해킹(Hacking)
버전	Ver.20180708
분류	디지털 보안 > Hacking
증토픽	IP Spoofing ARP 스푸핑 공격 TCP SYN Flooding Dos, DDos, Slowloris, rudy APT 랜섬웨어 사회공학

토픽 이름	해킹(Hacking)
버전	Ver.20180708
분류	디지털 보안 > Hacking
키워드(암기)	<p>특징 : 분산화, 자동화, 에이전트화, 은닉성</p> <p>유형 : 프로그램 취약점, 프로토콜 취약점, 악성코드, 시스템과 서비스 설정 취약점, 사회공학적</p> <p>종류 : 버버오버플로우 공격, 레이스 컨디셔닝, 포맷 스트링웹 어플리케이션 해킹 서비스 공격거부, 스니핑, IP 스펍핑, ARP 스펪핑, 세션 하이제킹 TCP SYN Flooding 공격, Smurfing Dos 공격, DDos, Trinoo</p> <p>직접적인 접근, 도청, 어깨 넘어로 훔쳐보기, 휴지통 뒤지기, 설문조사, Piggybacking</p>
리드문	보안 취약점의 악의적 이용 혹은 피해를 주는 행동, 해킹의 개요
암기법(해당경우)	

기출문제

번호	문제	회차
1	1. 크라임웨어(Crimeware)	113.1정보관리.1.1
2	7. 익명 네트워크 TOR(The Onion Routing)	113.1정보관리.1.7
3	3. 랜섬웨어 공격에 대하여 사전, 사후적 대응방안을 기술적, 관리적 관점에서 설명	113.1정보관리.3.3
4	13. 스투кс넷(Stuxnet)에 대해 설명하시오.	110.정보관리.1.13
5	11. 랜섬웨어(Ransomware)에 대해 설명하시오.	110.컴시응.1.11
6	4. 최근 ATP(Advanced Persistent Threats)공격과 변종 악성코드 공격이 늘어나고 있다, APT 공격기법과 악성코드(Malicious codes)에 대하여 설명하시오.	105.정보관리.3.4
7	3. 랜섬웨어와 파밍에 대해 설명	104.정보관리.1.3
8	6. 액티브 피싱(Active phishing)에 대하여 설명하시오.	101.정보관리.1.6
9	10. ARP 스펪핑(Address Resolution Protocol spoofing)의 개념과 대처방안에 대하여 설명하시오.	99.정보관리.1.10
10	13. 좀비 쿠키(Zombie cookie)에 대하여 설명하시오.	99.정보관리.1.13
11	5. Slow Read DDos Attack	99.컴시응.1.5
12	3. 최근 지하철, 커피숍, 도서관 등에서 무료로 제공하는 공공 무선접속장치 (AP)를 이용하여 인터넷에 접속하는 사용자가 크게 증가하고 있다. 이러한 환경에서 악성 AP를 이용한 피싱(Phishing)공격법에 대하여 설명하고, 시사점 및 대응방안을 기술	99.컴시응.2.3
13	<p>6. 웹해킹 공격을 사전에 예방하기 위하여 보안취약점 분석 및 시큐어 코딩(Secure Coding)의 중요성이 높아가고 있다.</p> <p>XSS(Cross Site Scripting) 공격의 2 가지 유형에 대하여 설명하시오.</p> <p>다음의 C 또는 JAVA 언어로 작성된 코드에 대하여 안전하지 않은 이유를 설명하고 안전한 코드로 변경하시오.</p>	99.컴시응.2.6

	<table border="1"> <thead> <tr> <th>안전하지 않은 C 코드</th><th>안전하지 않은 JAVA 코드</th></tr> </thead> <tbody> <tr> <td> <pre> 1: #include <stdio.h> 2: #include <stdlib.h> 3: #include <unistd.h> 4: #include <string.h> 5: void f() 6: { 7: char* rName = getenv("reportName"); 8: char buf[30]; 9: strcpy(buf, "/home/www/tmp/", 30); 10: strcat(buf, rName, 30); 11: unlink(buf); 12: } </pre> </td><td> <pre> 1: ... 2: public void f(Properties request) { 3: ... 4: String name = request.getProperty("filename"); 5: if(name != null) { 6: File file = new File("/usr/local/tmp/" + name); 7: file.delete(); 8: ... 9: ... 10: } </pre> </td></tr> </tbody> </table>	안전하지 않은 C 코드	안전하지 않은 JAVA 코드	<pre> 1: #include <stdio.h> 2: #include <stdlib.h> 3: #include <unistd.h> 4: #include <string.h> 5: void f() 6: { 7: char* rName = getenv("reportName"); 8: char buf[30]; 9: strcpy(buf, "/home/www/tmp/", 30); 10: strcat(buf, rName, 30); 11: unlink(buf); 12: } </pre>	<pre> 1: ... 2: public void f(Properties request) { 3: ... 4: String name = request.getProperty("filename"); 5: if(name != null) { 6: File file = new File("/usr/local/tmp/" + name); 7: file.delete(); 8: ... 9: ... 10: } </pre>	
안전하지 않은 C 코드	안전하지 않은 JAVA 코드					
<pre> 1: #include <stdio.h> 2: #include <stdlib.h> 3: #include <unistd.h> 4: #include <string.h> 5: void f() 6: { 7: char* rName = getenv("reportName"); 8: char buf[30]; 9: strcpy(buf, "/home/www/tmp/", 30); 10: strcat(buf, rName, 30); 11: unlink(buf); 12: } </pre>	<pre> 1: ... 2: public void f(Properties request) { 3: ... 4: String name = request.getProperty("filename"); 5: if(name != null) { 6: File file = new File("/usr/local/tmp/" + name); 7: file.delete(); 8: ... 9: ... 10: } </pre>					
14	<p>3. 악성코드는 시스템사용자나 소유자의 이익에 반하는 행위를 하는 프로그램 이다. 최근 출현하는 신.변종 악성코드들은 지속형 공격의 형태로 개인과 사회를 위협하고 있다.</p> <p>(1) 악성코드의 4 가지 유형을 설명하시오. (2) 악성코드를 개발하고 전파시키는 목적 3가지를 기술하시오</p>	99.컴시응.3.3				
15	<p>4. 최근 DDoS 공격이 지능화되면서, 공격트래픽에 대한 신속한 탐지 및 완화(Mitigation)를 어렵게 하고 있다.</p> <p>(1)DDoS 공격유형별(대역폭공격, 세션공격, 웹 HTTP 공격) 피해증상을 설명 하시오. (2)DDoS 대응을 위한 Anti-DDoS 시스템의 대응방식을 다음의 2 가지 경우로 나누어 설명하시오.</p> <p>첫째, 공격 IP가 변조된 경우 인증기능을 통해 대응하는 방식 둘째, 공격 IP가 변조되지 않은 경우 대응하는 방식</p>	99.컴시응.4.4				
16	<p>5. 정보 기술 모니터링(Information Technology monitoring)은 키 입력수, 실수율, 거래처리 건수 같은 수단을 이용해서 사람들의 행동을 추적하는 것이다. 일반적인 모니터링기술 (예, Key Logger Software, Spyware 등)을 설명하시오.</p>	99.정보관리.3.5				
17	<p>4. 악성코드 탐지 기법을 개발하기 위해서는 탐지하고자 하는 악성코드의 종류 및 특징을 분석해야 한다. 다음에 대해 설명하시오.</p> <p>가. 악성코드의 종류 악성코드 분석 방법</p>	98.정보관리.4.4				
18	4. APT(Advanced Persistent Threat) 공격기법과 대응방법에 대하여 설명하시오.	96.정보관리.3.4				
19	10. 파밍 (Pharming)	95.컴시응.1.10				
20	2. DDOS(Distributed Denial of Service) 공격의 유형을 설명하시오.	93.정보관리.1.2				
21	4. 최근 Ddos(Distributed Denial of Service) 공격으로 국가적인 혼란에 직면하였는데, 이런 Ddos 공격에 대한 전용 방어 장비의 종류(두가지 방식)와 중장기적인 대책에 대해 설명하시오	89.정보관리.4.4				
22	1. 윤리적 해커(Ethical Hacker)	89.컴시응.1.1				
23	1.13. DDoS (Distributed Denial-of-Service attack)	84.컴시응.1.13				

I. 보안 취약점의 악의적 이용 혹은 피해를 주는 행동, 해킹의 개요

가. 해킹(Hacking)의 정의

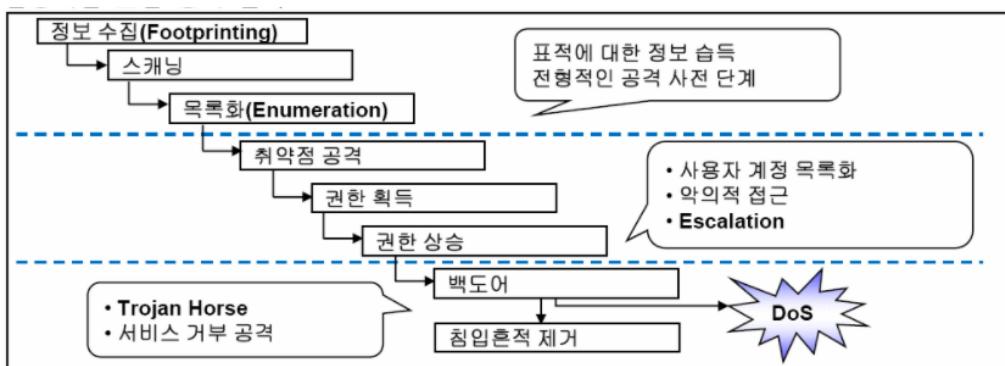
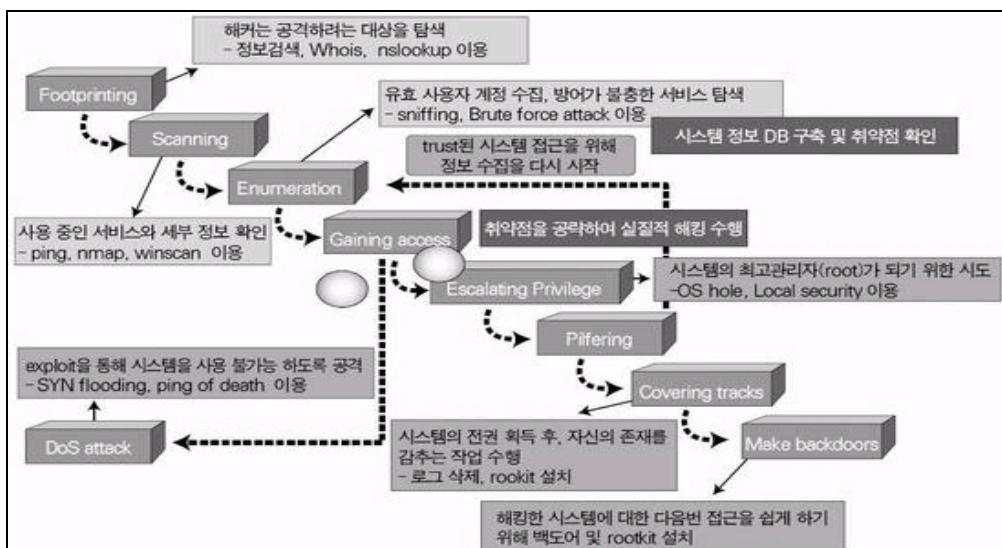
- 시스템 관리자가 구축해놓은 보안망을 무력화시키거나, 시스템 관리자 권한을 불법적으로 획득 및 악용해 다른 사용자에게 피해를 주는 일체의 행동
- 컴퓨터 네트워크의 보안 취약점을 찾아내어 이를 악의적으로 이용하는 행위

나. 해킹 공격의 특징

구분	내용
분산화 (Distributed)	원격조정이 가능한 Agent형 백도어를 설치하고 이를 이용해 다른 시스템을 공격하는 방법
자동화 (Automation)	인터넷웜 및 윈도우용 공격도구 최근의 공격스크립트의 자동화
에이전트화 (Agent)	원격명령으로 공격을 수행하거나 에이전트 기반 빠른 정보 입수
은닉성 (Stealth)	Agent를 이용한 분산공격기법은 침입탐지 시스템을 무력화 할 수 있는 공격으로 공격자의 위치를 은닉

II. 해킹 절차 구성도 및 구성요소

가. 해킹 절차 구성도



나. 해킹 절차의 구성 요소

구분	정의	수집정보
Footprinting	공격대상의 정보수집	DNS, IPACL, 보안장비, H/W, 인증 방법
Scanning	공격대상의 제공서비스 및 세부정보 확인	OS, 동적호스트, 제공서비스 및 포트
Enumeration	유효사용자계정 수집 및 시스템취약부분 수집	라우팅테이블, Snmp user&group name
gaining	공격대상에 접근을 시도하여 접근권한 획득	패스워드 도청, 패스워드 파일 획득
Escalation Privilege	관리자의 접근권한 획득	관리자에 대한 정보 수집
pilfering	단독시스템 권한 획득 후 신뢰관계시스템의 접근권한 확보를 위한 정보 재수집	사용자에 대한 정보 재수집
Covering Track	공격대상에 대한 모든 접근 권한 획득 후 침입에 관련한 정보 및 도구를 숨김	로그/감사정보
Creating Backdoor	재침입을 위해 백도어 설치	

III. 해킹의 주요 유형 및 기법

가. 해킹의 주요 유형

구분	내용
프로그램의 취약점을 이용한 공격	<ul style="list-style-type: none"> - 버퍼오버플로우(Buffer Overflow)공격 - 레이스컨디셔닝(race conditioning)공격 - 포맷스트링(format string)공격 - CGI/자바 스크립트의 취약점공격 - ASP, PHP 스크립트의 취약점 공격
프로토콜의 취약점을 이용한 공격	DoS와 DDoS, 스니핑(Sniffing), 스푸핑(Spoofing), 세션하이재킹(Session Hijacking), NetBIOS 크래킹
악성코드(Malicious Software, Malware)	바이러스, 트로이 목마, 백도어웜, 블라스트웜
사회공학적 해킹기법	인간기반(Human Based), 컴퓨터 기반(Computer Based)
시스템과 서비스 설정의 취약점을 이용한 공격	시스템과 시스템에서 제공하는 각종 서비스 설정과 관련 취약점을 이용 Ransomware, Waterhole

나. 프로그램의 취약점을 이용한 공격

구분	해킹 기법 및 대응책	
버퍼 오버플로우 공격 (Buffer Overflow)	해킹 기법	<ul style="list-style-type: none"> - 실행중인 프로세스의 실행흐름을 바꾸어서 자신이 원하는 코드를 실행시키는 형태의 공격방법 - “특정모듈호출 → 해당기능실행 → 호출이전모듈로 리턴”, 이때 리턴 주소를 원하는 곳으로 바꾸는 기법 - 해커들은 특정실행코드를 미리 메모리상에 저장, 리턴 주소가 그 코드의 시작부분을 가리키도록 함

구분		해킹 기법 및 대응책
레이스 컨디셔닝 (Race Conditioning)	대응책	<ul style="list-style-type: none"> - Stack Overflow, Heap Overflow로 분류 - 벤더에서 제공하는 소프트웨어 관련패치 적용, 최소권한으로의 프로그램 실행, 불필요한 서비스 제거 - 침입차단시스템을 통한 유해 트래픽 차단
	해킹 기법	<ul style="list-style-type: none"> - 운영체제의 멀티 태스킹 매커니즘의 취약점 이용 - 관리자 권한으로 실행되는 프로그램 중간에 끼어들어 자신이 원하는 작업을 하는 것
포맷스트링 (Format String)	대응책	<ul style="list-style-type: none"> - 임시파일을 생성할 때, 임시파일이 이미 존재하는지 체크, 그 파일을 지우고 새로 생성 - 생성한 파일이 심볼릭 링크인지를 검사 - 지속적인 프로세스의 보안취약성 점검 및 관리
	해킹 기법	<ul style="list-style-type: none"> - C언어의 포맷 스트링 (printf, fprintf, sprint 등)의 취약성을 이용한 공격기법 - 공격자가 원하는 부분에 값을 입력, 변경 가능 (메모리 내용, 메모리 주소값)
웹 애플리케이션 해킹 (Web Application)	대응책	<ul style="list-style-type: none"> - 항상 최신패치적용, 각종 보안도구 이용하여 방어 - Non-executable Stack option 사용
	해킹 기법	<ul style="list-style-type: none"> - 접근통제솔루션은 웹 서비스로 접근하는 패킷을 통제 하지 않고 내부로 유입 시키기 때문에 악의적으로 패킷을 조작해서 보낸다면 정상 패킷으로 간주하여 적절한 통제가 이뤄질 수 없음
	대응책	<ul style="list-style-type: none"> - 검증되지 않은 파라미터의 허용: 웹 요청에 대한 데이터형식, 데이터 길이 등의 예외규칙 적용 - 부적절한 접근통제: 웹 컨텐츠의 퍼미션 점검, 불안전한 ID점검, 절대경로를 통한 인증회피가능 점검 - 부적절한 계정과 세션관리: 패스워드변경통제의 관리, 세션아이디보호, 백엔드 인증 등

다. 프로토콜의 취약점을 이용한 공격

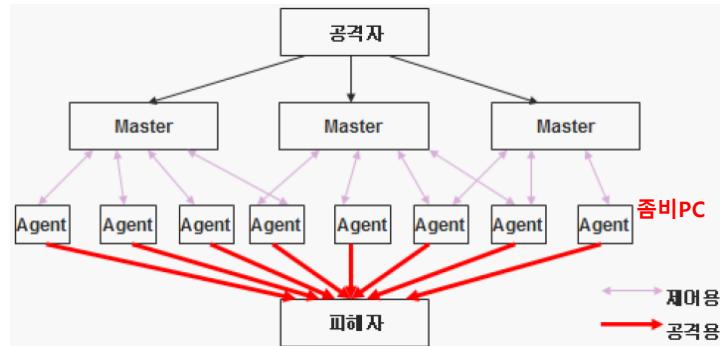
구분		해킹 기법 및 대응책
서비스거부 공격 (Denial of Service)	해킹 기법	<ul style="list-style-type: none"> - 시스템의 정상적인 서비스를 방해할 목적으로 대량의 데이터를 보내 대상 네트워크나 시스템의 성능을 급격히 저하시켜 대상시스템에서 제공하는 서비스들을 사용하지 못하게 하는 일반적 해킹수법 - 분산서비스 거부공격이란 이름으로 N개의 불특정 시스템이 단일 네트워크를 대상으로 공격을 시도하는 N:1 유형이 주류
	대응책	<ul style="list-style-type: none"> - 초기에 이상징후 탐지하여 빠른 대응 - 보안 솔루션 구축 및 적절한 관리 운영, 기업보안대책 지속적인 업데이트
스니핑 (Sniffing)	해킹 기법	<ul style="list-style-type: none"> - 정의: 컴퓨터 네트워크상에 흘러 다니는 트래픽을 엿듣는 도청장치, 스니퍼를 이용해 네트워크상의 데이터를 도청하는 행위 - 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 도청하는 것 의미 - 스니핑에 취약한 프로토콜: Telnet, Rlogin, Http, SNMP, FTP, SMTP 등

		<p>[시나리오]</p> <ul style="list-style-type: none"> (1) 다양한 공격 기법을 통해 실제 공격 대상 시스템에 관리자 권한을 얻어낸 후 스니핑 도구를 설치하여 스니핑 (2) 공격 대상 기업의 다른 호스트에 대한 접근 권한을 얻어내서 그 호스트를 이용하여 스니핑 (3) ISP장비에 대한 시스템 권한을 얻어내어 스니핑 도구를 설치하여 스니핑 																				
	대응책	<ul style="list-style-type: none"> - 패킷을 가로채더라도 내용을 알 수 없게 하는 암호화 기법이 일반적 방어기법 - SSL 적용, PGP, S/MIME, SSH VPN 																				
IP스푸핑 (IP Spoofing)	해킹 기법	<ul style="list-style-type: none"> - TCP/IP의 구조적 결함에서 출발한 방법으로 TCP시퀀스번호, Source routing, 소스 IP 주소를 이용해서 상대방 호스트가 자신의 호스트를 트러스트하게 만드는 방법(spoof:속이기/속임수) - IP 주소 등의 정보를 속임으로써 권한을 획득하고 중요 정보를 가로채어, 서비스 방해까지 행하는 TCP/IP프로토콜 결함을 이용한 해킹공격 <div style="border: 1px solid black; padding: 10px; width: fit-content; margin-left: auto; margin-right: auto;"> <p>IP스푸핑의 공격절차</p> <ol style="list-style-type: none"> 1) 패킷의 내용 변경하여 스크리닝 라우터와 방화벽 통화 2) 소스IP주소를 조작, 자신을 신뢰성있는 호스트로 인식 3) 원하는 호스트의 초기 시퀀스번호를 알아냄 4) 트로이목마 등의 프로그램설치, 호스트 접근 권한 혹은 루트 권한 획득 </div>																				
	대응책	<ul style="list-style-type: none"> - 공격자에게 RESET 신호를 보내어 공격을 차단하거나 공격 클라이언트를 차단하여 공격으로부터 서버를 보호하거나 운영체제를 Patch 또한 방화벽에서 불필요한 IP 접근을 방지 																				
ARP스푸핑 (ARP Spoofing)	해킹 기법	<ul style="list-style-type: none"> - LAN 카드의 고유한 주소인 MAC address를 동일 네트워크에 존재하는 다른 PC의 LAN 카드 주소로 위장, 다른 PC에 전달되어야 하는 정보를 가로채는 MITM(Man In The Middle) 공격 방식 <div style="border: 1px solid black; padding: 10px; width: fit-content; margin-left: auto; margin-right: auto;"> <table border="1" style="margin-bottom: 10px;"> <thead> <tr> <th colspan="2">호스트-A ARP Cache</th> <th colspan="2">호스트-B ARP Cache</th> </tr> <tr> <th>IP Addr</th> <th>Mac Address</th> <th>IP Addr</th> <th>Mac Address</th> </tr> </thead> <tbody> <tr> <td>192.168.1.2</td> <td>000112233445 000112233445</td> <td>192.168.1.1</td> <td>000112233445 000112233445</td> </tr> </tbody> </table> <table border="1" style="margin-bottom: 10px;"> <thead> <tr> <th>Port</th> <th>Mac Address</th> </tr> </thead> <tbody> <tr> <td>3</td> <td>000112233445</td> </tr> <tr> <td>1</td> <td>000102030405</td> </tr> <tr> <td>5</td> <td>000102030406</td> </tr> </tbody> </table> <p>Sniffer IP Addr : 192.168.1.10 MAC-A : 000112233445</p> </div>	호스트-A ARP Cache		호스트-B ARP Cache		IP Addr	Mac Address	IP Addr	Mac Address	192.168.1.2	000112233445 000112233445	192.168.1.1	000112233445 000112233445	Port	Mac Address	3	000112233445	1	000102030405	5	000102030406
호스트-A ARP Cache		호스트-B ARP Cache																				
IP Addr	Mac Address	IP Addr	Mac Address																			
192.168.1.2	000112233445 000112233445	192.168.1.1	000112233445 000112233445																			
Port	Mac Address																					
3	000112233445																					
1	000102030405																					
5	000102030406																					
	대응책	ARP 스폐핑 감지 소프트웨어 사용, ARP 캐시 정보를 변경되지 않도록 정적으로																				

		정의하여 사용 (ARP 신호를 받아도 무시하는 방법으로 관리함)
세션 하이재킹 (Session Hijacking)	해킹 기법	- 웹 브라우징 시 세션관리를 위해 사용되는 세션 아이디를 스니핑이나 무작위 추측공격(brute-force guessing)을 통해 도용하는 기법
	대응책	- 강력한 알고리즘에 의한 세션아이디 발급 - 세션아이디의 유효시간 및 계정 잠금 관리 - 길이가 길고 암호화된 세션아이디

라. DOS의 공격 기법

구분	내용
TCP SYN Flooding 공격	<p>- TCP 프로토콜의 3 Way Handshake를 악용</p> <p>(1) TCP 연결 요청 (발신: Host A, 수신: Host C) (2) Host C에게 응답 (3) Host C의 응답이 오지 않음 (4) TCP 연결 대기 큐가 Overflow 될 때 까지 계속 연결 요청</p> <ul style="list-style-type: none"> - 서버에 수 천 개의 TCP 접속(SYN) 요청 메시지를 보냄, 이 때 패킷 내부의 소스 IP주소를 속이거나 인터넷 상에서 사용하지 않는 IP 주소 값으로 변형 - 서버는 SYN/ACK 응답을 보낸 후, 클라이언트로부터 ACK가 올 때까지 기다리게 되고, 서버는 ACK 메시지를 받지 못하게 됨. - 이렇게 되면, 서버는 ACK를 받을 때까지, 버퍼와 같은 자원을 계속 종료하지 못하고 열어두게 되면서 <u>누적에 따른 시스템 다운 및 서비스를 중단하는 상황</u> 직면 - 불완전한 연결을 저장하기 위한 메모리 자료구조의 크기 제한으로 <u>서버 자원이 고갈되어 Buffer Overflow 에러 발생</u>
Smurfing DoS 공격	<p>Ping과 답변인 에코메시지로 인한 대량의 트래픽 발생 악용</p> <p>해커 → ICMP ECHO → 공격 대상 서버</p> <ul style="list-style-type: none"> - 광범위한 효과로 인해, 가장 무서운 DoS 방법 중의 하나이며, IP와 ICMP 특징을 악용 - 직접적인 브로드캐스트와 세가지 구성요소인 공격자, 증폭 네트워크, 표적을 최대한 이용 - 공격자는 증폭 네트워크의 브로드캐스트 주소로 공격, 서버가 요구하는 것처럼 패킷들의 원본주소를 위조하여 ICMP ECHO 패킷을 전송하고, ICMP ECHO 패킷을 수신한 증폭 네트워크 내의 모든 시스템은 공격 서버에 응답을 하게 됨 <p>* ICMP(Internet Control Message Protocol): 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고 에러를 알려주는 프로토콜</p>
DDoS(Distribute Denial of Service)	<ul style="list-style-type: none"> - 서비스에 대한 정당한 접근을 방해하거나 차단하고자 네트워크에 분산되어 있는 많은 에이전트를 이용하여 공격대상 서버에 동시에 과도한 서비스요청을 발생시키는 공격



- ① 공격자는 DDoS 에이전트를 확보하기 위해서 버퍼 오버플로우 등의 공격으로 일반 인터넷 사용자의 PC에 에이전트를 설치
- ② 설치된 에이전트는 마스터에 연결하여 DDoS 공격도구를 다운로드 받고, 공격 명령을 대기 함
- ③ 공격자는 마스터를 통해서 공격명령을 각 에이전트로 전달하고, 에이전트는 마스터로부터 수신한 공격명령에 따라서 피해자를 공격함

Trinoo

- 많은 소스로부터 통합된 UDP flood서비스 거부공격을 유발하는데 사용되는 도구
- 몇 개의 서버들과 많은 수의 클라이언트로 이루어짐
- 공격자는 마스터(서버)에게 하나 혹은 여러 개의 IP주소를 대상으로 서비스 거부 공격을 수행하라고 명령을 내리면 마스터는 특정한 기간으로 여러 개의 IP주소를 공격하도록 데몬과 통신함

마. 사회공학적 해킹기법

구분	설명	대응방안
인간기반 (Human Based)	<ul style="list-style-type: none"> - 인간 상호작용을 이용하여, 사람을 속여 보안 절차를 깨뜨리는 비기술적 침입 수단 - 공격대상에게 직접적인 접근이나 전화 등을 통해 접근하는 경우(상위기관 사칭, 기술지원 요원 가장) 	<ul style="list-style-type: none"> - 교육과 훈련을 통한 사용자에게 올바른 행동지침 제시 및 인식제고 - 시스템 차원의 대비책을 적절히 병행하여 사용자의 실수를 최소화하는 체계 구축 - 새로운 유형의 사회공학적 해킹에 대해 연구하고 신속하게 대처할 수 있는 정부차원의 체계 구축

사회공학(Social Engineering) 기법 사례

유형	방법	설명
직접적인 접근 (Direct Approach)	권력이용하기	조직에서 높은 위치에 있는 사람으로 가장
	동정심에 호소하기	무척 긴급한 상황에서 도움이 필요한 것처럼 행동
	가장된 인간관계 이용하기	어떤 사람의 친구로 가장해 신뢰감 형성
도청 (Eavesdropping)	도청장치 설치 혹은 유선 전화선의 중간을 따서 도청하거나 유리나 벽의 진동을 레이저로 탐지하여 이를 음성으로 바꾸어 도청	
어깨너머로 훔쳐보기 (shoulder surfing)	공격 대상의 주위에서 직접적인 관찰을 통하여 그가 기업 내에서 수행하는 업무 내역과 전화 통화 내역 등을 어깨 너머로 훔쳐보면서 공격 대상과 관련된 정보들을 수집	
휴지통 뒤지기 (Dumpster Diving)	가정 또는 직장에서 무심코 버리는 메모지, 영수증 또는 업무 중 발생된 자료 등 공격 대상과 관련된 문서들을 휴지통에서 수거하여 유용한 정보들을 수집	
설문조사 (Mail-outs)	공격 대상의 관심을 끌만한 사항을 설문한 후, 공격 대상의 개인적인 취미, 가족사항 등의 개인 정보들과 함께 사회적인 활동과 관련된 다양한 정보를 수집	
Piggybacking (Tailgating)	출입통제 시스템에서 신원이 확인된 앞 사람을 따라 출입	

IV. 해킹의 대응 방안 관물기 템플릿을 1Page로 만들것! 해킹, malware, DDos 든 다 가져다 쓸수 있게!

구분	방법	내용
관리적방안	- 보안정책의 수립, 교육 등을 통한 절차준수 - 보안감사 및 보안 컨설팅 시행	
물리적방안	- 출입통제강화 - 서류 및 파일의 유출 금지 강화	
기술적방안	네트워크 보안	- 방화벽(Firewall) 도입 - IDS(Intrusion Detection System), IPS 도입 - VPN(Virtual Private Network) 도입
	서버보안	- Secure OS, Secure IDS 도입 - OS Patch
	DB 보안	- 사용자인증실시 - 데이터에 대한 접근 권한관리, RBAC
	통합보안	- EAM(Extranet Access Management), ESM(Enterprise Security Management) 등 통합 보안체계 구축

[참고]

가. 악성프로그램 종류 (Malicious Software, Malware)

악성코드	설명
바이러스 (Virus)	- 정상적인 프로그램이나 데이터를 파괴하도록 특수하게 개발된 악성 프로그램(Malicious Program) - 자기 복제를 하며, 파일에 손상을 주거나 하드 디스크의 정보를 파괴하는 등 부작용을 일으킴
웜 (Worm)	- 네트워크를 통해 자신을 복제하고 전파할 수 있는 악성 프로그램 - 단순히 자기 복사 기능만 가진 프로그램으로 시스템 과부하 발생

트로이 목마 (Trojan Horse)	- 겉으로 보기에는 전혀 해를 끼치지 않을 것처럼 보이지만 실제로는 바이러스 등의 위험인자를 포함하고 있는 프로그램 - 자기 복사능력이 없다는 것이 컴퓨터 바이러스와의 차이점
백도어	- 프로그램 개발이나 유지보수, 유사 시 문제 해결 등을 위해 시스템 관리자나 개발자가 정상적인 절차를 우회하여 시스템에 출입할 수 있도록 임시로 만들어 둔 비밀 출입문
스파이웨어	- 다른 사람의 컴퓨터에 잠입하여 개인정보를 빼내거나 광고용으로 사용되는 소프트웨어
악성 봇(Malicious Bot)	- 악성봇은 감염된 컴퓨터에서 일반 프로세스처럼 존재하지만 스스로 움직이지 않고 공격자가 원격으로 제어할 수 있게 만드는 악성코드 - 공격자의 명령에 따라 스팸메일을 전송하게 하거나 분산서비스 방해 공격(DDoS), 또는 정보 유출을 수행
루트킷	-루트킷은 전통적인 UNIX 시스템에서 관리자 계정을 뜻하는root와 소프트웨어 컴포넌트를 뜻하는kit의 합성어로서, 컴퓨터의 관리자 권한을 유지하고 자신의 존재를 운영체제 또는 다른 프로그램으로부터 숨기는 악성코드 유형을 의미

나. 악성프로그램 대응방안

VII. 악성 프로그램 예방대책 및 대응방안

구분	예방대책	설명
관리적 측면	컴퓨터 바이러스 관련 정보속지	컴퓨터바이러스 활동에 대한 달력 및 신종컴퓨터 바이러스에 대한정보를 통하여 감염을예방
	보고체계 정립	ID/PW 적용기준점검 바이러스 보고체계 가동 전문 바이러스업체와의 협조체계구성
	비상시를 대비하여 복구디스크 생성	컴퓨터 바이러스감염에 의한 문제발생에 대비하여 항상 복구디스크를 준비
기술적 측면	최신 버전 백신 프로그램 사용	백신프로그램 사용시항상 최신 버전으로 업데이트하여 사용
	전자메일 첨부파일검사	①메일에 첨부된파일은 반드시 백신프로그램으로 검사한 후 사용 ②출처 및 내용이 분명하지않은 소프트웨어나 파일, 낯선 사람에게서 온메일의 첨부파일 등을 실행시키지않음
	정기적인데이터백업 정품 SW 사용	중요한 데이터는 정기적으로 백업 불법복제 소프트웨어의 사용금지
	Web Server 취약성점검	네트워크 트래픽 점검 및 모니터링 시스템 취약성점검 및 패치적용
	방화벽 활용	방화벽로그를 활용한 백도어 IP 점검 및 조치
	자동감시 기능 사용	백신프로그램의 자동감시기능을 사용하여 시스템을 보호 “끌”

출제문제

회차	과목	교시	문제
모의_2017.07	응용	1	6. IP Spoofing에 대해 설명하시오

토픽	IP Spoofing
키워드	IP 기반 인증 무력화
암기법	

I. IP Spoofing의 개요

가. IP Spoofing 정의

- IP Protocol의 인증 취약점을 악용하여 공격자가 자신의 IP address를 공격하고자 하는 네트워크의 호스트 IP Address로 바꾸어 IP 기반의 인증을 무력화 시키는 공격을 의미

나. IP Spoofing 공격하기 위한 절차

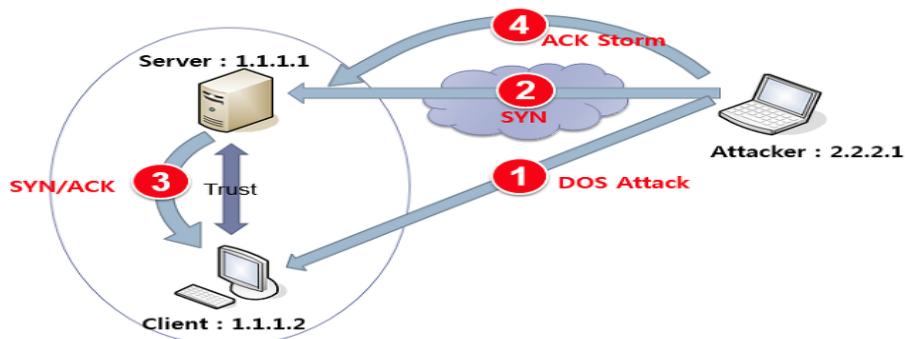
- Target System과 Client는 신뢰관계 형성(ID, Pw 없이 접근)
- IP Protocol 취약점을 습득하기 위해서는 Sniffing 공격이 선행

다. IP Spoofing 공격에서 이용하는 IP Protocol의 취약점

- 인증: IP의 Source address로 상대를 식별 및 인증
-> 암호화 과정이 없고 IP 헤더를 변경 가능
- 세션보호: IP의 Sequence Number로 세션인증
-> Sequence Number는 추측이 가능하게 설계, 이를 이용한 세션 획득

II. 원격지에서 IP Spoofing 공격 원리

가. Sequence Number 획득 이후 상황



1. 공격자는 클라이언트에 TCP SYN Flooding 공격 (rsh, rlogin)
2. 공격자는 클라이언트의 IP로 속여 서버에 연결
3. 서버는 SYN/ACK 패킷을 보내나 클라이언트는 TCP SYN Flooding 공격 때문에 연결이 이루어지지 않아 서버 패킷은 사라지게 된다 (미확인)

4. 공격자는 클라이언트에 ACK 패킷을 보낸 것처럼 속이면서, IP Spoofing 명령어가 들어있는 패킷을 보내 신뢰 관계에 있는 클라이언트라고 속이면 연결이 이루어지게 됨

III. IP Spoofing 공격 방지 대책

- 외부에서 들어오는 패킷 중에서 출발지 IP주소(Source IP Address)에 내부망 IP 주소를 가지고 있는 패킷을 라우터 등에서 패킷 필터링을 사용하여 방어
- 내부사용에 의한 공격은 막을 수 없으므로 각 시스템에서 TCP Wrapper, ssh설치 운영하고 rsh rlogin 등과 같은 인증과정이 없는 서비스는 미사용
- IP Spoofing TCP/IP 설계와 구현의 문제이므로 새 프로토콜을 사용하지 않는 이상 완벽한 보호대책은 존재 할 수 없으므로 지속적인 관리와 점검필요

출제문제

회차	과목	교시	문제

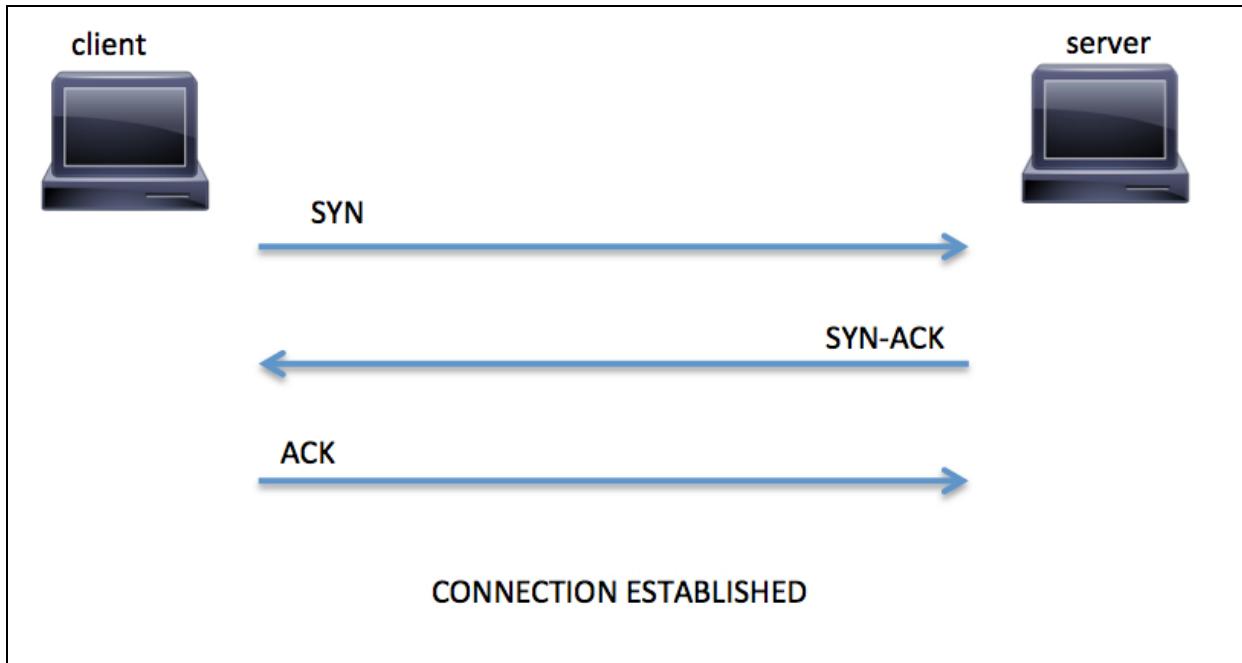
토픽	TCP SYN Flooding
키워드	TCP 프로토콜의 3 Way Handshake 를 악용, Buffer Overflow
암기법	

I. TCP SYN Flooding의 개요

가. TCP SYN Flooding의 정의

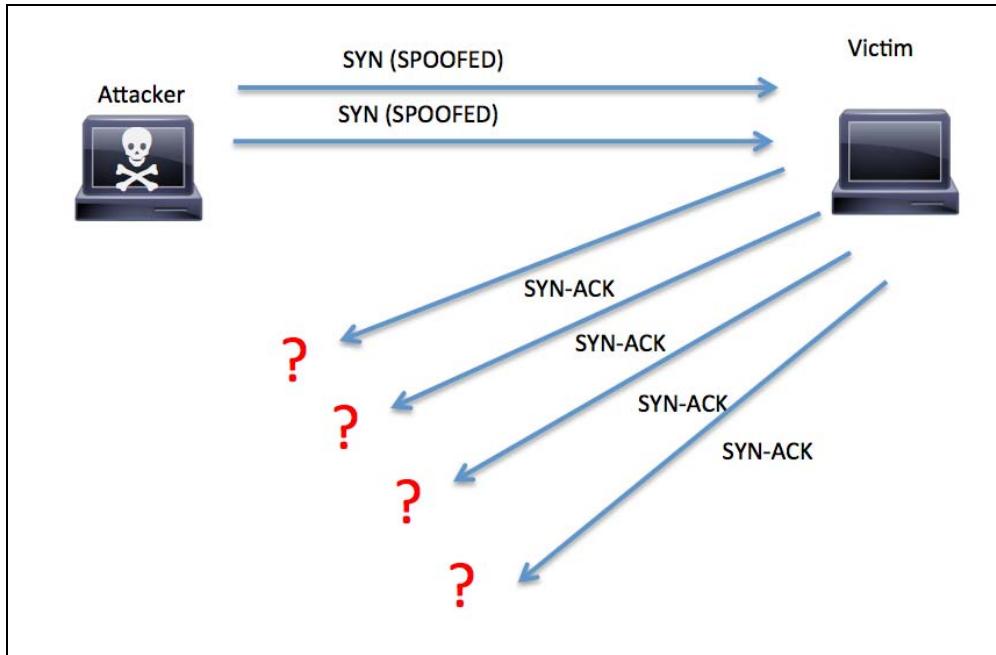
- TCP 프로토콜의 3 Way Handshake를 악용한 Dos (서비스 거부 공격)의 일종
- TCP SYNC/ACK 프로토콜 시퀀스에서 세션 종료를 시키지 않고 계속 유지시켜 부하를 가중시키는 방법

나. TCP 프로토콜의 3 Way Handshake



- 1) 클라이언트는 서버에 SYN (동기화) 메시지를 전송하여 연결을 요청
- 2) 서버는 클라이언트로 SYN-ACK를 전송함으로써 요청을 승인
- 3) 클라이언트는 ACK (확인 응답)에 응답하고, 연결이 설정

II. TCP SYN Flooding 공격 방법



- 1) 공격자는 서버에 접속을 요청하는 SYN 만 수행하고 서버로부터 SYN-ACK 응답을 받은 후 ACK 응답을 보내지 않음,
- 2) 서버는 응답이 올 것을 기다리는 Half Open 상태가 되어 연결이 초기화 대기 전까지 메모리 공간인 백로그 큐(Backlog Queue)에 계속 저장
- 3) 새로운 연결이 들어오면 백로그 큐가 꽉 차게 되어 더 이상 서버의 연결을 받을 수 없는 상태가 됨(서비스 거부상태)

III. TCP SYN Flooding 대처방법

- 1) 백로그 큐를 늘려준다: 임시방편 근본적인 해결방안 아님
- 2) Syncookies 기능을 사용: 변형 3 Way handshake로 TCP헤더 특정부분 암호화
- 3) 시스코 TCP 인터셉트 솔루션 사용

토픽	정보보안 > 해킹 > DoS, DDoS		
----	-----------------------	--	--

출제문제

회차	과목	교시	문제
111	컴시응	4	2.DDoS 공격의 인지, 공격 유형 파악, 공격 유형에 따른 방안에 대하여 설명하시오
99	컴시응	1	5. Slow Read DDos Attack
99	컴시응	3	<p>4. 웹서비스의 응답시간을 줄이고 가용성을 확보하기 위해 웹캐시(Web Cache)가 사용되고 있다.</p> <p>(1) 웹캐시의 사전인출(Prefetching)기법과 유효성 사전확인(Prevalidation)기법에 대해 설명하시오.</p> <p>(2) 동적 웹 콘텐츠에 대한 캐싱처리가 상대적으로 어려운 사유를 설명하시오.</p> <p>(3) 웹캐시 기반 DDoS 사이버 대피소 구축 시 고려해야 할 사항들을 설명하시오.</p>
99	컴시응	4	<p>4. 최근 DDoS 공격이 지능화되면서, 공격트래픽에 대한 신속한 탐지 및 완화(Mitigation)를 어렵게 하고 있다.</p> <p>(1) DDoS 공격유형별(대역폭공격, 세션공격, 웹 HTTP 공격) 피해증상을 설명하시오.</p> <p>(2) DDoS 대응을 위한 Anti-DDoS 시스템의 대응방식을 다음의 2 가지 경우로 나누어 설명하시오.</p> <p>첫째, 공격 IP 가 변조된 경우 인증기능을 통해 대응하는 방식 둘째, 공격 IP 가 변조되지 않은 경우 대응하는 방식</p>
93 회	관리	1 교시	2. DDOS(Distributed Denial of Service) 공격의 유형을 설명하시오
89 회	관리	4 교시	4. 최근 DDOS(Distributed Denial of Service) 공격으로 국가적인 혼란에 직면하였는데, 이런 DDOS 공격에 대한 전용 방법 장비의 종류(두가지 방식)와 증가기적인 대책에 대해 설명하시오.
84	조직	1	1.13. DDOS(Distributed Denial-of-Service attack)
합숙_2017.01	응용	Day-1	8. 보안설정이 미흡한 공유기를 통한 금융정보 유출, DDoS 등의 다양한 공격이 발생하고 있다. 공유기를 통해 발생 가능한 보안 위협과, 이에 대응하기 위해 제조사에서 제품 설계/개발 시 반영해야 할 사항에 대해 설명하시오
합숙_2017.01	공통	Day-3	2. 지난해 10 월 22 일 트위터와 넷플릭스, 뉴욕타임즈, 위싱턴포스트 등과 같은 서비스가 접속이 제대로 이루어지지 않아 많은 불편을 초래하였는데 이는 DNS 서비스를 대상으로 하는 DDoS 공격이였다. 최근 DDoS 공격대상이 DNS 서비스로 전환되고 있는데 DNS(Domain Name System) 구성에 대해 설명하고 DNS 취약점과 DNS를 이용한 서비스 거부(Dos)공격에 대해 설명하시오
합숙_2012.02	공통	5 일차	이동통신 기반의 DDoS
모의_2017.12	관리	2	4. DDoS 공격기법인 Slowloris 와 RUDY 의 개념 및 공격원리에 대해 설명하시오.
모의_2017.01	관리	3	<p>1. 최근 인터넷을 기반으로 사이버상에서 개인정보 유출, 금융사기, DDOS(Distributed Denial of Service) 공격, APT (Advanced Persistent Thread) 공격 등 사이버 위협이 지속적으로 발생하고 있으며, 공격의 형태는 다양하지만 모든 공격에는 악성코드가 원인이 되고 있다. 또한, 기하급수적으로 증가하는 강력한 사이버 공격에 대처하기 위해 사전에 이를 방어할 수 있는 적극적인 방어 기술이 요구되고 있다. 이에 다음에 대해 설명하시오.</p> <p>가. 기존 악성코드 분석 기술의 한계</p>

			나. 사이버게놈(Cyber Genome)의 개념 다. 사이버게놈(Cyber Genome)분석에서 사용되는 주요 기술
모의_2017.01	컴시용	3	6. 지난 10 월 21 일 금요일, 수천만의 분산된 IP 주소에서 대규모 공격이 도메인 서비스 업체인 Dyn 을 덮쳤다. DDoS 공격의 대부분은 보안에 취약한 IoT 기기가 악성 프로그램에 감염되어 공격을 수행한 것으로 파악되었다. 다음 물음에 답하시오. 가. DDoS 공격원리 및 공격유형 나. Slow Read DDoS Attack 과 Slowloris 비교 다. 미라이(Mirai) 봇넷의 동작원리 및 대응방안
모의_2014.11	관리	3 교시	최근 방화벽은 해킹 시도를 탐지하는 것보다 해킹 시도를 차단하는 데 많이 사용된다. 다음 내용에 대해 설명하시오. 가. 해킹사고 분석 관점에서 가장 중요한 방화벽의 기능 나. DDoS 공격시 종점 검토 내용 다. 해킹사고 대응 결과 보고서에 들어가는 내용
모의_2014.11	응용	3 교시	최근 방화벽은 해킹 시도를 탐지하는 것보다 해킹 시도를 차단하는 데 많이 사용된다. 다음 내용에 대해 설명하시오. 가. 해킹사고 분석 관점에서 가장 중요한 방화벽의 기능 나. DDoS 공격시 종점 검토 내용 다. 해킹사고 대응 결과 보고서에 들어가는 내용
모의_2013.12	응용	4 교시	DDoS(Distributed Denial of Service) 공격유형에 따른 시스템 보호와 방어를 위해 사용하는 자원을 향시 모니터링하고 차단정책 수립하고 적용하는 것이 무엇보다 중요하다. DDoS 의 공격 유형별 공격방식을 5 가지 이상 설명하고, 대응 절차와 DDoS 공격유형별 차단정책 적용 방안을 제시하시오.
모의_2013.11	관리	1 교시	DDoS(Distributed Denial of Service) 대응절차 및 공격유형에 따른 대응방안을 설명하시오.
모의_2013.01	응용	1 교시	DrDOS 를 설명하고 DDOS 와 비교하시오.
모의_2010.08	조직	2 교시	4. 정보보호 책임자로 IDC 에서 서비스중인 대규모 시스템에 Anti-DDoS 장비를 도입하고자 한다. Anti-DDoS 시스템 구성방안과 구축 시 고려사항, 구축 완료 후 DDoS 모니터링 방안과 대응체계를 제언하시오.

토픽	DoS, DDoS
키워드	전통필수토픽 DDoS, HTTP Flooding 등
암기법	

I. 대량의 데이터 전송을 통한 서비스 거부 공격 DoS 의 개요

가. 서비스 거부 공격(Denial Of Service)의 정의

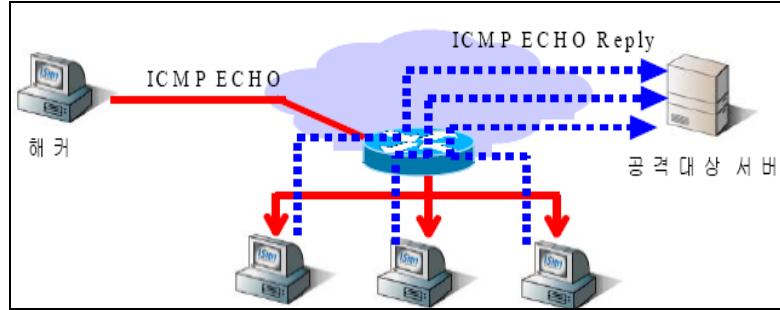
- 정상적인 서비스를 하는 자원을 무리하게 요청해서 원활한 서비스가 제공될 수 없도록 하는 공격

나. 서비스 거부 공격의 형태

공격 형태	내용
시스템 과부하 공격	<ul style="list-style-type: none"> - 프로세스, 네트워크 고갈 공격 - 디스크 채우기 공격
네트워크 서비스 방해 공격	<ul style="list-style-type: none"> - Syn, TCP/UDP Flooding - Smurf, land 공격

다. DoS(Denial of Service) 공격 유형

구분	내용
TCP SYN Flooding 공격	<p>- TCP 프로토콜의 3-Way Hand Shake 악용</p> <pre> graph TD A[Hacker Host A] -- "(1) TCP 연결 요청 (발신: Host C, 수신: Host B)" --> B[Host B] B -- "(2) Host C에 응답" --> C[Host C (Unreachable)] C -- "(3) Host C의 응답이 오지 않음" --> B B -- "(4) TCP 연결 대기 큐가 Overflow 될 때 까지 계속 연결 요청" --> C </pre> <p>① 서버에 수천 개의 TCP 접속(SYN) 요청 메시지를 보냄, 이 때 패킷 내부의 소스 IP 주소를 속이거나 인터넷 상에서 사용하지 않는 IP 주소 값으로 변형</p> <p>② 서버는 위조된 클라이언트 IP 주소로 SYN/ACK 응답을 보낸 후, 클라이언트로부터 ACK가 올 때까지 기다리게 되고, 서버는 ACK 메시지를 받지 못하게 됨</p> <p>③ 서버는 ACK를 받을 때까지 버퍼와 같은 자원을 계속 종료하지 못하고 열어두게 되면서 누적에 따른 <u>시스템 다운 및 서비스 중단하는 상황</u> 직면</p> <p>④ 불완전한 연결을 저장하기 위한 메모리 자료구조의 크기 제한으로 <u>서버 자원이 고갈되어 Buffer Overflow 에러 발생</u></p>
Smurfing DoS 공격	<p>- 광범위한 효과로 인해, 가장 무서운 DoS 방법 중의 하나이며 IP와 ICMP특징을 이용(echo 메시지로 인한 대량 트래픽 발생)</p>



- 직접적인 브로드캐스트와 세가지 구성요소인 공격자, 증폭 네트워크, 표적을 최대한 이용
 - 공격자는 증폭 네트워크의 브로드캐스트 주소로 공격, 서버가 요구하는 것처럼 패킷들의 원본 주소를 위조하여 ICMP ECHO 패킷을 전송하고, ICMP ECHO 패킷을 수신한 증폭 네트워크 내의 모든 시스템은 공격 서버에 응답을 하게 됨
- ※ ICMP(Internet Control Message Protocol): 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고 예러를 알려주는 프로토콜

	<ul style="list-style-type: none"> - 많은 소스로부터 통합된 UDP flood서비스 거부공격을 유발하는데 사용되는 도구 - 몇 개의 서버들과 많은 수의 클라이언트로 이루어짐 - 공격자는 마스터(서버)에게 하나 혹은 여러 개의 IP주소를 대상으로 서비스 거부 공격을 수행하라고 명령을 내리면 마스터는 특정한 기간으로 여러 개의 IP주소를 공격하도록 데몬과 통신함
--	---

II. 명령제어와 좀비 PC를 통한 서비스 거부공격, DDoS의 개요

가. DDoS(Distributed Denial of Service)의 정의

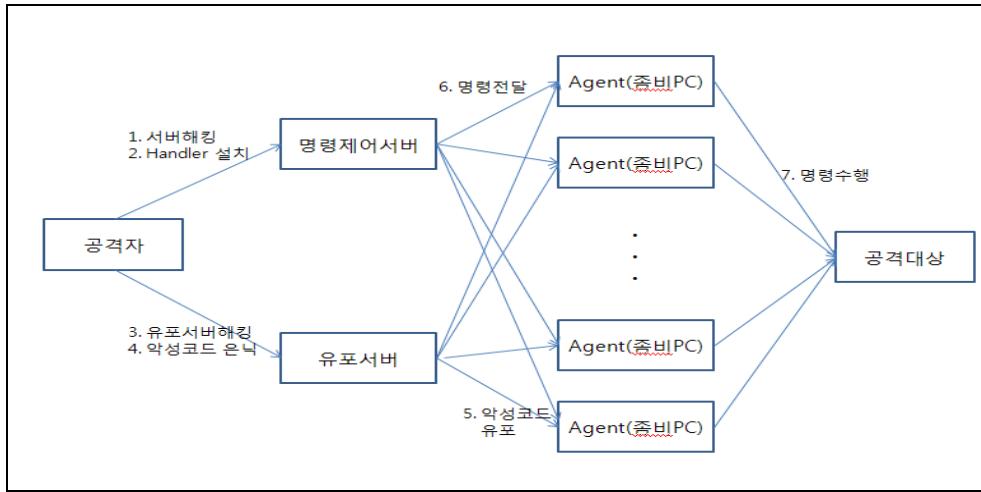
- 서비스에 대한 정당한 접근을 방해하거나 차단하고자 네트워크에 **분산**되어 있는 많은 에이전트를 이용하여 공격대상 서버에 동시에 과도한 서비스 요청을 발생 시키는 공격
- DDoS공격은 주로 해커에 의해서 악성코드 제어서버(Bot C&C)를 통해 감염 PC를 관리하고, 수많은 감염 PC에서 동시에 공격 대상 목표에 막대한 트래픽을 유발시킴

나. DDoS(Distributed Denial of Service)의 특징

특징	설명
온닉 분산공격	<ul style="list-style-type: none"> - 네트워크에 분산되어 분포하는 좀비인 에이전트를 이용하여 공격 - 일반 사용자의 컴퓨터에 온닉한 악성코드를 통해서 사용자가 인식하지 못하는 동안 공격 수행
방어의 어려움	<ul style="list-style-type: none"> - 네트워크에 분산되어 공격함으로써 모든 소스를 차단 어려움 - IP를 위조하거나 에이전트를 변경하여 공격함으로써 차단 어려움
랜섬(Ransom) 공격	<ul style="list-style-type: none"> - 공격자는 DDoS 공격을 통해서 피해자의 서비스를 마비시킨 후, 협박을 통해서 공격중단을 대가로 금전적인 보상을 요구함
대량 좀비PC	대량의 패킷을 발생시킬 좀비 PC 필요, 공격전에 사전에 좀비 PC 확보
Agent 설치	시스템의 네트워크/호스트 취약점을 이용하여 시스템 접근 후 공격용 AGENT 설치
명령제어서버 (C&C)	설치된 AGENT에 대한 공격명령 수행 및 제어

다. DDoS 공격 개념도 및 구성요소

1) 개념도



- 바이러스 악성코드 전파를 위해서 악성코드를 특정 경유지 또는 파일에 감염/해킹하여 배포
- 일반 사용자는 악성코드 경유지에 방문 또는 악성코드 파일을 열면서 사용자 PC도 악성코드에 감염
- 특정시간 공격자에 의한 DDoS 공격 수행 명령
- 특정 사이트에 대한 대규모 공격 진행

2) 구성요소

구성요소	설명
공격자(Attacker)	- DDoS 공격을 주도하는 공격자의 컴퓨터를 의미함
마스터(Master)	- 다수의 DDoS 에이전트의 연결을 관리하는 시스템 - 공격자에게 직접 명령을 받아 에이전트에게 명령 전달을 실행
에이전트(Agent)	- 일반 사용자의 컴퓨터에 익스포하여 마스터에 연결하며 관리되는 악성코드 - 마스터의 명령에 따라 공격 대상에 직접적인 공격하는 시스템

3) 에이전트 유포방식

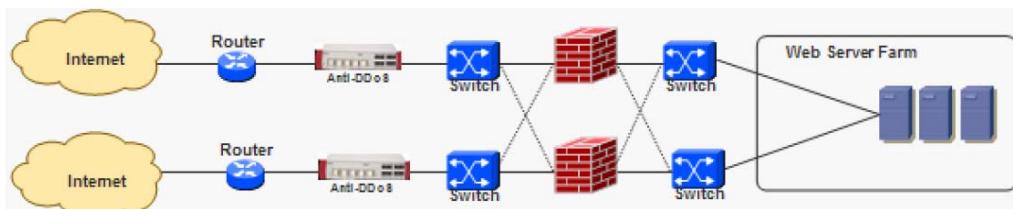
구분	설명
P2P	정상 소프트웨어에 악성코드 (에이전트)를 삽입하여 사용자 설치 유도
웜/바이러스	웜/바이러스의 감염으로 인한 에이전트의 설치
사회공학(Social Engineering)	- 이메일등을 통해서 첨부파일 형태로 사용자에게 전달 후, 설치 유도 - 인간 상호 작용을 이용, 사람을 속여 보안 절차를 깨트리는 비기술적 침입 수단
홈페이지	취약한 웹서버를 해킹한 후, 사용자 방문시 악성코드의 자동 설치

라. DDoS 공격유형 및 대응 방안 (공격영향 쓸수 있어야함)

항목	PPS 증가	웹서비스 저연	대용량 트래픽 전송
사용 프로토콜	TCP	HTTP	UDP/ICMP
공격사례	Syn flooding TCP Connection flooding	HTTP flooding	UDP flooding ICMP flooding
공격형태	64byte이하 크기로 수십만~ 수백만 PPS발생	동일 URL 접속 시도	1000~1500byte 패킷으로 수십 Gbyte 트래픽 발생
공격영향	네트워크 장비, 보안장비, 서버등의 부하 발생	웹서버 부하 발생	회선 대역폭 고갈
피해범위	공격 대상 시스템, 동일 네트워크의 모든 시스템	공격 대상 웹서버	동일 네트워크에 사용중인 모든 시스템
IP Spoofing	변조/실제 IP	실제 IP	변조/실제 IP

분류	방어기술	설명
PPS 증가	비정상 IP 차단	- RFC1918에서 지정한 비공인 IP 차단 - 멀티캐스팅, 사설 IP등 특정 목적을 가진 IP 차단
	공격 IP 차단	- 공격 근원지 IP를 조사하여 IDC/ISP와 공조하여 트래픽의 Null routing(Ignored) 처리를 통한 공격 트래픽 차단
	Syn Proxy 사용	- Syn Proxy/Cookie 기능을 제공하는 보안 장비 및 네트워크 장비를 이용하여 비정상적 TCP 패킷 차단
	장비 패치	- 취약한 네트워크 장비 및 서버에 대한 패치
웹서비스 지연	서버 설정변경	- KeepAlive를 Off로 변경, Maxclient를 최대수치로 조정
	웹서버 증설	- 서비스를 위한 웹서버의 추가를 통한 부하 분산
	공격 IP 차단	- 공격 근원지 IP에 대한 방화벽 또는 라우터에서 차단
대용량 트래픽 전송	불필요한 서비스차단	- 가능한 네트워크 최상단에서 불필요한 UDP 및 ICMP 서비스 차단
	공격 IP 차단	- 공격 근원지 IP를 조사하여 IDC/ISP와 공조하여 트래픽의 Null routing처리를 통한 공격 트래픽 차단
	DNS 서버 다중화	- 다중 DNS 서버를 운영하여 제 3의 등록기관에 DNS 등록

마. Anti-DDoS 솔루션 구성



- 방화벽 앞에 위치, 네트워크 행위기반분석 하는 DDoS 공격 대응 전용시스템 도입

- ※ (실전) 1. ISP업체에 보안개선 (동영상 요구나 과도한 접근 막아달라)
- 2. IDC 센터 차단 요구
- 3. Anit-DDoS 솔루션 구성
- 4. 웹서버, DB용량, CPU증설 등

출제문제

회차	과목	교시	문제
모의_2017.12	관리	2	4. DDoS 공격기법인 Slowloris 와 RUDY 의 개념 및 공격원리에 대해 설명하시오.
모의_2017.01	컴시응	3	6. 지난 10 월 21 일 금요일, 수천만의 분산된 IP 주소에서 대규모 공격이 도메인 서비스 업체인 Dyn 을 덮쳤다. DDoS 공격의 대부분은 보안에 취약한 IoT 기기가 악성 프로그램에 감염되어 공격을 수행한 것으로 파악되었다. 다음 물음에 답하시오. 가. DDoS 공격원리 및 공격유형 나. Slow Read DDoS Attack 과 Slowloris 비교 다. 미라이(Mirai) 봇넷의 동작원리 및 대응방안

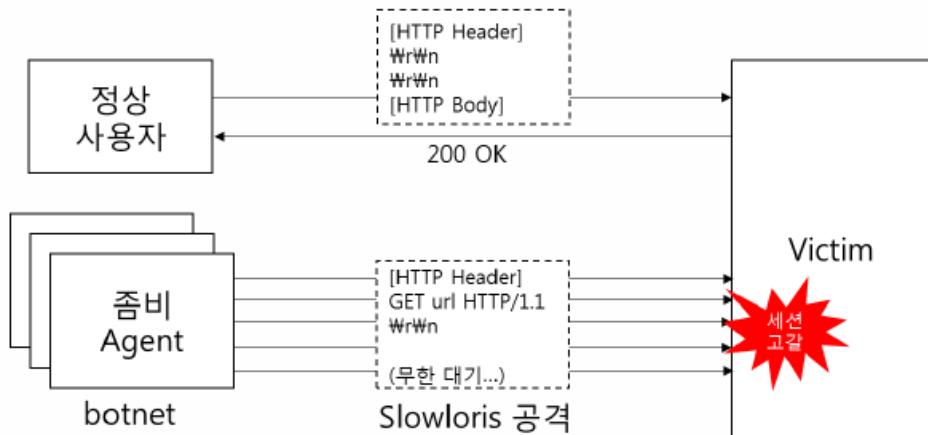
토픽	Slowloris
키워드	웹 서버와 다수의 커넥션을 맺은 후 각 커넥션 별로 완료되지 않은 비정상 HTTP 헤더를 전송함으로써 웹 서버의 커넥션 자원을 고갈 시키는 DDoS 공격 기법
암기법	

I. Slowloris의 개념

- 웹 서버와 다수의 커넥션을 맺은 후 각 커넥션 별로 완료되지 않은 비정상 HTTP 헤더를 전송함으로써 웹 서버의 커넥션 자원을 고갈 시키는 DDoS 공격 기법
- HTTP 프로토콜(RFC 2616)에서 헤더와 바디를 개행문자(CRLF) 2개로 구분한다는 점을 이용한 공격 방법

II. Slowloris의 공격원리와 대응

가. Slowloris의 공격원리



- 정상적인 HTTP GET request는 헤더와 바디를 개행문자(CRLF) 2개로 구분하여 구성.
- Slowloris 공격은 서버와 커넥션을 맺은 후 HTTP request 구성 시 헤더 뒤에 개행문자(CRLF)를 1개만 넣고 대기함
- 결국 서버는 HTTP request가 완성될 때까지 대기하다가 커넥션 자원이 고갈되어 서비스 불가

나. Slowloris에 대한 대응

- HTTP GET 요청에서 CRLF구분자를 1번만 사용하는 패킷을 원천차단(시그니처탐색)
- 최대 동시 접속에 대한 임계치 설정
- User-Agent 필드에 알려진 툴이 명시 되어 있는지 패턴매칭으로 사전 차단
- 웹서버 보안 패치 적용 및 최신버전으로 업그레이드(IIS, Apache 등)
- 많은 패킷을 사용하지 않고도 서비스를 불가능하게 만드는 Application 계층 공격이므로 다양한 측면의 보안 대책 필요.

"끝"

출제문제

회차	과목	교시	문제
모의_2017.12	관리	2	4. DDoS 공격기법인 Slowloris와 RUDY의 개념 및 공격원리에 대해 설명하시오.

토픽	RUDY
키워드	웹 서버와 다수의 커넥션을 맺은 후 각 커넥션 별로 데이터를 매우 느리게 전송함으로써 웹 서버의 커넥션 자원을 고갈시키는 DDoS 공격 기법(RUDY는 R-U-Dead-Yet의 줄임 말)
암기법	

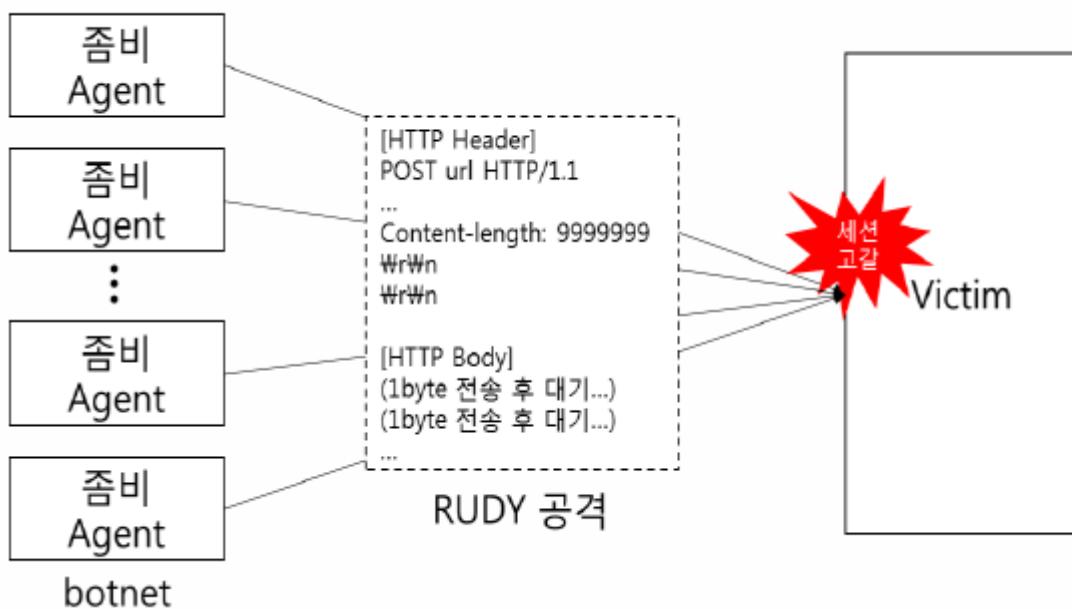
I. RUDY의 개념 및 공격원리

가. RUDY의 개념

- 웹 서버와 다수의 커넥션을 맺은 후 각 커넥션 별로 데이터를 매우 느리게 전송함으로써 웹 서버의 커넥션 자원을 고갈시키는 DDoS 공격 기법(RUDY는 R-U-Dead-Yet의 줄임 말)
- HTTP 프로토콜(RFC 2616)에서 POST method 사용시 헤더에 content-length를 명시하도록 되어 있는데, 이때 데이터 전송에 대한 제약사항이 없는 점을 이용한 공격 방법
- 큰 데이터를 보낼 예정이라고 명시한 후 작은 단위로 전송하여 커넥션을 점유하는 방식

II. RUDY의 공격원리와 대응방안

가. RUDY의 공격원리



- HTTP POST request는 전송할 데이터 사이즈를 헤더의 content-length 필드에 명시
- 웹 서버는 content-length에 명시된 크기만큼의 데이터가 전송될 때까지 커넥션을 맺고 대기
- RUDY 공격은 서버와 커넥션을 맺은 후 content-length에 매우 큰 값을 입력하고, Body에 데이터를 매우 천천히 전송함
- 결국 서버는 데이터 전송을 기다리다가 커넥션 자원이 고갈되어 서비스 불가

나. RUDY의 대응방안

- Content-length 임계치 설정
- Request timeout 설정(실제로 네트워크 상태가 좋지 않아 데이터 전송이 느린 경우도 있으므로 운영 환경에 맞게 설정)
 - 최대 동시 접속에 대한 임계치 설정
 - User-Agent 필드에 알려진 툴이 명시 되어 있는지 패턴매칭으로 사전 차단

- 웹서버 보안 패치 적용 및 최신버전으로 업그레이드(IIS, Apache 등)
- 많은 패킷을 사용하지 않고도 서비스를 불가능하게 만드는 Application 계층 공격이므로 다양한 측면의 보안 대책 필요.

토픽	정보보안 > 해킹 > APT		
----	-----------------	--	--

출제문제

회차	과목	교시	문제
96	관리	3	4. APT(Advanced Persistent Threat) 공격기법과 대응방법에 대하여 설명하시오.
합숙_2016.07	공통	Day-4	1. APT(Advanced Persistent Threat)을 설명하시오.
합숙_2016.01	공통	Day-4	APT 공격 기법이 계속 진화하며 기업 환경에 위협 요소로 부각되고 있다. APT 공격 기법에 대해 설명하고 이를 방어하기 위한 기술과 대응 장비들의 탐지 기법에 대해 설명하시오.
합숙_2015.07	공통	Day-4	주요 APT(Advanced Persistent Threat) 공격유형 및 공격 유형별 대응방안에 대해 기술하시오.
합숙_2015.01	응용	Day-1	최근 해킹, APT 공격 등 기업의 정보시스템에 대한 침입시도가 많아지고 있어 보안관제서비스의 중요성이 높아지고 있다. 보안관제서비스의 의미와 수행하는 업무에 대해서 설명하고, 보안관제에서의 침입탐지 프로세스를 제시하시오
합숙_2015.01	응용	Day-3	최근 APT 공격 등 사이버 공격이 지능화됨에 따라 원인 분석에 수개월 이상이 소요되고 대부분의 공격이 기존 보안장비로 탐지하기 어려워 지면서 네트워크 트래픽을 장기간 보존하고 무결성을 확보하기 위한 사이버 블랙박스 기술이 부각되고 있다. 사이버 블랙박스와 다수의 사이버 블랙박스에서 수집된 정보를 기반으로 인텔리전스한 분석정보를 제공할 수 있는 통합보안상황 분석기술에 대하여 설명하시오
합숙_2012.08	공통	3 일차	APT(Advanced Persistent Threat)
합숙_2012.02	공통	7 일차	최근 국내외적인 보안사고들은 기존의 보안사고와 비교할 때, 개인 해커에 의한 것이 아니라 특수목적의 조직에 의해 시도하여 발생하였다는 특징이 있다. APT(Advanced Persistent Threat) 공격의 개념, 공격기술, 대응방법, APT 공격 사례에 대하여 설명하시오.
합숙_2011.08	공통	7 일차	APT(Advanced Persistent Threat) 공격
모의_2017.01	관리	3	1. 최근 인터넷을 기반으로 사이버상에서 개인정보 유출, 금융사기, DDoS(Distributed Denial of Service) 공격, APT (Advanced Persistent Thread) 공격 등 사이버 위협이 지속적으로 발생하고 있으며, 공격의 형태는 다양하지만 모든 공격에는 악성코드가 원인이 되고 있다. 또한, 기하급수적으로 증가하는 강력한 사이버 공격에 대처하기 위해 사전에 이를 방어할 수 있는 적극적인 방어 기술이 요구되고 있다. 이에 다음에 대해 설명하시오. 가. 기존 악성코드 분석 기술의 한계 나. 사이버게놈(Cyber Genome)의 개념 다. 사이버게놈(Cyber Genome)분석에서 사용되는 주요 기술
모의_2016.05	관리	3 교시	최근 APT(지능형지속위협) 공격에 의해 코드서명 인증서가 탈취되어 이슈화가 되고 있다. 코드서명과 인증기법에 대해 설명하고 이것을 안전하게 보호하기 위한 방안에 대해 설명하시오.
모의_2016.05	응용	3 교시	최근 APT(지능형지속위협) 공격에 의해 코드서명 인증서가 탈취되어 이슈화가 되고 있다. 코드서명과 인증기법에 대해 설명하고 이것을 안전하게 보호하기 위한 방안에 대해 설명하시오.
모의_2016.04	관리	1 교시	10. APT(Advanced Persistent Threat)공격기법에 대해 설명하시오.
모의_2015.12	관리	4 교시	최근 해킹, APT 공격 등 기업의 정보시스템에 대한 침입시도가 많아지고 있어

			보안관제서비스의 중요성이 높아지고 있다. 보안관제서비스의 의미와 수행하는 업무에 대해서 설명하고, 통합보안상황 분석시스템의 개념 및 기술요소를 설명하시오.
모의_2015.12	응용	4 교시	최근 해킹, APT 공격 등 기업의 정보시스템에 대한 침입시도가 많아지고 있어 보안관제서비스의 중요성이 높아지고 있다. 보안관제서비스의 의미와 수행하는 업무에 대해서 설명하고, 통합보안상황 분석시스템의 개념 및 기술요소를 설명하시오.
모의_2015.11	응용	4 교시	귀하는 기업의 보안관리자로서 상황에 따라 적응하는 보안구조(Adaptive Security Architecture)를 설계하고 위협에 대한 감지 및 대응하기 위한 분석기술에 대해 설명하시오.
모의_2015.06	응용	3 교시	최근 금융 A사는 Compliance 대응으로 인해 망 분리 사업을 추진하여 성공적으로 구축 완료하였다. A사의 보안담당자라고 가정하고, 외부 메일을 통한 APT 공격을 예방하기 위한 보안 전략방향 및 구체적인 기반 기술에 대해 기술하시오.
모의_2015.01	응용	4 교시	지능화되는 공격인 APT 공격은 엔드포인트에 유포되는 악성코드의 예방탐지 및 대응이 핵심이다. APT 대응을 위한 방안 중 엔드포인트 보호에 대하여 다음을 설명하시오. 가. 엔드포인트 공격목표 및 기법 나. 평판기반 탐지보안 다. 행위기반 탐지보안
모의_2014.04	응용	3 교시	해킹의 유형별 분류와 최근 해킹공격의 특징인 APT 해킹절차에 대하여 상술하시오.
모의_2013.11	관리	3 교시	APT(Advanced Persistent Threat)가 보안을 크게 위협하고 있다. 다음에 대해서 답하시오. 가. APT 개념을 설명하시오. 나. APT 공격에서 사용할 수 있는 다양한 공격 방법에 대해서 자세히 기술하시오 다. APT 공격에 대응 방안을 제시하시오.
모의_2013.11	응용	3 교시	APT(Advanced Persistent Threat)가 보안을 크게 위협하고 있다. 다음에 대해서 답하시오. 가. APT 개념을 설명하시오. 나. APT 공격에서 사용할 수 있는 다양한 공격 방법에 대해서 자세히 기술하시오 다. APT 공격에 대응 방안을 제시하시오.
모의_2013.07	응용	1 교시	APT(Advanced Persistent Threat)에 대해 설명하시오.
모의_2013.04	응용	4 교시	APT(Advanced Persistent Threat)의 개념 및 공격기법과 대응방법에 대하여 설명하고, ATP 공격대응을 위한 기업에서의 보안관제서비스와 보안활동에 대하여 기술하시오.
모의_2012.11	응용	1 교시	Adaptive HTTP Streaming에 대해 설명하시오.
모의_2012.04	관리	2 교시	APT(Advanced Persistent Threat)의 개념과 특징, 공격기법과 공격기술, 대응방법에 대하여 설명하시오.
모의_2011.10	공통	1 교시	8. APT(Advanced Persistent Threat)에 대하여 설명하시오.

토픽	APT
키워드	침투, 검색, 수집, 유출 Drive by Download(DBD: 드라이브 바이 다운로드)
암기법	

I. 다양한 기술과 기법을 이용한 의도적이고 지속적인 지능형 타깃 공격, APT의 개요

가. APT (Advanced Persistent Threat)의 정의

- 다양한 IT기술과 방식들을 이용해 조직적으로 특정 목적을 위해 다양한 보안 침해 방법들을 생산해 지속적으로 특정 대상에게 가하는 일련의 보안 위협

나. APT의 특징

특 징	설 명
명확한 타겟 (Victim)	APT공격의 목적은 특정 조직이 표적 대상에 대해서 경제적, 정치적, 전략적 이득을 위한 정보를 가져오기 위한 것임. 불특정 다수가 아닌 명확한 표적을 정하여 지속적인 정보 수집 후 공격 감행
지속적	특정조직이 특정목적을 달성하기 위해 끊임없이 새로운 기술과 방식을 지속적으로 이용하여 표적 대상에게 치명적인 손상을 가함.
우회 공격	시스템에 직접 침투하는 것뿐 아니라, 표적내부직원들이 이용하는 다양한 단말을 대상
지능화	한가지 기술만이 아닌 Zero-day 취약점, 악성코드 등 다양한 보안위협공격기술 사용

II. APT의 공격 시나리오 및 공격 기법

가. APT 공격 시나리오

APT 공격 프로세스			
침투 -공격자가 취약한 시스템이나 직원들을 악성코드로 감염시켜 네트워크 내부로 침투	검색 침투한 내부 시스템 및 인프라 구조에 대한 정보를 수집한 후 다음 단계를 계획	수집 보호되지 않은 시스템상의 데이터 수집 또는 시스템 운영 방해	유출 공격자의 근거자료 데이터 전송 시스템운영 방해 또는 장비 파괴

나. APT 공격시나리오에 따른 공격 기법

단계	공격기법	설명
침투 (Incursion)	훔친 인증정보, SQL인젝션, 악성코드 등을 사용하여 오랜 시간에 걸쳐 공격 대상 시스템에 활동 거점을 구축	훔친 인증정보, SQL인젝션, 악성코드 등을 사용하여 오랜 시간에 걸쳐 공격 대상 시스템에 활동 거점을 구축
	관찰 (Reconnaissance)	- 표적대상을 수개월에 걸쳐 철저히 분석 - 최종 목표 달성을 위한 1차 공격대상 탐색
	사회공학 (Social Engineering)	- 신뢰하는 개인, 조직을 가장하는 등 사회공학 기법을 사용하여 악성코드 전송

	제로데이취약점 (Zero-day vulnerabilities)	- 아직 발견되지 않았거나 사용하지 않는 보안 취약점 이용하여 1차 공격 목표에 대해 공격 수행
	수동공격 (Manual Operation)	자동화 대신 각각의 개별 시스템과 사람을 표적으로 삼고, 고도의 정교한 공격을 감행
검색 (Discovery)	APT공격자는 한 번 시스템에 침입하면 목표로 하는 기관의 시스템에 대한 정보를 수집하고 기밀 데이터를 자동으로 검색	
	다중벡터 (Multiple Vector)	APT 공격시 일단 악성코드가 호스트 시스템 내에 구축이 되면 소프트웨어, 하드웨어 및 네트워크의 취약점을 탐색하기 위해 추가적인 공격 툴들을 다운로드
	은밀한 활동 (Run silent, run deep)	APT의 목표는 표적의 내부에 잠복하면서 장시간 정보를 확보 하는 것이므로, 모든 검색 프로세스는 보안탐지를 회피하도록 설계됨
	연구 및 분석 (Research and analysis)	정보 검색은 네트워크 구성, 사용자 아이디 및 비밀번호등을 포함하여 확보된 시스템과 데이터에 대한 연구 및 분석을 수반함
수집 (Capture)	보호되지 않은 시스템의 데이터는 공격자에게 노출	
	은닉 (Convert)	1차 공격 성공후, 정상이용자로 가장하여 정보수집 및 모니터링 활동을 진행
	권한상승 (privilege escalation & lateralization)	시스템 접근을 위한 시스템 접근 권한을 가진 직원에 대한 계정정보를 수집하기 위한 각종 접근 행위. *Brute Force Attack : 계정정보 수집
제어 (Control)	APT 공격자는 표적 시스템의 제어권한을 장악하며, 각종 기밀 데이터를 유출하여 SW 및 HW에 손상을 입힘	
	유출 (Exfiltration)	기밀데이터가 웹메일 또는 암호화된 패킷, 압축파일의 형태로 공격자에게 전송
	중단 (Disruption)	APT 공격자는 원격시동이나 SW, HW 시스템을 자동종료할 수도 있음
	적응/지속	시스템 최종목표 정보획득 후 지속적 모니터링, 장기적 정보유출 - 지속적 접근이 가능하도록 다양한 백도어 설치

III. APT 공격 사례

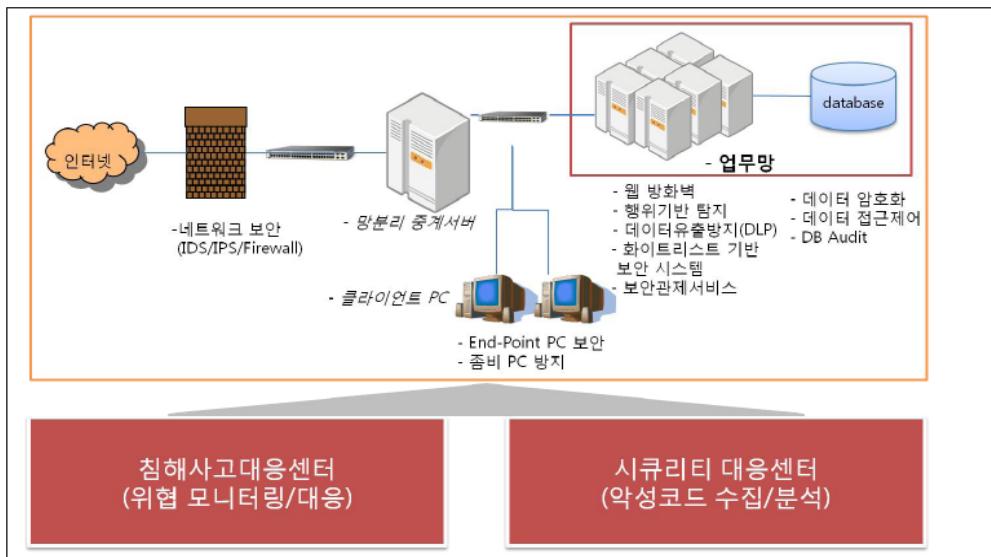
사례	내용
스턱스넷 (Stuxnet)	2010년 7월 이란 원자력 발전소 작동을 방해한 악성코드로 SCADA[Supervisory Control And Data Acquisition] 시스템을 임의로 제어하는 데 사용됨. 이 악성코드를 내부 폐쇄망에서 다른 시스템들로 유포하기 위해 여러 개의 취약점을 사용함. 원자력 발전소 내부에서 사용하는 독일 지멘스 소프트웨어의 구조를 정확하게 파악하여 관련 파일을 변조함.
오퍼레이션 오로라	2011년 1월 구글 본사는 기업 내부에 외부로부터 침해 사고 발생을 공개함. 이 공격은 구글 외에 어도비, 주니퍼, 야후 등 34개 업체를 공격 대상으로 함. 공격 목적은 기업 내부 첨단 기술 관련 기밀 데이터의 탈취였음. Internet Explorer의 제로 데이[Zero Day] 취약점이었던 MS10-002[CVE-2010-0249]를 악용했으며, 기업 임직원에게 취약한 웹 페이지의 주소를 전송해 악성코드에 감염되게 함.

나이트 드래곤	나이트 드래곤 공격은 2009년 11월 무렵부터 최소 1년 이상 카자흐스탄, 그리스, 대만과 미국에 위치한 글로벌 오일, 가스 및 석유 화학 업체를 대상으로 조직적으로 진행된 것으로 알려짐. 웹 서버 해킹, 악성코드 제작 및 유포, 그리고 다양한 해킹 툴이 사용됨.
EMC/RSA 공격	2011년 3월 EMC/RSA 보안 사업 본부가 외부의 침입을 당해 인증 관련 정보가 외부로 유출되었다는 사실이 공개됨. 이 공격은 SNS를 이용해 공격 목표에 대한 정보를 수집하고, 사회공학 기법을 이용해 공격 목표에 악성코드를 감염시킨 후 범용 소프트웨어의 알려지지 않은 제로데이 취약점 등을 이용해 정보를 유출한 것임

IV. APT 대응방법

가. APT 대응 체계

- APT 공격은 지능적이며, 고도의 기술력을 기반으로 행해지는 공격이므로, End-to-End로 전방위적인 보안체계 수립이 필요하며, 망분리와 요소기술을 기반으로 안전한 시스템 아키텍처를 제시함
- 또한 침해사고 대응센터와 시큐리티 대응센터를 분리, 운영하여, 예방과 대응활동을 균형있게 추진



나. APT 대응 활동

- APT 발생 이전과 이후로 나누어, 위험예방전략, 악성코드 유입 최소화, 악성코드 감염예방, 데이터 유출 예방, 위험탐지와 대응활동 등을 수행

시기	활동	내용
위험발생 이전 (시큐리티 대응센터)	위험 예방 전략 수립	<ul style="list-style-type: none"> - 보안관제 수행 - 위험분석 수행 - 보안전략 유효성 분석
	악성코드 유입 최소화	<ul style="list-style-type: none"> - 보안 인식 교육 수행 - 지속적 보안 업데이트 관리 - 보안 소프트웨어 설치 및 운영
위험발생 이후 (침해사고 대응센터)	악성코드 감염 예방	<ul style="list-style-type: none"> - 어플리케이션 화이트리스트 - 접근 권한의 최소화 - 네트워크 접근 제한 및 분리 - 신원확인 및 접근 권한관리
	데이터 유출 예방	<ul style="list-style-type: none"> - 중요 데이터 보호 - 중요 데이터 유출 예방

시기	활동	내용
	위험 탐지와 대응	<ul style="list-style-type: none">- 호스트 및 네트워크 이상징후 탐지- 침해사고 대응 프로세스 수행- 침해사고 포렌식 프로세스 수행

“끝”

토픽	정보보안 > 해킹 > 랜섬웨어(Ransomware)		
----	------------------------------	--	--

출제문제

회차	과목	교시	문제
113	관리	3	3. 랜섬웨어 공격에 대하여 사전, 사후적 대응방안을 기술적, 관리적 관점에서 설명하시오.
110	컴시응	1	11. 랜섬웨어(Ransomware)에 대해 설명하시오.
107 회	관리	1	5. 랜섬웨어(Ransomware)를 정의하고, 감염경로와 방지방법을 제시하시오.
104	관리	1	3. 랜섬웨어(Ransom ware)와 파밍(Parming)에 대해 설명하시오.
합숙_2017.08	공통	Day-1	3. 랜섬웨어 및 가상화폐 투자 과열로 인해 비트코인이 주목 받고 있고, 비트코인의 단점을 보완해 스마트계약 및 분산 어플리케이션이 가능한 이더리움이 큰 성공을 거두고 있다. 비트코인의 구조 및 비트코인의 단점에 대해 설명하고, 이를 보완한 이더리움에 대해 설명하시오.
합숙_2017.08	응용	Day-5	7. 2017년 5월 전세계를 강타한 랜섬웨어 워너크라이(WannaCry)의 공격방법과 대응방법에 대해 설명하고, 랜섬웨어를 대응하기 위한 예방방법을 제시하시오.
합숙_2017.01	공통	Day-3	3. 최근 랜섬웨어에 의한 기업 피해가 증가하고 있다. 이와 관련하여 다음 질문에 답하시오. 가. 랜섬웨어의 침투 경로 및 공격 기법 나. 기업보안 관점에서의 랜섬웨어 대응 방안
합숙_2016.07	공통	Day-4	4. 랜섬웨어의 감염경로 중 하나인 멀버타이징(Malvertising)에 대하여 설명하고 대응 방안을 제시하시오
합숙_2016.01	관리	Day-1	최근 국내에서 랜섬웨어로 인한 피해가 급증하고 있다. 신 변종 랜섬웨어가 지속적으로 발견되고 있으며 기업뿐만 아니라 개인 사용자에게까지 피해가 확산되고 있다. 랜섬웨어(Ransomware)의 특징과 감염경로, 공격절차 및 대응방안에 대해 설명하시오.
합숙_2015.07	공통	Day-3	1. 랜섬웨어와 랜섬웹에 대해 설명하시오.
합숙_2013.01	공통	2 일차	악성코드 유형 중 랜섬웨어(Ransom ware)에 대해 설명하시오.
모의_2017.07	관리	2	1. 2017년 5월 전세계를 강타한 랜섬웨어 워너크라이(WannaCry)의 공격방법과 대응방법에 대해 설명하고, 랜섬웨어를 대응하기 위한 예방방법을 제시하시오.
모의_2016.10	응용	2 교시	2. 최근 랜섬웨어는 다양한 형태의 변종을 중심으로 빠르게 진화하고 있다. 다음에 질문에 대해 설명하시오. 가. 변종 랜섬웨어의 종류와 특징 나. 랜섬웨어의 감염경로 다. 대응방안
모의_2016.06	관리	2 교시	랜섬웨어의 공격 기법이 갈수록 진화하고 있다. 랜섬웨어의 유형과 최근 이슈가 되는 멀버타이징(Malvertising)에 대해 설명하고 랜섬웨어를 대응하기 위한 방법을 제시하시오.
모의_2016.06	응용	2 교시	랜섬웨어의 공격 기법이 갈수록 진화하고 있다. 랜섬웨어의 유형과 최근 이슈가 되는 멀버타이징(Malvertising)에 대해 설명하고 랜섬웨어를 대응하기 위한 방법을 제시하시오.

모의_2016.01	응용	3 교시	사이버공격이 지능화됨에 따라 다양한 방법으로 공격이 되고 있다. 최근 이슈가 되는 DBD(Drive by Download)와 랜섬웨어에 대해 설명하고 각각의 대응방안을 설명하시오. 그리고 사이버공격에 대한 보안강화 및 능동적 대응을 위한 보안 네트워크를 구성하시오.
모의_2015.12	응용	4 교시	최근 랜섬웨어는 개인 PC 부터 서버 그리고 모바일까지 그 영향 범위를 확대하고 있으며 다양한 형태의 변종을 만들어내는 등 빠르게 진화하고 있다. 이러한 변종 랜섬웨어의 종류와 특징, 대응방안에 대해서 설명하시오.
모의_2015.07	관리	1 교시	11. 랜섬웨어(Ransomware)의 공격방식과 대응방안에 대해 설명하시오.

토픽	랜섬웨어(Ransomware)
키워드	금품 요구 악성프로그램, 감염경로, 종류와 특징, 대응방안 - Drive-by-Download, 워터링홀, Spear Phishing, 사회공학적공격
암기법	

I. 컴퓨터 사용자의 파일의 암호화를 수행한 후 복호화를 위한 금품 요구, 랜섬웨어의 개요

가. 랜섬웨어(Ransomware)의 정의

- Ransom(몸값)과 Software(소프트웨어) 합성어로, PC에 있는 중요한 자료를 암호화 후, 피해자에게 돈을 지급 하도록 강요하는 악성코드
- 인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레드시트, 그림 파일 등을 암호화해 열지 못하도록 만든 후 돈을 보내주면 해독용 열쇠 프로그램을 전송해 준다면 금품을 요구하는 악성 프로그램

나. 랜섬웨어의 특징

특징	설명
사회공학 기법	랜섬웨어의 배포를 위한 사회공학적 기법을 주로 사용 대표적인 사례로 이메일을 통한 랜섬웨어 배포
금품 요구	사용자의 파일을 암호화하여 접근할 수 없도록 한 후 복호화 프로그램의 제공을 위한 금품 요구
암호화	사용자의 PC에 저장되어 있는 문서나 이미지 파일 등을 대상으로 암호화 수행

II. 랜섬웨어의 공격프로세스, 공격기법 및 분류

가. 랜섬웨어의 공격프로세스



- 랜섬웨어는 이메일을 통해 배포되면 일부는 AntiVirus를 우회하기 위해 설치 이후 암호화 모듈을 다운로드 받아 수행함.

나. 랜섬웨어의 공격 기법

기법	설명
이메일	- 사용자의 PC에 랜섬웨어를 설치하기 위한 설치 파일 혹은 프로그램을 배포 시 이메일을 이용
위변조된 웹사이트	- 자주가는 웹사이트에 악성코드 삽입 후 사이트 접속 시 감염시킴 - OS나 SW취약점을 통해 웹사이트 변조 후 방문 시 악성코드 유포
첨부파일/악성코드 실행	- 사회공학적 접근 방식, 첨부파일, 악성코드 실행 유도

다. 랜섬웨어의 분류

구분	상세설명
심플로커 (SimpleLocker)	모바일 랜섬웨어의 일종으로 스마트폰의 사진이나 동영상, 문서를 암호화 후 금전 요구.
크립토락커 (CryptoLocker)	피해자 PC의 파일을 암호화한 후 비트코인이나 현금을 요구, 돈을 보내지 않으면 이를 풀어주지 않겠다고 협박
스케어웨어 (Scareware)	가장 단순한 형태의 악성코드로 대체로 가짜 안티바이러스 프로그램이나 바이러스 제거 툴로 위장해 PC에 문제가 많으니 돈을 내고 이를 고쳐야 한다고 경고
락-스크린 (Lock-Screen)	감염되면 PC를 전혀 사용 할 수 없고, 일반적으로 풀 사이즈 원도 창을 여러 개 띄워 FBI나 사법부 로고를 박아놓고 불법 다운로드 등으로 법을 어겼으니 벌금을 내야 한다며 협박

III. 랜섬웨어의 대응 방안

구분	항목	대응 방안
관리적 측면	이메일 관리	알 수 없는 발신자가 보낸 이메일의 첨부파일을 열 때 주의를 기울일 필요 있음
	AntiVirus	AntiVirus의 주기적인 업데이트 필수
기술적 측면	랜섬웨어 제거	시스템의 주요 서비스 동작을 수행하지 않는 모드로 디바이스를 동작시켜 랜섬웨어를 식별하여 제거
	백업	주기적인 시스템 백업을 수행하여 랜섬웨어 설치 이전의 시점으로 복원 가능
	복호화키 추출	- 랜섬웨어를 분석하여 프로그램 내에서 복호화키를 추출 - RSA와 같은 비대칭키 암호화 기술은 암호화키와 복호화키가 서로 달라 사실상 암호화된 파일의 복호화는 불가능

- 랜섬웨어에 대한 원천적인 대응은 불가능하기 때문에 출처가 불명확한 프로그램은 실행하지 않아야 함.

토픽 이름	사회공학(Social Engineering)
키워드(암기)	인간관계, 신뢰, ROI, 사회공학사이트, 사회적 관계, 공격적 위협, 보안의식 포렌식, 유대관계기반, 컴퓨터기술 기반
암기법	

기출문제

번호	문제	회차
1	보안학적 측면에서의 사회공학(Social Engineering)	114.정보관리.1

참고 사이트 : <http://blog.lgcns.com/1330>

I. 신뢰기반의 해킹 방법, 사회공학기법의 개요

가. 사회공학(Social Engineering) 기법의 정의

- 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여 정상 보안 절차를 깨트리기 위한 비기술적 침입 수단

사람과 사람 사이에 존재하는 기본적인 신뢰를 바탕으로 공격을 하거나 원하는 정보를 취득하는 행위

나. 사회공학기법에 취약한 조직

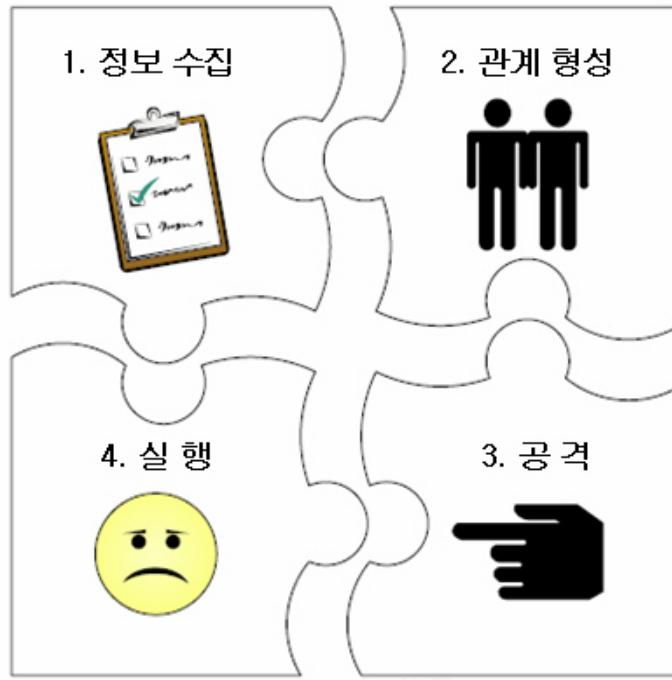
- 조직원 수가 많은 조직
- 조직의 구성체가 여러 곳에 분산되어 있는 조직
- 조직원의 개인정보가 노출된 조직
- 적절한 보안 교육이 부재된 조직
- 정보가 적절히 분류되어 관리되지 않는 조직

다. 사회공학 공격의 대상

- 정보의 가치를 잘 모르는 사람
- 특별한 권한을 가진 사람
- 제조사, 벤더
- 해당 조직에 새로 들어온 사람

II. 사회공학 기법의 공격 흐름도 및 절차

가. 사회공학 기법의 공격 흐름도



나. 공격 절차

공격 절차	설명	방법
정보수집 Information Gathering	- 공격자는 제일 먼저 공격 대상과 관련된 가족 관계, 직장 생활 그리고 사회 모임 등의 개인적이거나 사회적인 활동 등과 관련된 다양한 정보들의	- 직접적인 접근(Direct Approach) - 어깨너머로 훔쳐보기(Shoulder Surfing) - 휴지통 뒤지기(Dumpster Diving) - 설문 조사(Mail-outs) - 시스템 분석(Forensic analysis)

	<p>수집을 시도</p> <ul style="list-style-type: none"> - 공격자는 이 단계에서 수집한 다양한 정보들을 다음 단계인 관계 형성(Developing Relationship)을 위해서 사용 	<ul style="list-style-type: none"> - 인터넷(Internet)
관계 형성 Developing Relationship	<ul style="list-style-type: none"> - 인간 기반(Human Based) 또는 컴퓨터 기반(Computer Based)의 수단들을 공격자는 적절하게 활용하여 공격 대상에게 접근 - 관계 형성 단계에서는 가장(假裝, Masquerade)이라는 것이 공격자에 의해 발생 	<ul style="list-style-type: none"> - 중요한 인물(Important User) - 도움이 필요한 인물(Helpless User) - 지원 인물(Support Personnel) - 역 사회 공학(Reverse Social Engineering)
공격 Exploitation	<ul style="list-style-type: none"> - 공격자가 수집한 다양한 정보들을 바탕으로 공격 대상과 충분한 신뢰감을 형성하였다고 판단 할 경우에 진행 - 이 세 번째 단계로 넘어가기 위해서는 공격자 자신을 공격 대상이 더 이상 의심하지 않는다는 판단이 중요하게 작용 	<ul style="list-style-type: none"> - 의견 대립 회피 - 사소한 요청에서 큰 요청으로 발전 - 감정에 호소 - 신속한 결정
실행 Execution	<ul style="list-style-type: none"> - 공격 대상은 공격자가 요청한 사항에 대해 직접적인 실행으로 옮김으로써 이로 인해 실질적인 피해가 발생 - 공격자는 요청 사항으로 인해 확보한 유형의 또는 무형의 자산을 이용하여 실질적인 목적을 수행 	<ul style="list-style-type: none"> - 책임 회피 - 보상 심리 - 도덕적 의무감 - 사소한 문제

III. 사회공학 기법의 유형

가. 인간기반 사회공학 기법(Human Based Social Engineering)

유형	방법	설명
직접적인 접근 Direct Approach	권력이용하기	<ul style="list-style-type: none"> - 조직에서 높은 위치에 있는 사람으로 가장하여 정보를 획득
	동정심에 호소하기	<ul style="list-style-type: none"> - 무척 긴급한 상황에서 도움이 필요한 것처럼 행동, 예를 들면, 어떤 업무를 처리하지 못하면 자신이 무척 난처해지며 정상적인 절차를 밟기가 곤란하다고 호소
	가장된 인간관계 이용하기	<ul style="list-style-type: none"> - 조직내의 개인정보를 획득하여, 어떤 사람의 친구로 가장해 상대로 하여금 자신을 믿도록 한 뒤 정보를 획득
도청 Eavesdropping	<ul style="list-style-type: none"> - 도청 장치를 설치하거나 유선 전화선의 중간을 따서 도청 - 유리나 벽의 진동을 레이저로 탐지하여 이를 음성으로 바꾸어 도청 - 휴대폰도 도청이 가능 	
어깨너머로 흡쳐보기 shoulder surfing	<ul style="list-style-type: none"> - 공격 대상의 주위에서 직접적인 관찰을 통하여 그가 기업 내에서 수행하는 업무 내역과 전화 통화 내역 등을 어깨 너머로 흡쳐보면서 공격 대상과 관련된 정보들을 수집하는 방식 	
휴지통 뒤지기 Dumpster Diving	<ul style="list-style-type: none"> - 가정 또는 직장에서 무심코 버리는 메모지, 영수증 또는 업무 중 생성한 문건 등 공격 대상과 관련된 문서들을 휴지통에서 수거하여 유용한 정보들을 수집하는 방식 	

설문조사 Mail-outs	- 공격 대상의 관심을 끌만한 사항을 설문지로 작성한 후 이 설문조사를 통하여 공격 대상의 개인적인 취미, 흥미 사항, 가족 사항과 관련된 개인정보들과 함께 동호회 활동과 같은 사회적인 활동과 관련된 다양한 정보를 수집하는 방식
Piggybacking(Tailgating)	- 출입통제 시스템에서 신원이 확인된 앞 사람을 따라 들어가 신원 확인을 피하는 방식

나. 컴퓨터 사회공학 기법(Computer Based Social Engineering)

유형	설명
시스템 분석 Forensic analysis	- 공격 대상이 사용하는 컴퓨터 시스템에 공격자는 직접적이거나 간접적인 접근을 통하여 해당 컴퓨터 시스템에 존재하는 공격 대상이 작성한 다양한 문서들 그리고 웹 사이트 방문 기록 등 온라인상에서의 활동과 관련된 다양한 정보들을 수집하는 방식
악성소프트웨어 전송	- 서비스를 제공하는 사이거나 벤더인 것으로 가장하여, 악성 코드를 패치인 것처럼 공격 대상에게 발송할 수 있음 - 가까이에 있는 사람이라면 악성 코드를 CD나 USB 메모리에 담아 그 사람의 시스템에서 몰래 실행시키는 것만으로도 충분히 가능
인터넷을 이용한 공격	- 인터넷에 존재하는 다양한 검색 엔진을 이용하여 인터넷에 존재하는 공격 대상과 관련된 개인정보 및 사회 활동과 관련된 다양한 정보를 수집하는 방식 - 이름, 소속 회사, 직책, 주민등록 번호, 주소, 전화번호, 이메일 ID 획득 가능
피싱 Phishing	- 개인정보(Private Data)와 낚시(Fishing)의 조합으로 개인정보를 불법으로 도용하기 위한 속임수의 한 유형 - 일반적으로 피싱은 이메일을 통해서 이루어짐
파밍 Pharming	- 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나, DNS(도메인네임시스템) 이름을 속여 사용자가 진짜 사이트로 오인하도록 유도하여 개인정보를 훔치는 수법

IV. 사회공학 기법의 방어의 어려움 및 대응전략

가. 방어의 어려움

- 공격 기법의 대상이 바로 사람이기 때문에 100% 완벽한 방어는 불가능
- 보안에서 가장 취약한 부분은 사람(Human being is the weakest link in a security system)
- 완벽에 가까운 물리적 보안(Physical Security) 및 시스템 보안(System Security) 그리고 보안 정책(Security Policies)을 모두 갖추고 있다고 하더라도 사람은 외부에서 걸려온 전화 한 통화로 인해 이 모든 것을 우회할 수 있는 방법을 외부에 제공 해 줄 수도 있음
- 사회공학 기법을 이용한 공격의 성공을 어렵게 할 수 있는 전략을 수립하는 것이 현실적인 방안

나. 단계별 대응 전략

대응 전략	설명	방법
정보 수집 (Information Gathering) 단계에서의 대응	- 공격자가 공격 대상과 관계 형성(Developing Relationship)에 있어서 필수적인 요소인 관련 정보들을 수집하는 것을 사전에 어렵도록 하는 것이 목적 - 공격자가 사회 공학 공격 흐름의 2단계인 공격 대상과의 관계 형성(Developing Relationship)이 가능해지는 것 자체를 방해하는 것이 주된 목적	- 개인 신상 정보와 관련한 문서 관리 철저 - 온라인상의 개인 정보 관리 철저

공격(Exploitation) 단계에서의 대응	<ul style="list-style-type: none"> - 공격자가 자신의 특수한 목적을 수행하기 위한 사항을 요청하더라도 공격 대상이 이를 거부함으로써 실행(Execution)되지 않도록 방해하는 것이 주된 목적 	<ul style="list-style-type: none"> - 사회 공학 기법의 공격 형태 인지 - 배경 조사(Background Check)
실행(Execution) 단계에서의 대응	<ul style="list-style-type: none"> - 공격 대상이 공격자의 특수한 목적을 위한 요청 사항을 이미 수행하였으므로 보안 사고 예방 차원에서의 접근이 아니라 사고 대응(Incident Response) 차원에서 접근 - 유출된 정보를 공격자가 특수한 목적으로 활용하지 못하도록 하여 피해를 최소화하는 것이 목적 	<ul style="list-style-type: none"> - 신속한 관계 기관 신고

"끝"

"The Biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you."

"기업 정보 보안에 있어서 가장 큰 위협은 컴퓨터 바이러스, 패치가 적용되지 않은 중요한 프로그램이나 잘못 설정된 방화벽이 아니다. 가장 큰 위협은 바로 당신이다."

케빈 미트닉(Kevin Mitnick)

4

APT(Advanced Persistent Threat) 공격기법과 대응방법에 대하여 설명하시오.

출제 도메인	- 보안
주요 키워드	- 스톡스넷, 공격프로세스(침투, 검색, 수집, 유출), 공격기법(제로데이공격 등), 대응방안
난이도	★ ★ ★ ☆ ☆ (별5개 기준)
참고 자료	- APT 공격의 비밀을 파헤치다.(안철수연구소 보안매거진 월간 “安”) - 차세대 보안위협과 대응방안(시만텍)
문제 소견	-
기출 풀이 담당 기술사	- 이 총 현 (제95회 정보관리기술사, skytango@naver.com)

1. “다양한 기술과 기법을 이용한 의도적이고 지속적인 보안 위협”, Advanced Persistent Threat의 개요

가. “지능형 타깃 위협”, Advanced Persistent Threat의 정의

Advanced	보안 위협을 제작하기 위해, 한 가지에만 제한된 것이 아닌 광범위한 많은 기술을 사용하는 것을 의미함
Persistent	보안 위협을 행하는 주체는 특정한 목적을 가지며, 그 목적이 달성될 때까지는 공격대상에게 끊임 없이 지속적으로 공격을 가하는 것을 의미함
Threat	악성코드, 취약점공격, 해킹과 사회공학기법 등 공격대상에게 “위협”을 끼치는 것을 의미
- 다양한 IT 기술과 방식들을 이용해 조직적으로 경제적이거나 정치적인 목적을 위해 다양한 보안 위협들을 생산해 지속적으로 특정대상에게 가하는 일련의 보안 위협 행위	

나. Advanced Persistent Threat의 대표적인 사례

- APT의 대표적인 사례로는 스톡스넷, 오퍼레이션 오로라, 나이트 드래곤, EMC/RSA 공격 등이 있으며, 피해의 영향도가 큰 대형사고가 많음.

사례	내용
스ток스넷 (Stuxnet)	2010년 7월 이란 원자력 발전소 작동을 방해한 악성코드로 SCADA[Supervisory Control And Data Acquisition] 시스템을 임의로 제어하는 데 사용됨. 이 악성코드를 내부 폐쇄망에서 다른 시스템들로 유포하기 위해 여러 개의 취약점을 사용함. 원자력 발전소 내부에서 사용하는 독일 지멘스 소프트웨어의 구조를 정확하게 파악하여 관련 파일을 변조함.
오퍼레이션 오로라	2011년 1월 구글 본사는 기업 내부에 외부로부터 침해 사고 발생을 공개함. 이 공격은 구글 외에 어도비, 주니퍼, 야후 등 34개 업체를 공격 대상으로 함. 공격 목적은 기업 내부 첨단 기술 관련 기밀 데이터의 탈취였음. Internet Explorer의 제로 데이[Zero Day] 취약점이었던 MS10-002[CVE-2010-0249]를 악용했으며, 기업 임직원에게 취약한 웹 폐이지의 주소를 전송해 악성코드에 감염되게 함.
나이트 드래곤	나이트 드래곤 공격은 2009년 11월 무렵부터 최소 1년 이상 카자흐스탄, 그리스, 대만과 미국에 위치한 글로벌 오일, 가스 및 석유 화학 업체를 대상으로 조직적으로 진행된 것으로 알려짐. 웹 서버 해킹, 악성코드 제작 및 유포, 그리고 다양한 해킹 툴이 사용됨.
EMC/RSA공격	2011년 3월 EMC/RSA 보안 사업 본부가 외부의 침입을 당해 인증 관련 정보가 외부로 유출되었다는 사실이 공개됨. 이 공격은 SNS를 이용해 공격 목표에 대한 정보를 수집하고, 사회 공학 기법을 이용해 공격 목표에 악성코드를 감염시킨 후 범용 소프트웨어의 알려지지 않은 제로데이 취약점 등을 이용해 정보를 유출한 것임

2. Advance Persistent Threat의 공격기법

가. Advanced Persistent Threat의 공격 프로세스

- APT 공격 프로세스는 침투, 검색, 수집, 유출의 단계를 거쳐 진행되며, 각각의 단계별로 다양한 공격기법을 활용함



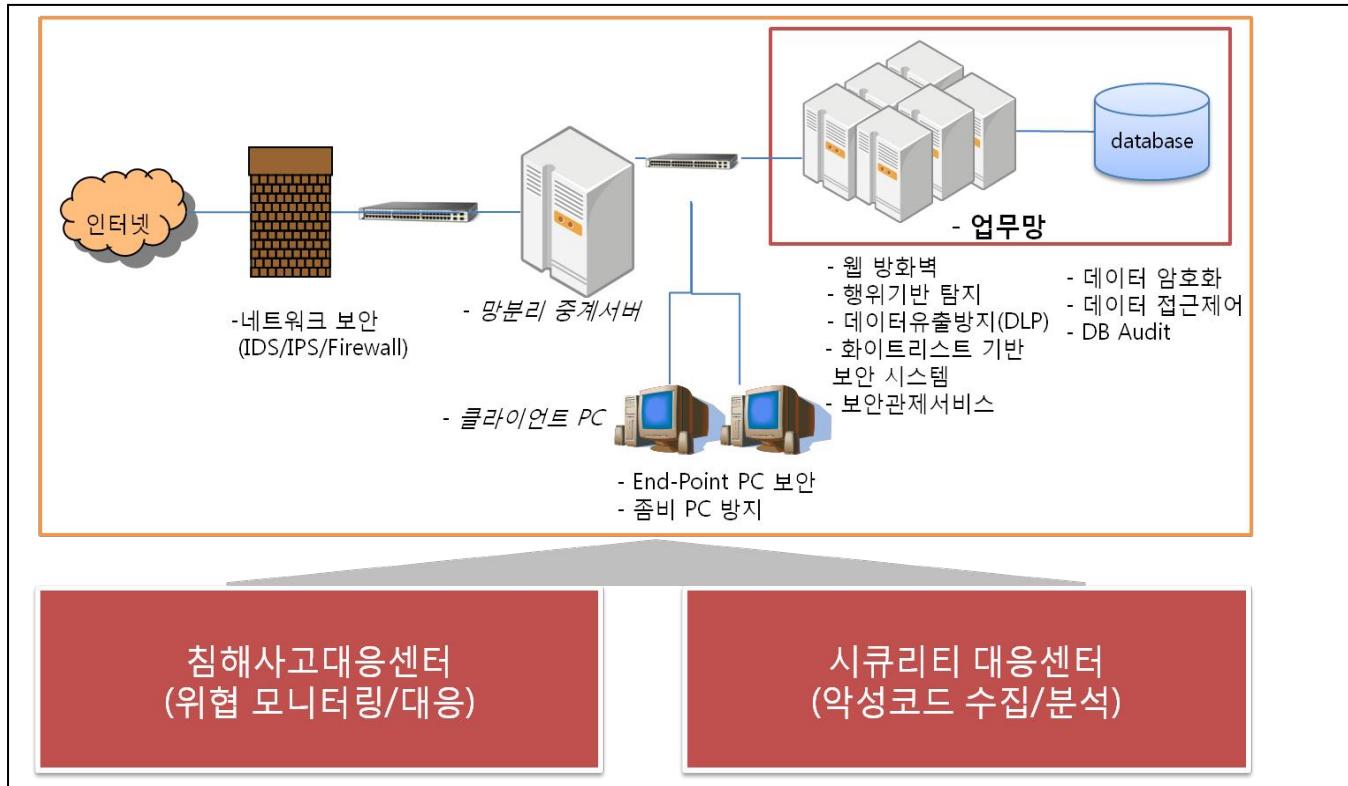
나. Advanced Persistent Threat의 공격 프로세스별 공격기법

침투 단계	관찰 (Reconnaissance)	APT 공격자들은 표적으로 삼은 시스템, 프로세스 및 파트너와 협력업체를 포함한 사람들을 파악하기 위해 수개월에 걸쳐 공격 목표를 철저히 연구, 분석함
	사회공학 (Social Engineering)	목표 시스템으로의 침투를 위해 공격자들은 내부 임직원이 실수나 부주의로 링크를 클릭하거나 첨부파일을 열게끔 유도하는 사회 공학적 기법을 접목. 예를 들어 공격자가 A라는 기업의 시스템 관리자를 노린다면 공격자는 사전에 이 관리자의 개인 블로그, 트위터, 페이스북 등을 검색해 생년월일, 가족 및 친구관계, 개인 및 회사 이메일 주소, 관심 분야, 진행중인 프로젝트 등의 정보를 수집한 후 이를 이용해 피싱 메일을 보냄
	제로데이 취약점 (Zero-day vulnerabilities)	개발자들이 패치 등을 제공하기 전에 소프트웨어 개발자들 모르게 공격자들이 악용할 수 있는 보안상 허점
	수동공격 (Manual operations)	APT는 자동화 대신 각각의 개별 시스템과 사람을 표적으로 삼아 고도의 정교한 공격을 감행
	다중벡터 (Multiple vectors)	APT 공격 시 일단 악성코드가 호스트 시스템에 구축되면 소프트웨어, 하드웨어 및 네트워크의 취약점을 탐색하기 위해 추가적인 공격 툴들이 다운로드 될 수 있음
검색 단계	온밀한 활동 (Run silent, run deep)	APT의 목표는 표적의 내부에 잠복하면서 장시간 정보를 확보 하는 것이므로, 모든 검색 프로세스는 보안탐지를 회피하도록 설계됨
	연구 및 분석 (Research analysis) and	정보 검색은 네트워크 구성, 사용자 아이디 및 비밀번호 등을 포함하여 확보된 시스템과 데이터에 대한 연구 및 분석을 수반함
	장시간 활동 (Long-term occupancy)	APT는 오랜 기간 지속적으로 정보를 수집하도록 설계됨. '인포메이션 위페어 모니터(Information Warfare Monitor)' 보고서에 따르면, 고스트넷(GhostNet)으로 알려진 대규모 사이버 스파이 사건은 2007년 5월 22일에 데이터를 수집하기 시작해 2009년 3월 12까지 지속된 것으로 나타남. 평균적으로 감염된 호스트가 활동한 시간은 145일이었고, 가장 긴 감염 시간은 660일이었음.
수집 단계	유출 (Exfiltration)	기밀 데이터가 웹 메일 혹은 암호화된 패킷, 압축파일 형태로 공격자에게 전송됨
	지속적인 분석 (Ongoing analysis)	수집된 정보는 전략적 기회를 포착하기 위한 연구에 이용. 이러한 데이터는 이 분야의 전문가들에게 하나의 지침서가 되어 영업 비밀을 캐내거나 경쟁사의 행동을 예측하여 대응 방안을 수립하는데 도움이 될 수 있음
	중단 (Disruption)	공격자는 원격 시동이나 소프트웨어 및 하드웨어 시스템의 자동 종료를 할 수도 있음. 많은 물리적 장치가 내장형 마이크로 프로세서에 의해 제어되고 있는 만큼 시스템이 교란될 가능성이 커짐. 명령 및 제어 서버는 은밀하게 표적 시스템을 제어하고 심지어 물리적 피해를 발생할 수도 있음.

3. Advance Persistent Threat의 대응방법

가. APT 대응 체계

- APT 공격은 지능적이며, 고도의 기술력을 기반으로 행해지는 공격이므로, End-to-End로 전방위적인 보안체계 수립이 필요하며, 망분리와 요소기술을 기반으로 안전한 시스템 아키텍처를 제시함
- 또한 침해사고 대응센터와 시큐리티 대응센터를 분리 운영하여, 예방과 대응 활동을 균형있게 추진



나. APT 대응 활동

- APT 발생 이전과 이후로 나누어, 위험예방전략, 악성코드 유입 최소화, 악성코드 감염 예방, 데이터 유출 예방, 위험탐지와 대응 활동 등을 수행

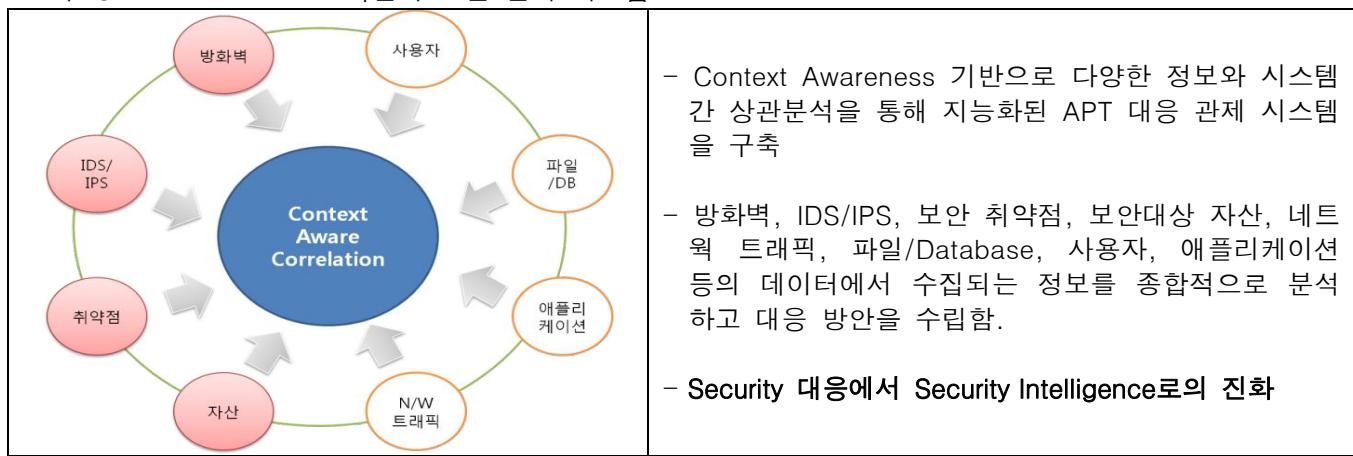
시기	활동	내용
위험발생 이전 (시큐리티 대응센터)	위험 예방 전략 수립	<ul style="list-style-type: none"> - 보안관제 수행 - 위험분석 수행 - 보안전략 유효성 분석
	악성코드 유입 최소화	<ul style="list-style-type: none"> - 보안 인식 교육 수행 - 지속적 보안 업데이트 관리 - 보안 소프트웨어 설치 및 운영
위험발생 이후 (침해사고 대응센터)	악성코드 감염 예방	<ul style="list-style-type: none"> - 어플리케이션 화이트리스트 - 접근 권한의 최소화 - 네트워크 접근 제한 및 분리 - 신원확인 및 접근 권한관리
	데이터 유출 예방	<ul style="list-style-type: none"> - 중요 데이터 보호 - 중요 데이터 유출 예방
	위험 탐지와 대응	<ul style="list-style-type: none"> - 호스트 및 네트워크 이상징후 탐지 - 침해사고 대응 프로세스 수행 - 침해사고 포렌식 프로세스 수행

4. Advance Persistent Threat 대응을 위한 차세대 융합 보안 기술

가. 보안 대응 관점의 Context Awareness 기술의 활용

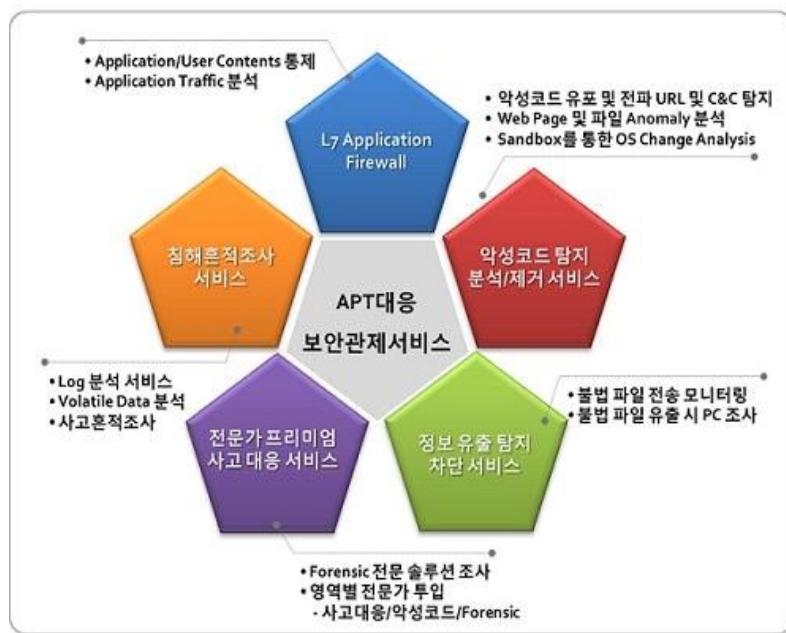


나. Context Awareness 기반의 보안 관제 시스템



“끝”

* 참고 : 3, 4단락에서는 문제에서 이야기한 대응방법에 수험생만의 차별화된 대응방법을 제시하는 것이 중요. 본 풀이에서는 “망분리”를 중심으로 답안을 작성하였으나, 보안 관제서비스 중심 등 각자의 장점 살려서 대응방안을 작성하는 것이 중요함. 보안관제 서비스로 풀 경우, 아래와 같이 큰 그림을 “가” 단락에 제시하고, 상세 내용을 “나” 단락에 기술.



10. APT(Advanced Persistent Threat) 공격기법에 대해 설명하시오.

정보관리

B) 10. APT 공격기법		
I. 치명적인 지속공격 APT 개요		
구분	공격기법	설명
특성	- 특정 목표를 사회공학적 기법을 활용하여 간접적, 지속적인 방법으로 피해를 가하는 사이버 대리행기	
APT 공격기법		
가. 사회공학 기법의 공격기법		
구분	공격기법	설명
직접적	- 흐려보기 - D/W 해킹	- Online/off line 사회공학 기법을 통한, 팀의 경로 확보
간접적	- Phishing - Smishing	- 목표 대상에 대한 감염 및 라이트 mail로 공격 기습

번호	사건	인력자원	인력기반의 침입방법에 대한	
	감염	마이터링	기록적 감지 및 DB 관리	
	공격기법	침투준비점검	침투 대상의 Network 분석	
II. 지속적 Savitae 기법의 공격기법				
구분	공격기법	설명		
침투	- Dugu - Driveby Download	- 침투, 감시를 위한 - 유행성이 있는 접촉이거나 URL 주소		
검색	- Vaccine 감염 - 암호화암복	- Vaccine, Anti-Epileptic - 암호화, 암호화 및 암호화		
수집	- Register 검색 - 물어검색	- Register 검색 및 카페 - Target 물어검색, 수집		
제어	- FluxNet - HackTivism	- 시설 관리위한 툴 활용 - 대형 제어 및 위협 행동제어		
- 당시 사회공학기법, 지속적 Savitae 기법과 대응방법				
구분	대응 방안	CSFI		
감지	- APT 운영 대응 리인 - APT 예방 대응 체계 수립	- 운영 리스크 분석 - 운영자/개발자 학습		
학제·연관	- 가능한 캐릭터疫苗 - 예방 위한 SDLC 보안	- 가능한 캐릭터 - 예방 보안		
정보기관	- 보안 사고 대처 관리 체계 - 대응 정책, 가능한 캐릭터	- 특별법 제정 - 민관 협력 체계 구축 및 운영		

10. APT(Advanced Persistent Threat) 공격기법에 대해 설명하시오

정보관리

문제 10)	APT 공격기법.
답)	<p>I. 전방위, 오랜 기간의 공격, APT의 개념</p> <pre> graph TD A[APT] -- 목적 --> B[기습] A -- 정밀 탈취, 금전 요구 --> C[정밀 탈취] A -- 비즈니스 정보 누출, 상각 --> D[비즈니스 정보 누출, 상각] B -- 기업/기관 타겟 --> E[기업/기관 타겟] C -- 정밀 탈취 --> F[정밀 탈취] D -- 정밀 탈취 --> G[정밀 탈취] </pre> <p>수행기간 측면</p> <ul style="list-style-type: none"> ✓ 최소 몇개월 ~ 몇년 ✓ 사내공작, 악성코드, DDoS
II.	<p>- 정밀 탈취, 금전 요구를 위한 기업 주요 정보 탈취 기법</p> <p>APT (Advanced Persistent Threat)의 기법</p> <p>가. APT 수행개념도</p>

번호	✓ 목표 설정	✓ 자료 수집	✓ 내부 침투	✓ 정보 수집	✓ 정보 탈취	✓ 소스 탐색
① 타당성 수립	✓	✓	✓	✓	✓	✓
② 침투 및 탈취						
③ 피해						
- APT 공격은 목표 설정부터 정보 탈취까지 치밀한 께획하여 이루어지는 기업/조직의 정보자산 탈취 기법						
IV. APT의 공격기법						
구분/단계	APT 공격기법	수명				
타당성 수립	SNS 수집 인터넷	SNS, 인터넷 등에서 대상 조직의 인물 정보 조사.				
침투 및 탈취	사내공작기법 백도어 악성코드	email, USB, Drived by Download 재침입을 위한 흥로 마련 제로시스템, 네트워크 마비				
피해	정보 탈취 백도어	정보/재산/지식 탈취 차후 침입을 위한 흥로 마련				
- APT는 정해진 기업이라기보다 침입/탈취를 위한 선진 악성 기법의 종동일임. 정해진 기업 없음						
V. APT 방지를 위한 기업/조직 대책						
구분	M&B.					
조직적측면	CEO/CIO 등 경영진의 인사 제고					
IT/M.	통합 위기 관리시스템 구축 및 운영					
정기적 Audit	정기적 점검을 통한 적절한 점검 '꼼'					

10	APT(Advanced Persistent Threat)		
문제	APT(Advanced Persistent Threat) 공격기법에 대해 설명하시오.		
도메인	보안	난이도	★ ★ ☆ ☆ ☆ (별 5 개 기준)
출제의도	기업, 금융기관 등의 컴퓨터를 지속적으로 공격하는 APT 공격이 증가하고 있어 이에 대해 이해 필요		
핵심 내용 키워드	<ul style="list-style-type: none"> 사전조사(Reconnaissance), 제로데이(Zero-Day)공격, 사회공학적 기법(Social Engineering), 은닉(Convert), 권한상승(Privilege Escalation and Lateralization), 지속(Persistent), 		
목차예시	<ol style="list-style-type: none"> APT(Advanced Persistent Threat) 공격의 개념 APT 공격의 프로세스 및 공격기술 APT 공격의 대응방법 		
채점 점수 가이드	<ol style="list-style-type: none"> APT 공격의 개념, 이해 부족 (1~2점) APT 공격기법의 기본 이해 수준 (3~5점) APT 공격기법의 정확한 제시 (5~6점) APT 공격의 대응 등 추가요소 설명(+α) 		
참고문헌	최신 정보보호기술 동향: APT 및 그 대응 – 정보통신산업진흥원		
출제자	홍 성우 기술사(제 84 회 정보관리기술사 / innoitpe@daum.net)		

1. APT(Advanced Persistent Threat) 공격의 개념

- APT는 특수목적을 가진 조직이 하나의 표적에 대해 다양한 IT 기술을 이용해서 지속적으로 정보를 수집하고 취약점을 파악하여 이를 바탕으로 피해를 끼치는 공격

구분	내용
A(Advanced)	<ul style="list-style-type: none"> APT 공격을 수행하는 조직에서 사용하는 기술적인 범위와 수준을 지칭 한 가지 기술만을 사용하는 것이 아니라 제로데이(Zero-Day) 취약점 공격, 기존 보안 제품을 우회하는 특수목적의 악성코드 제작 등 IT인프라와 관련된 다양한 기술을 이용한다는 의미 내포
P(Persistent)	<ul style="list-style-type: none"> APT 공격을 수행하는 조직의 특정목적 달성을 위한 태도 특정목적 달성을 위해 끊임없이 새로운 기술과 방식이 적용된 공격을 지속적으로 한다는 의미
T(Threat)	<ul style="list-style-type: none"> 정보보호 분야의 위협 자체를 말하는 것 악성코드, 취약점, 해킹 등의 IT 기술에 의해 발생하는 위협으로 자동화된 툴이나 단순 스캐닝 기술에만 의존하지 않고 사람이 직접 표적을 분석하고 이를 바탕으로 다양한 공격을 시도하는 사회공학적 기법을 모두 포함함

2. APT 공격의 프로세스 및 공격기술

가. APT 공격의 프로세스



나. APT 주요 공격 기술

단계	설명	공격기법
침투 (Incursion)	사전조사 (Reconnaissance)	<ul style="list-style-type: none"> 공격대상을 분석하고, 공격방법을 연구하여 최종 목표를 달성하기 위한 1차 공격 대상을 찾는 것 표적 대상의 주요 간부, 관리자, 연구원 등 정보에 직/간접 접근 가능 대상자를 찾는 것
	사회공학 (Social Engineering)	<ul style="list-style-type: none"> 신뢰하는 개인, 조직을 가장하여 악성코드를 제로데이 취약점이 있는 첨부파일이나 링크 등을 이메일, 메신저, SNS 등을 통해 전송하는 것을 의미
	제로데이 취약점 (Zero-day vulnerabilities)	<ul style="list-style-type: none"> 아직 발견되지 않았거나 사용하지 않는 보안 취약점을 이용하거나, 기존 보안제품에서 탐지되지 않는 악성코드를 이용하여 1 차 공격 목표에 대해 공격을 수행하는 것을 의미
	지속(Persistent)	<ul style="list-style-type: none"> 공격자가 참을성을 가지고 오랜 기간 동안 목표를 관찰하고 활동하는 것 중요정보 유출 이후에도 공격자가 표적대상에 지속적으로 접근할 수 있도록 다양한 백도어를 설치하는 것도 여기에 포함
검색 (Discovery)	다중벡터 (Multiple Vector)	<ul style="list-style-type: none"> APT 공격 시, 일단 악성코드가 호스트 시스템 내에 구축이 되면 소프트웨어, 하드웨어 및 네트워크의 취약점을 탐색하기 위해 추가적인 공격툴들을 다운로드
	은밀한 활동 (Run silent, run deep)	<ul style="list-style-type: none"> APT의 목표는 표적의 내부에 잠복하면서 장시간 정보를 확보하는 것이므로, 모든 검색 프로세스는 보안 탐지를 회피하도록 설계됨

정보관리(1교시)

	연구 및 분석 (Research and analysis)	<ul style="list-style-type: none"> 정보 검색은 네트워크 구성, 사용자아이디 및 비밀번호 등을 포함하여 확보된 시스템과 데이터에 대한 연구 및 분석을 수반함
수집 (Capture)	은닉 (Convert)	<ul style="list-style-type: none"> 1 차 공격에 성공한 후, 서두르지 않고, 정상적인 이용자로 가장하여 정보수집 및 모니터링 등의 활동을 하는 것으로, 합법적인 계정과 프로토콜 및 시간대를 이용하여 현재 계정이 갖는 권한 내에 수집 가능한 모든 정보를 수집하는 것이 특징
	권한상승 (privilege escalation & lateralization)	<ul style="list-style-type: none"> 1 차 공격이 성공한 후, 은닉을 통해 조직 내 각종 정보를 수집한 후, 시스템 접근을 위한 시스템 접근 권한을 가진 직원에 대한 계정정보를 수집하기 위한 각종 접근행위를 의미 패스워드 등의 계정정보를 획득하기 위한 Brute Force 공격 등도 포함
제어 (Control)	유출(Exfiltration)	<ul style="list-style-type: none"> 기밀데이터가 웹메일 또는 암호화된 패킷, 압축파일의 형태로 공격자에게 전송
	중단(Disruption)	<ul style="list-style-type: none"> APT 공격자는 원격시동이나 SW, HW 시스템을 자동 종료 할 수도 있음

3. APT 공격의 대응방법

- APT 공격의 효과적인 대응을 위해서는 조직 내부의 보안정책 및 체계를 분석하여 기술적, 관리적 대책을 수립하고, 이를 바탕으로 보안관리 체계를 정비하여 재구축하여야 함

대응방법	보안 강화 내용	대상 조직
보안관리운영, 교육	<ul style="list-style-type: none"> 조직의 종합적인 보안위험 분석 후 보안체계 재정비 효과적인 보안교육 실시 	보안정책관리 조직
엔드포인트 보안	<ul style="list-style-type: none"> APT공격의 1차대상인 엔드포인트 보안 강화 인터넷, 이메일, 메신저, P2P 통신서비스 제한 	엔드포인트 단말
접근권한관리	<ul style="list-style-type: none"> 조직의 중요정보보호에 대한 접근권한관리, 권한관리자 최소화, 접근권한 세분화, 사람/기기 인증 추가 	권한관리 인가자
중요정보 암호화 및 DLP운영	<ul style="list-style-type: none"> 조직 내 중요정보는 암호화 저장, 정보유출방지를 위한 DLP(Data Loss Prevention)솔루션 운영 	암호화 솔루션
계층형 방어 (Layered Defense)	<ul style="list-style-type: none"> 단계별, 용도별 배치로 계층적 방어 구현 	- CPNT Layered 방어

"끝"

고득점 전략 및 학습가이드	APT 공격기법에 대한 세부적인 내용까지 학습하고 이에 대응할 수 있는 방안도 함께 학습
----------------------	---

1	APT
문제	APT(Advanced Persistent Threat)을 설명하시오.
도메인	정보보안
출제배경/의도	정보보안 도메인 전체 내용을 APT 관점에서 핵심적인 내용을 요약하여 제시
키워드	<ul style="list-style-type: none"> ● 특정 타겟 존재, 맞춤형 공격 ● 공격기법, 대응방안 ● 보안인텔리전스(Security Intelligence)
목차예시	<ol style="list-style-type: none"> 1. 특정 타겟에 대한 맞춤형 공격, APT 의 개요 2. 공격기법과 대응방안 3. APT 대응 위한 보안인텔리전스
채점 점수 가이드	<p>① APT의 개념, 이해 부족 (1~3점) ② 기본 이해 수준 (3~5점) ③ 공격기법과 대응방안을 전반적으로 제시 (5~6점) ④ 추가요소 설명(+α)</p>
난이도	★ ★ ★ ☆ ☆ (별 5 개 기준)
학습 가이드	APT 가 이루어지는 과정에서 어디에서 공격이 이루어지는지, 대응을 하는 포인트는 어디인지 파악
출제자	이아람 기술사(제 107 회 정보관리기술사 / aram.inpure@gmail.com)

1. 특정 타겟에 대한 맞춤형 공격, APT의 개요

가. APT(Advanced Persistent Threat) 정의

- 개인이나 기업, 기관 등 명확한 타겟이 있어 목적을 달성하기 위해 장기간 수행되는 지능적 공격

나. 목적과 절차

- 개인정보 유출, 사업기밀 유출, 금전 요구 등의 목적으로 공격 시도
- 공격 절차는 일반적으로 기획, 침투, 수집, 유출과 같이 이루어짐

2. 공격기법과 대응방안

가. 공격기법

공격기법	설명	세부 공격기법
사회공학	- 사람의 심리를 이용하여 권한을 획득하는 등 사람을 대상으로 하는 공격	<ul style="list-style-type: none"> ● 스피어피싱, 악성메일, 워터링홀, 파밍, 스캠
웹 공격	- 웹 서비스의 특성과 취약성을 이용하여 수행하는 공격	<ul style="list-style-type: none"> ● SQL인젝션, XSS, CSRF, 웹쉘 업로드, 디운로드, 디렉토리리스팅, 재생공격 ● OWASP Top 10
시스템 공격	- 함수의 취약성이나 권한 제어의 미흡 등을 이용하여 권한을 상승하거나 DoS(Denial of Service)를 수행하는 공격	<ul style="list-style-type: none"> ● 버퍼오버플로우, 포맷스트링, 레이스컨디션
네트워크 공격	- 송수신 패킷을 도청하거나 변조, 또는 대규모 트래픽을 생성하여 전송함으로써 기밀성, 무결성, 가용성을 훼손하는 공격	<ul style="list-style-type: none"> ● 스니핑/스푸핑, MITM, 랜드어택, SYN 플러드, 스머프, 티어드롭
악성코드	- 최근 드라이브바이다운로드(DBD, Drive By Download)가 악성코드 배포 방법으로 확산	<ul style="list-style-type: none"> ● 바이러스, 웜, 트로이목마, 애드웨어, 스파이웨어, 랜섬웨어

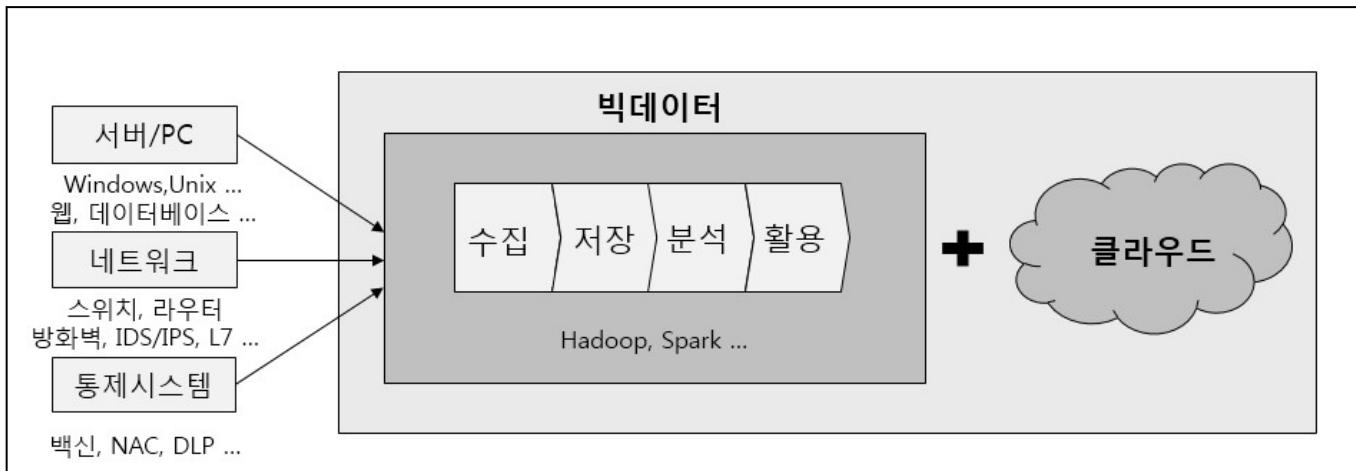
- 여러 공격기법이 복합적, 단계적으로 공격에 사용됨

나. 대응방안

대응방안	설명	고려사항
정책	- 조직 체계와 프로세스, 자산 분류 등 관리적 보안 대책	<ul style="list-style-type: none"> ● 거버넌스, 컴플라이언스, 조직, 자산, 위험 분석, 인증, 교육, 통제프로세스
관리	- 기 도입된 시스템의 보안수준을 유지하고, 신규 도입된 시스템의 안전한 운영	<ul style="list-style-type: none"> ● 보안표준, 정기/상시 점검, 감사(Audit)
접근통제	- 접근하려는 대상에 적절한 권한 부여	<ul style="list-style-type: none"> ● 예방/적발/교정통제, 네트워크/시스템/데이터베이스 통제
암호화	- 데이터가 유출되더라도 보호하기 위한 최후의 보안 수단	<ul style="list-style-type: none"> ● 암호화 대상, 알고리즘, 보안강도/키길이, 키관리

- 날로 지능화되는 APT에 대응하기 위한 빅데이터, 클라우드 기반의 보안인텔리전스를 구현 필요

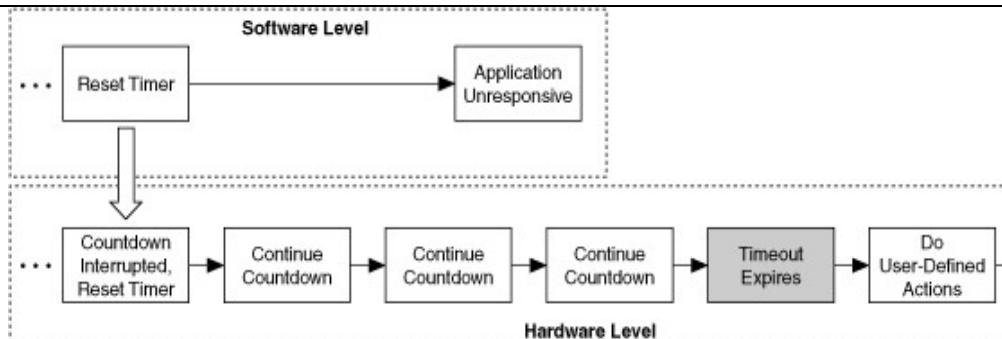
3. APT 대응 위한 보안인텔리전스



- 오탐을 최소화하고 자동 대응 가능한 수준의 체계를 갖추기 위한 인공지능, 딥러닝 적용
- IoT(Internet of Things) 등 ICT 환경이 복잡해짐에 따라 미래의 보안 모델로 주목

"끝"

- 소프트웨어는 하드웨어 타이머를 시작하여 특정 숫자부터 카운트 다운하고 타이머가 0에 도달 할 때 수행 할 작업을 정의
- 응용 프로그램이 위치독 타이머를 시작한 후에 타이머가 주기적으로 0이 되지 않도록 타이머를 주기적으로 다시 설정

오류
발생

- 소프트웨어 오류로 인해 응용 프로그램이 타이머를 다시 설정하지 못하게 되면 하드웨어 카운터가 소프트웨어와 독립적이므로 0에 도달할 때까지 카운트 다운을 계속하기 때문에 시간이 만료됨
- 위치독 타이머가 만료되면 하드웨어가 복구 절차를 수행

- 위치독 소프트웨어는 타이머 만료시의 작업 정의 및 하드웨어 타이머 시작 후 주기적으로 타이머의 초기화 수행

나. 위치독 타이머 소프트웨어 예시

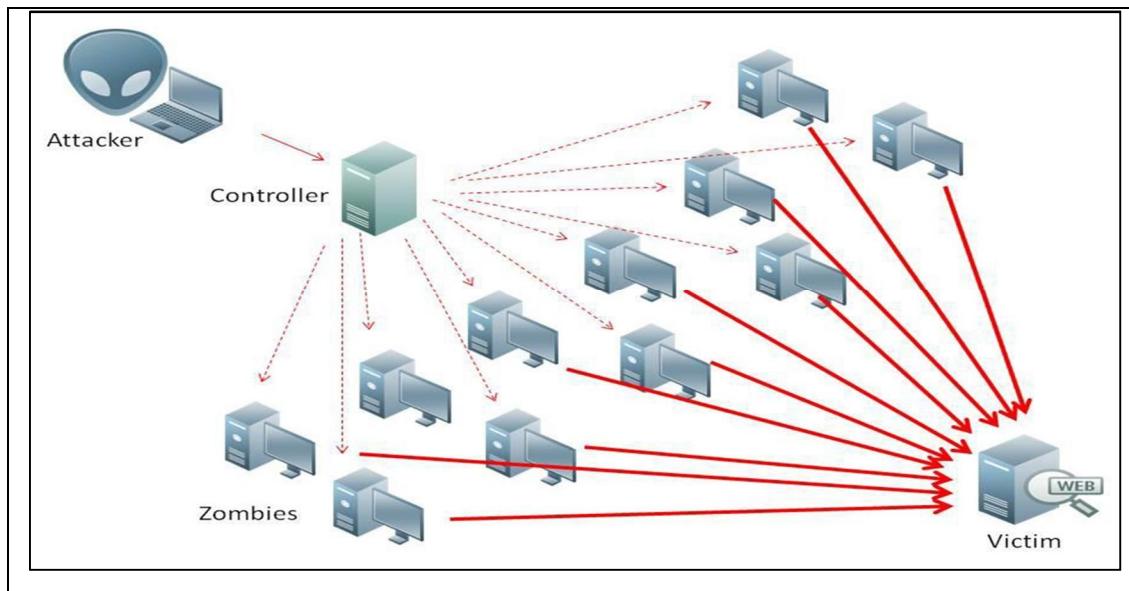
소프트웨어 (소스코드)	설명
<pre> uint16 volatile * pWatchdog = (uint16 volatile *) 0xFF0000; main(void) { hwinit(); for (;;) //continuous loop { *pWatchdog = 10000; // set the watchdog timer read_sensors(); control_motor(); display_status(); } } </pre>	<p>(워치독 타이머)</p> <ul style="list-style-type: none"> - 타이머가 만료(Expire)되면 시스템을 리셋하기 위한 신호를 전송 <p>(소프트웨어)</p> <ul style="list-style-type: none"> - 프로그램 루프를 실행하는 동안 워치독 타이머의 카운트가 초기화됨 - 프로그램 동작에 문제가 없이 주기적으로 카운트가 초기화되는 경우 카운트는 만료되지 않음 - 루프 명령이 실행에 실패하면 카운트는 초기화되지 않으므로, 타이머가 만료되어 시스템이 리셋됨

"끝"

2	DDoS
문제	DDoS 공격의 인지, 공격 유형 파악, 공격 유형에 따른 대응 방안에 대하여 설명하시오.
도메인	정보보안
정의	다수의 시스템에 분산/설치된 Agent(악성 프로그램)를 통해 동시에 서비스 거부 공격을 하는 방법
키워드	인지(유입 트래픽 크기, 웹서버 접속 로그, 동시접속 정보, 유입 트래픽 샘플링) 공격 유형 파악(패킷 덤프, 시나리오 기반) 대응 방안(ACL, PPS/요청수 임계치, 연결 타임아웃)
출제의도분석	상대적으로 보안이 취약한 사물인터넷(IoT) 기기 증가 추세. 사물인터넷 기기를 이용한 DDoS 공격 증가에 따른 대응절차 확인
답안작성 전략	DDoS 대응절차에 대해 가이드를 기준으로 실무적인 대응방안과 함께 제시
참고문헌	DDoS 공격대응 가이드 (KISA, 2012)
모범목차	<ol style="list-style-type: none"> 1. DDoS 공격대응 개요 2. DDoS 공격의 인지 및 공격 유형 파악 3. DDoS 공격 유형에 따른 대응방안
풀이 기술사님	방형철 기술사 (제 110 회 컴퓨터시스템응용기술사 / rebirth-v6@hanmail.net)

1. DDoS 공격대응 개요

가. DDoS(Distributed Denial of Service)의 개념



- DoS(Denial of Service): 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격
 - DDoS(Distributed Dos): 다수의 시스템에 분산/설치된 Agent(악성 프로그램)를 통해 동시에 서비스 거부 공격을 하는 방법
 - Drive by Download 등의 방식을 통해 악성 프로그램이 설치된 Zombie PC 를 이용하여 Victim 시스템을 일시에 공격
- 나. DDoS 공격대응 절차 및 목적

Notes

단계	절차	목적
1 단계	공격 인지를 위한 체크포인트	- 웹서비스 관련 이벤트 발생 시 해당 원인이 DDoS 공격으로 인한 것인지에 대한 명확한 판단이 필요
2 단계	DDoS 공격 유형 파악	- DDoS 공격 유형을 명확히 파악하여 차단정책 설정을 위한 근거로 활용
3 단계	공격유형에 따른 차단정책 정의 및 대응	- 공격의 유형과 목적을 명확히 판단하여 차단정책을 설정함으로써 웹서비스의 가용성 확보
4 단계	공격 대응 후, 사후조치	- 공격트래픽 분석을 통해 공격 내용을 상세히 규명함으로써 추가 발생할 수 있는 공격 대비를 위해 정책을 업데이트하고 좀비 PC IP를 확보

2. DDoS 공격의 인지 및 공격 유형 파악

가. DDoS 공격의 인지

Check Point	설명
유입 트래픽 크기 (Incoming Traffic Volume)	<ul style="list-style-type: none"> - 방화벽, IDS 등의 네트워크 장비를 통해 웹서비스 운영 망으로 유입되는 트래픽의 BPS 와 PPS 규모를 확인하여 평시와 비교 - 유입 트래픽의 크기가 비정상적인 증감을 나타내는 경우, 공격 발생 여부를 의심할 수 있음
웹서버 접속 로그 (WebServer Access Log)	<ul style="list-style-type: none"> - 서버의 접속 로그를 확인하여 비정상 접속 증가여부 확인 ※ 예) 메인페이지 등 특정 페이지에 대한 지속적 요청 여부
동시접속 정보 (Concurrent Connection)	<ul style="list-style-type: none"> - 웹서버와 클라이언트가 유지하고 있는 연결(Connection) 규모를 확인하여 평시대비 증감률 비교
유입 트래픽 샘플링 (Incoming Traffic Sampling Capture)	<ul style="list-style-type: none"> - 웹서버 운영망으로 유입되는 트래픽을 적절히 샘플링하고 실제 트래픽을 분석하여 DDoS 공격 여부 검증 ※ Sampling Capture 만으로도 비정상 여부 확인 가능

- 비정상 이벤트 발생 시 DDoS 공격이 원인인지에 대한 신속하고 명확한 판단 필요
- BPS(Bit Per Second), PPS(Packet Per Second): 네트워크 트래픽 규모를 파악하기 위한 기본 단위 ($10Mbps = 15,000PPS$)

나. DDoS 공격 유형 파악

구분	세부 방법	설명
유입 트래픽을 이용한 DDoS 공격 유형 파악	패킷 덤프(Packet Dump)를 이용한 유입 트래픽 확보	<ul style="list-style-type: none"> - tcpdump 와 같은 트래픽 캡쳐 툴을 이용하여 분석하고자 하는 기간 동안의 유입 트래픽 일부를 PCAP (Packet CAPture) 형태로 저장
	확보된 트래픽 분석(Analysis)	<ul style="list-style-type: none"> - DDoS 공격 특징을 파악하기 위해 프로토콜 정보, HTTP 헤더 정보, 연결 정보 확인
	시나리오 기반(Scenario Drawn)의 공격유형 파악	<ul style="list-style-type: none"> - 대역폭 소진공격, DB 부하 유발공격, 웹서버 자원 공격 등 대표적인 DDoS 공격 유형 파악

Notes

기타 방법을 이용한 DDoS 공격 유형 파악	웹서버 접속 로그 (WebServer Access Log)	<ul style="list-style-type: none"> - 서버 접속로그를 확인하여 접속자의 요청 페이지에 대한 통계와 특정 시간 동안 발생되는 요청 횟수에 대한 통계 확인 - 시스템 로그 및 네트워크 트래픽 분석을 통해 공격 유형을 파악하고 대응방안 수립
--------------------------	----------------------------------	---

3. DDoS 공격 유형에 따른 대응방안

가. 공격 유형에 따른 차단정책 정의 및 대응

구분	공격 유형	대응 방안
대역폭 소진 공격	UDP Flooding , ICMP Flooding	<ul style="list-style-type: none"> - 대응: 웹서버 망을 보호하는 방화벽이나 웹서버망 상단에 위치한 라우터에서 해당 프로토콜을 차단하도록 ACL(Access Control List) 설정
	TCP Flooding	<ul style="list-style-type: none"> - 대응: 소스 IP(Source IP)별로 PPS(Packet Per Second) 임계치 설정 ※ 대용량 TCP Flooding 공격은 프로토콜 기준으로 차단하는데 한계가 존재
웹서버 자원 소모 공격	Syn(Ack/Fin) Flooding	<ul style="list-style-type: none"> - 특징: 웹서버 OS의 TCP 스택(Stack) 자원을 소모 - 대응: ①소스 IP 별로 PPS 임계치를 설정하거나 ②패킷 헤더 검사를 통해 정상적인 옵션 필드값을 가지지 않는 비정상 패킷 차단
	Slow Header Flooding, Slow Data Flooding	<ul style="list-style-type: none"> - 특징: 완료되지 않은 연결(Connection) 상태를 지속적으로 유지 - 대응: 하나의 요청에 대한 연결 타임아웃을 설정하여 특정 타임아웃이 지나면 연결을 종료시켜 차단
DB Connection 부하유발 공격	Get Flooding , Post Flooding	<ul style="list-style-type: none"> - 특징: 다량의 HTTP 요청으로 웹서버와 DB 연동에 부하 유발 - 대응: ①클라이언트로부터의 요청 수에 대한 임계치를 설정하여 임계치를 초과하는 소스 IP의 접속을 차단하거나 ②HTTP 헤더를 확인하여 표준에 맞지 않는 필드 값을 차단 시그니처(Signature)로 설정
봇 vs 브라우저 식별		<ul style="list-style-type: none"> - 대응: 일반적인 봇은 브라우저와 달리 웹서버의 응답코드에 반응하여 행동하지 않으므로 웹서버에서 302 moved temporary 와 같은 코드로 응답하여 봇이 발생시키는 요청을 차단

- 분석된 공격 유형의 특성에 기반하여 차단정책을 설정함으로써 시스템의 가용성 확보 및 피해 최소화

나. 공격 대응 후 사후조치

사후조치	설명
공격 시점의 BPS, PPS, CPS 변화 추이 확인	<ul style="list-style-type: none"> - 공격 규모를 확인하여 웹서버의 가용성이 침해될 수 있는 지점을 확인하여 정확한 분석정보가 반영된 차단정책 업데이트

4

최근 DDoS 공격이 지능화되면서, 공격트래픽에 대한 신속한 탐지 및 완화(Mitigation)를 어렵게 하고 있다.

(1) DDoS 공격유형별(대역폭공격, 세션공격, 웹 HTTP 공격) 피해증상을 설명하시오.

(2) DDoS 대응을 위한 Anti-DDoS 시스템의 대응방식을 다음의 2 가지 경우로 나누어 설명하시오.

첫째, 공격 IP가 변조된 경우 인증기능을 통해 대응하는 방식

둘째, 공격 IP가 변조되지 않은 경우 대응하는 방식.

출제도메인	디지털 씨큐리티
주요 키워드	- 좀비 PC, Agent, 악성코드, 대역폭 공격, 세션 공격, 웹 HTTP 공격, IP 변조
난이도	★ ★ ☆ ☆ ☆ (별5개 기준)
참고문헌	- DDoS 공격대응 가이드, 한국인터넷진흥원 - DDoS 공격 유형별 대응방안 설명, 금융보안연구원 - KPC 기술사 IMPACT 실전모의고사 제13회, 제21회 해설집
문제소견	- 2003년 7.7 DDoS 대란 이후 계속적으로 출제되고 있으므로 깊게 준비 필요
기출풀이 작성기술사	강지양 기술사(제98회 컴퓨터시스템응용기술사 / jiyang.kang@gmail.com)

1. Agent를 이용한 분산서비스 거부공격, DDoS의 개요

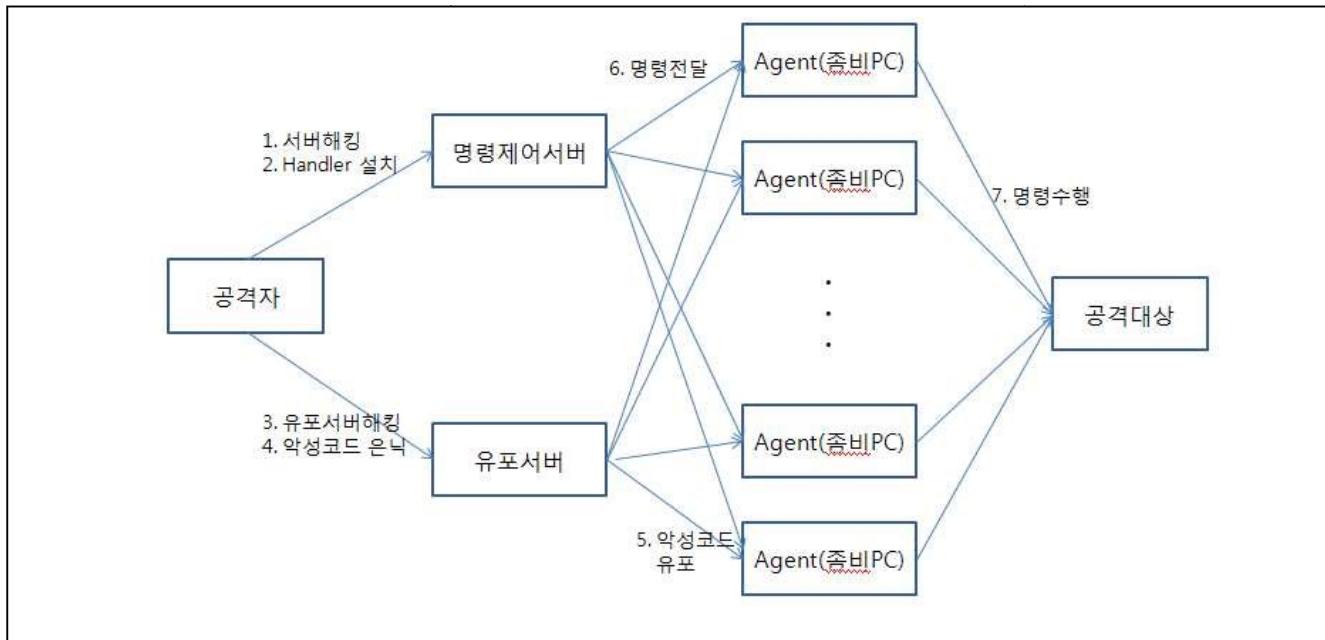
가. DDoS(Distributed Denial of Service)의 정의

- 여러 대의 컴퓨터(좀비 PC)를 일제히 동작하게 하여 특정 사이트를 공격, 엄청난 분량의 패킷을 동시에 범람시켜 네트워크 성능 저하나 시스템 마비를 가져오게 하는 해킹 기법

나. DDoS의 특징

특징	설명
대량의 좀비 PC	대량의 패킷을 발생시킬 대량의 PC 필요
취약점 이용	시스템의 취약점을 이용한 시스템 접근 후 Agent 설치
은닉 분산공격	네트워크에 분산되어 분포하는 좀비 PC에 은닉한 악성코드를 통해서 사용자가 인식하지 못하는 동안 공격 수행
명령 제어 서버	설치된 Agent에 대한 공격명령 수행 및 제어
방어의 어려움	- 네트워크에 분산되어 공격함으로써 모든 소스를 차단하기 어려움 - IP를 위조하거나 에이전트를 변경하여 공격함으로써 차단이 어려움

다. DDoS 공격의 개념도



- 1) 바이러스 악성코드 전파를 위해서 악성코드를 특정 경유지 또는 파일에 감염/해킹하여 배포시킴
- 2) 일반 사용자는 악성코드 경유지에 방문 또는 악성코드 파일을 열면서 사용자 PC도 악성코드에 감염
- 3) 특정시간 공격자에 의한 DDoS 공격 수행 명령
- 4) 특정 사이트에 대한 대규모 공격 진행

구성요소	설명
공격자 (Attacker)	- DDoS 공격을 주도하는 공격자의 컴퓨터를 의미함
마스터 (Master)	- 여러 대의 DDoS 에이전트의 연결을 관리하는 시스템 - 공격자에게 직접 명령을 받아 에이전트에 명령 전달을 실행함
에이전트 (Agent)	- 일반 사용자의 컴퓨터에 은닉하며 마스터에 연결하여 관리되는 악성코드 - 마스터의 명령에 따라 공격 대상(Victim)에 직접적인 공격을 시도하는 코드
공격대상 (Victim)	- DDoS 공격의 대상이 되는 시스템

2. DDoS 공격의 유형 및 유형별 피해증상

가. DDoS 공격의 유형 분류

특징	대역폭 공격	세션 공격	웹 HTTP 공격
사용 프로토콜	주로 UDP/ICMP	TCP	HTTP
공격 PC 위치	국내	국내/국외	국내/국외
IP 변조 여부	변조/실제IP	변조/실제IP	실제IP
공격 유형	1000~1500 byte 패킷 전송, 1GByte 이상, 수십만 PPS	64 byte 이하 패킷 전송 100MB, 수십만~수백만 PPS	동일 URL 접속 시도
공격 효과	회선 대역폭 초과	네트워크 장비, 보안장비, 서버 등의 부하 발생	웹서버 부하 발생
피해 시스템	동일 네트워크에서 사용중인 모든 시스템	공격 대상 시스템 또는 동일 네트워크에서 사용 중인 모든 시스템	공격 대상 시스템

나. DDoS 공격유형별 피해증상

공격유형	피해증상	세부 공격기술	설명
대역폭 공격	공격대상 네트워크의 대역폭을 고갈 시켜 서비스 마비 유도	UDP Flooding	<ul style="list-style-type: none"> - UDP의 비연결성 및 비신뢰성, source address와 source port를 spoofing하기 쉬운 약점을 이용해 과다한 트래픽을 Victim에 전송함으로써 Victim간 네트워크를 마비 - 공격자가 Victim A에게 source IP address 를 Victim B의 IP address로 spoofing하여 대량의 UDP 패킷을 전송 <p style="text-align: center;">① UDP Flood Source IP = Victim B IP</p> <p style="text-align: center;">Attacker → Victim A</p> <p style="text-align: center;">② Response</p> <p style="text-align: center;">Victim A → Victim B</p> <p style="text-align: center;">③ 네트워크 과부하</p>
		ICMP Flooding	<ul style="list-style-type: none"> - 활성화된 서비스나 포트가 필요하지 않는 유일한 프로토콜인 ICMP의 특징을 악용, 대량의 ICMP 패킷을 공격자가 직접 Victim에게 전송하는 방법으로 그 변종의 예로 Smurfing, Welchian worm 등이 있음. - 공격자가 Source IP address를 Victim의 IP address로 설정한 후, broadcast address로 ICMP echo request 패킷을 전송하면 그 하위 모든 시스템들이 ICMP echo reply 패킷을 Victim으로 전송하게 되어 대량의 패킷들이 집중하여 네트워크 부하를 높임 (Smurfing) <p style="text-align: center;">① ICMP echo request broadcast Source IP = Victim IP</p> <p style="text-align: center;">Attacker → Internet</p> <p style="text-align: center;">② Reachable Host</p> <p style="text-align: center;">Victim → ICMP echo reply</p> <p style="text-align: center;">③ 네트워크 과부하</p>
세션 공격	서버의 CPU, 대기 큐 및 Connection 자원의 고갈 유도	IP Spoofed Syn Flooding	<ul style="list-style-type: none"> - IP 변조 후 다량의 SYN 패킷을 서버로 전달하여 서버의 대기 큐 (Backlog Queue)를 가득 채워 새로운 클라이언트의 연결요청을 무시하도록 하여 장애를 유발시키는 공격 - TCP 프로토콜이 데이터를 보내기 전에 연결을 먼저 맺어야 하는 특징을 이용 - 공격자는 unreachable 한 호스트인 IP주소로 Spoofing하여 계속하여 연결요청 (SYN/ACK) 패킷을 보냄 - 공격 받은 서버는 다수의 SYN_RECEIVED 세션 상태가 발생

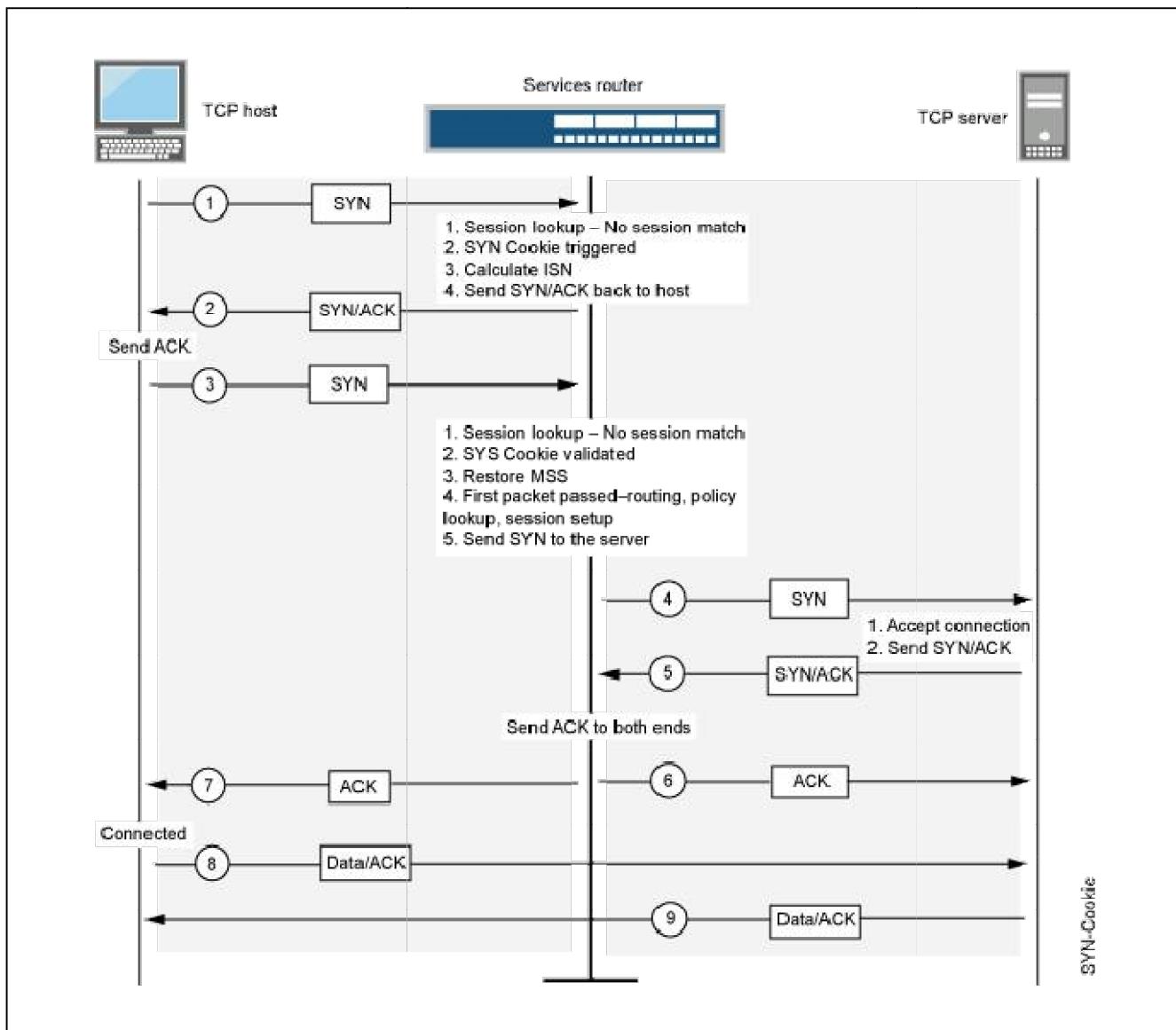
			<p>① SYN Spoofed & Unreachable IP address</p> <p>② SYB / ACK</p> <p>③ SYN Flood</p> <p>④ Backlog Queue overflow</p>
		TCP Connection Flooding	<ul style="list-style-type: none"> - TCP 3-Way Handshake 과정을 과도하게 유발함으로써 서비스의 과부하를 유발 (3-Way Handshaking 정상 완료) - IP를 변조하지 않고, 다량의 SYN 패킷을 공격 대상 서버로 전송 - 공격 받은 서버는 다수의 ESTABLISHED 세션 상태가 발생 - ① TCP 세션 연결을 유지하는 DDoS 공격, ② TCP 세션 연결/해제를 반복하는 DDoS 공격, ③ TCP 세션 연결 후 정상적인 트랜잭션(Transaction)처럼 보이는 트래픽을 발송하는 DDoS 공격으로 구분
		TCP Out-of-State Packet Flooding	<ul style="list-style-type: none"> - 다량의 ACK/SYN+ACK/FIN/RST 등의 패킷을 공격 대상 서버로 전송 - 일부 네트워크 장비 및 서버의 CPU 사용량이 올라가는 등 오작동 발생 가능
웹 HTTP 공격	웹 서버 및 데이터베이스 서버의 CPU 및 Connection 자원 고갈 유도	HTTP Flooding	<ul style="list-style-type: none"> - 동일한 URL을 반복 요청하여 웹서버가 URL에 해당되는 데이터를 클라이언트에게 회신하기 위해 서버 자원을 사용하도록 하는 공격 - 웹서버는 한정된 HTTP 처리 Connection 용량을 가지기 때문에 용량 초과시 정상적인 서비스가 어려워짐 <p>Repeated HTTP Get Requests Single Connection</p> <p>Attacker</p> <p>Public Web Servers</p> <p>Misuse of Service Resources</p> <p>Repeated HTTP Get Requests Multiple Connections</p> <p>Attacker</p> <p>Public Web Servers</p> <p>Misuse of Service Resources</p>
		CC (Cache Control) Attack	<ul style="list-style-type: none"> - HTTP 메시지의 캐시 옵션을 조작하여 캐싱 서버가 아닌 웹 서버가 직접 처리하도록 유도하여 캐싱 서버의 기능을 무력화하고 웹서버의 자원을 소진시키는 공격

3. Anti-DDoS 시스템 대응방식 2가지

가. 공격 IP가 변조된 경우 인증기능을 통해 대응하는 방식

대응 방식	내용	적용 공격 유형
Syn Proxy 또는 Cookie 기능 사용	<ul style="list-style-type: none"> - Syn Proxy/Cookie 기능을 제공하는 보안 장비 및 네트워크 장비 이용. 단, 장비의 성능 파악 후 적용 필요 - Syn Proxy: 사용자가 세션을 맺기 위해 SYN을 보내면 보안장비에서 SYN ACK로 응답하고 사용자는 ACK를 다시 보내 정상적인 세션을 이를 때, 보안장비는 사용자를 SYN Proxy table에 인증 등록하여, 이후 해당 사용자는 보안장비를 통해 통신하는 방식. <pre> sequenceDiagram participant Client participant Firewall participant Server Client->>Firewall: 1) SYN Note over Firewall: Allocate TCB resources Note over Firewall: Request verified legal Firewall->>Client: 2) SYN/ACK (Cookie) Firewall->>Server: 3) ACK Client->>Server: 4) SYN Server->>Client: 5) SYN/ACK Client->>Server: 6) ACK Note over Firewall: Proxy for subsequent packets Client->>Firewall: Data (x) Firewall->>Server: Data (x) Client->>Firewall: Data (y) Firewall->>Server: Data (y) ... </pre>	<ul style="list-style-type: none"> - IP Spoofed Syn Flooding 공격 - IP Spoofed TCP Out-of-State Packet Flooding 공격 (ACK/SYN+ACK/FIN 등)
비정상 IP에 대한 ACL 적용	<ul style="list-style-type: none"> - RFC1918에서 지정한 비공인 IP - 특정 목적을 가진 IP 및 IANA에서 reserved한 IP 	
해외 트래픽 차단 (NULL 라우팅 적용)	<ul style="list-style-type: none"> - ISP/IDC 등과 협조하여 국제 GW에서 해외 트래픽 차단 (NULL 라우팅) - 라우터 간의 Dynamic Routing을 통한 점진적인 트래픽 감소 유도 	

(참고) Syn Proxy/Cookies 동작흐름도 (출처: 쥬니퍼네트웍스)



나. 공격 IP가 변조되지 않은 경우 대응하는 방식

대응 방식	내용	적용 공격 유형
공격의 진원지가 국외일 경우	<ul style="list-style-type: none"> - ISP/IDC 등과 협조하여 국제 GW에서 해외 트래픽 차단 (NULL 라우팅) - 라우터 간의 Dynamic Routing을 통한 점진적인 트래픽 감소 유도 	<ul style="list-style-type: none"> - TCP Connection Flooding 공격 (3-Way Handshaking 정상 완료) - IP 변조되지 않은 TCP Out-of-State Packet Flooding 공격 (ACK/SYN+ACK/FIN 등)
공격의 진원지가 국내일 경우	<ul style="list-style-type: none"> - C&C 서버의 조정을 받고 있는 봇넷 PC에 의한 경우가 대부분 - 대외기관에서 공격 IP를 제공하여 봇넷 샘플 확보 - 샘플 분석을 통하여 C&C 서버와 봇넷 PC와의 통신 차단 (대외기관 등 협조) - 긴급한 보안 프로그램 업데이트 수행(보안업체 협조) - 공격 소스 IP가 소수일 경우, ACL을 이용하여 차단 	<ul style="list-style-type: none"> - HTTP Flooding
DDoS 대응 시스템 사용	<ul style="list-style-type: none"> - 민원 접수 및 모니터링을 통하여 장애 발생 가능성에 대비 	
서버 설정 변경	<ul style="list-style-type: none"> - KeepAlive를 off로 변경 - MaxClient를 최대 수치로 조정 	<ul style="list-style-type: none"> - HTTP Flooding
웹 서버 증설	<ul style="list-style-type: none"> - 물리적 웹 서버 대수 증설 	

불필요한 UDP/ICMP 서비스 차단	- 가능한 최상위 구간(국제 GW, IDC 라우터 등)에서 차단	- UDP/ICMP Flooding
NULL 라우팅 적용	- 공격 대상 서버에 대한 NULL 라우팅을 적용하여 점진적으로 공격 트래픽 감소 - 동일네트워크에서 운영중인 다른 서버/서비스 보호	
DNS 서버 다중화	- 다중 DNS 서버 운영 - 제3의 등록기관에 DNS 등록	
DNS 전용 회선 준비	- 서비스 네트워크 회선과 별도로 우회할 수 있는 DNS 전용 회선 마련	
보안 시스템 사용	- IDS, TMS 등과 같은 모니터링 시스템을 통하여 공격 트래픽에 대한 분석 - 생성된 패턴을 IPS, L7 스위치 등에 적용하여 차단	- 특정 패턴을 가진 DOS 공격 - 네트워크 장비, 서버 등의 취약점을 이용한 DOS 공격
보안 패치	- 취약한 네트워크 장비 및 서버에 대한 패치	- 네트워크 장비, 서버 등의 취약점을 이용한 DOS 공격

4. DDoS 공격 대응 사전 준비 및 공격 단계별 고려사항

가. DDoS 공격 대응 사전 준비

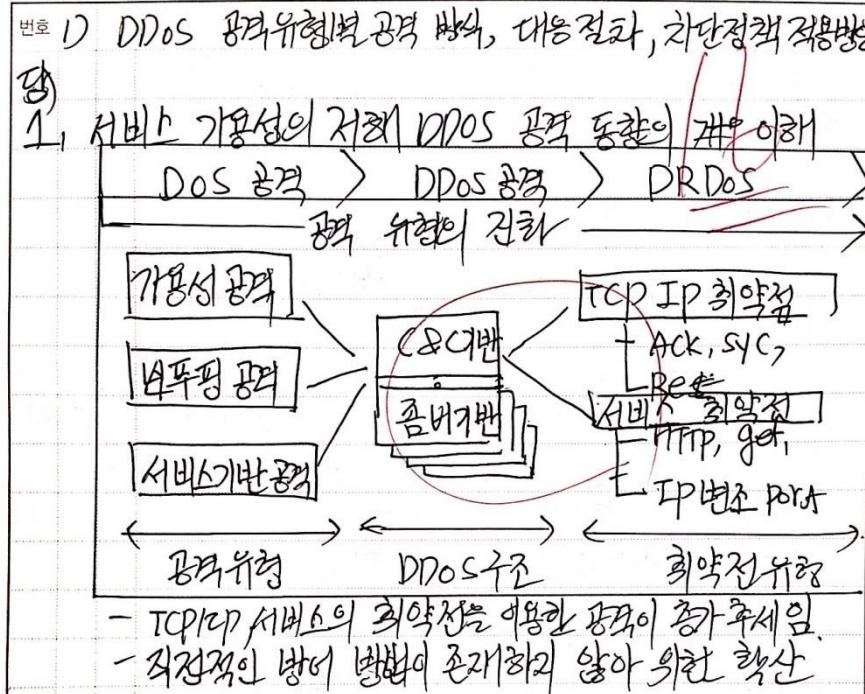
사전 준비	구분	세부 사항
기 설치된 시스템을 이용한 모니터링 체계 구축	MRTG를 이용한 네트워크 모니터링	- PPS(Packet per Second) 모니터링 - BPS(Bits per Second) 모니터링
	네트워크 장비 및 서버 성능 모니터링	- 각종 네트워크/보안 장비 및 서버에 대한 성능 모니터링 - 서버 모니터링
	로그 분석을 통한 모니터링	- 출발지 및 목적지 IP - 서버 접속 로그 - 애러 로그
모니터링 시스템 및 DDOS 공격 대응 시스템 활용	Netflow, FlowScan 등을 이용한 모니터링	- IP 프로토콜(TCP, UDP, ICMP 등) 분포 - 서비스별 사용량
	모니터링 시스템을 이용한 모니터링	- 네트워크 현황 분석 - 임계치 설정을 통한 알림 기능 사용 - 응답 시간(Response Time) 측정 - 패킷 분석
	DDOS 공격 대응 시스템	- NBA 기반의 DDOS 공격 대응 전용 시스템 - DDOS 공격 대응 기능이 추가된 IPS - 웹 가속기, L7 보안스위치 - 기타 보안 시스템 등

나. 공격 단계별 고려사항

단계	고려사항	내용
공격에 대비한 사전 준비	모니터링 체계 구축	- 공격 징후 및 공격 발생 시, 즉시 인지 및 분석 가능
	단일 명령 체계 확립	- 공격에 대비한 업무 분장
	비상연락망 사전 구축	- 대외 협력 기관과의 협조 체계 및 비상연락망 사전 구축
공격 발생시	공격 확산 방지	- 대응방안에 따른 초동 대응 - 네트워크 수준으로의 공격 확산 방지
	ISP/IDC 등과의 적극적인 협력	- 실시간 정보 공유 및 공동 대응 방안 마련
	대외 협력 기관과의 협력	- 샘플 확보 및 분석 - 보안 프로그램(백신) 업데이트, 봇넷 제거 등

“끝”

1. DDoS(Distributed Denial of Service) 공격유형에 따른 시스템 보호와 방어를 위해 사용하는 자원을 항상 모니터링하고 차단정책 수립하고 적용하는 것이 무엇보다 중요하다. DDoS의 공격 유형별 공격방식을 5가지 이상 설명하고, 대응 절차와 DDoS 공격유형별 차단정책 적용 방안을 제시하십시오.

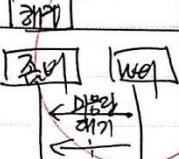
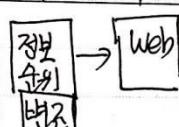


2. DDoS 공격유형별 공격 방식

가) TCP/IP의 회약점 기반 공격

구분	구조	설명
ACK Flood	대량 ACK 요청	- 해커의 ACK로 IP 도용 전략 - 서비스는 ACK 무한 대기로 차단 고장

Sym Flood	대량 SYN 요청 → ACK → 대기	- Sym의 대량 해커 번으로 통한 공격 - 대량 패킷 차단 고장
RST	대량 RST 요청 → ACK → Reset	- 연결 끊기 요청 - 무한 연결 끊기 수동 - 차단 고장, Timeout
IP 변조 공격	대량 DNS IP 번조 → 서버	- 해커가 DNS IP 번조 - 요청 정보의 서비스 고장 - 서비스 흐름을 차단
기타 공격	- 스머핑 공격 - Pming 공격 - 패킷 조작	- 브로드 캐스트 방정 공격 - 특정 서비스로 평공격 - Tear drop 기반 공격
- 가용성 및 이용성이 위한 공격이 주로 이론		
나) 서비스 회약점 기반 유형의 공격		
구분	구조	설명
HTTP GET Flood	대량 GET 요청 → Web	- GET 요청은 존버 서비스 통해 무한 요청 수동 - Web 페이지 세션 고장
SlowDown Attack	slow → ACK → ACK 전송	- 대량의 레이저 출현 작은 용량의 레이저 전송 - Array 2000k 신호 후 1 byte 씩 전송

CROSS SITE 기반		특정 Web 페이지를 무한 클릭 하도록 Browser page 상에서 공격
HTTP POST 공격		- 요청에 대한 대량의 대기, 서버 고장 유발 - 서비스 요청은 미종료 상태
Reflect 서비스 리스팅		- 정보 속도는 google 등에서 변조하여 특정 SITE 전송을 유도하는 기법
		- 서비스 기반 공격으로 구별과 차단이 쉽지 않은 - 요청자와 위치 기반 일정시간 차단 정책 구현

3. DDoS 대응 대응 철학 및 DDoS 차단 정책 적용방법
가 DDoS 대응 개론

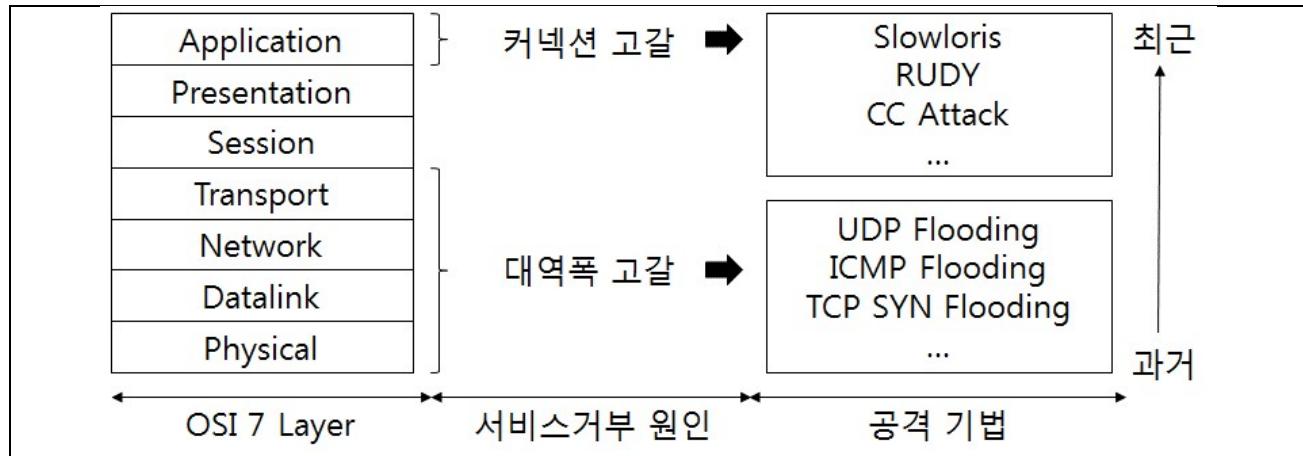
대응체계구조	보호자산 - 보호자산 선정 위험분석 - 위험 분석 수준
일관체계구조	조직 : - 대응(CCERT) 조직 구성 프로세스: - 대응 Manual 구성
보내려면	Rule기반 - DDoS 차단기반 평판기반 - ByName 분석

대응	개선	일관체계	위급변수 체계 구축
		내부적	- DDOS, ZPS 기반 차단
		외부적	- 국가(erfc), ISP 협력
		- 장기적이고 전문적인 관리 체계에서 구성	
주제	정책 유형	차단 정책	
TCP/IP 죄악성	ACK Flood SYN Flood RST Flood IP 변조	Sink hole Block hole Proxy 공격	- 대용량 패킷 통신 IP로 전환 - 특정 IP로 DNS 기반 폐기 처리 캐시 저지 - 사용변경 가능 여부
서비스 죄악성	HTTP get Flood Slow Down CROSS SITE SECURE CODE HTTP POST 분위기변조 공격	웹방화벽 파밍워드박스 SECURE CODE - IP 주체 - 사전 대처 - 패킷 필터	- 특정 IP 차단 - 연속 패킷 차단 - 보안 고정 강화 - 대량 패킷 차단 - 딥패킷기반 서비스
		- 보호정책 및 장비로 기반하여 대량의 IP 차단 수립 - 연속적 모니터링이 체계로 유지하고 관리 - 통합 모니터링 체계화에서 사전 위험 분석 - SECURE CODE 체계, 적용의 확장	

4 DDoS 공격기법인 Slowloris 와 RUDY			
문제	DDoS 공격기법인 Slowloris 와 RUDY의 개념 및 공격원리에 대해 설명하시오.		
도메인	보안	난이도	★ ★ ★ ☆ ☆ (별 5개 기준)
출제의도	DDoS 공격은 예전에 대량의 트래픽을 발생하는 기법에서 세션 등 자원을 고갈시키는 방향으로 진화하고 있습니다. 기본적인 DDoS 공격기법은 언제든지 출제될 수 있기 때문에 유사한 유형의 공격기법을 함께 숙지하여 관련 문제에 대응할 수 있도록 합니다.		
핵심 내용 키워드	<ul style="list-style-type: none"> - Slowloris : HTTP 세션 고갈, GET method, CRLF(WrWn) - RUDY: HTTP 세션 고갈, POST method, content-length 		
목차예시	<ol style="list-style-type: none"> 1. DDoS 공격기법의 유형 2. Slowloris 공격기법의 개념 및 공격원리 3. RUDY 공격기법의 개념 및 공격원리 4. Slowloris 와 RUDY에 대한 대응방안 		
채점 점수 가이드	<p>① 개념, 이해 부족 (1~8점) ② 기본 이해 수준 (9~13점) ③ 정확한 기술 제시 (14~15점) ④ 추가요소 설명(+α)</p>		
참고문헌	위키피디아(https://en.wikipedia.org/wiki/Slowloris_(computer_security))		
고득점전략 및 답안작성 가이드	최근 DDoS 공격은 Application Layer 의 프로토콜 취약점을 이용하는 방향으로 진화하고 있습니다. 그 중에서도 가장 많이 사용되는 HTTP 프로토콜의 기본적인 동작을 이해하고, 프로토콜에 내재된 취약점을 악용한 공격방법까지 숙지하면 네트워크 도메인과 보안 도메인에서 시너지를 발휘할 수 있을 것이라고 생각합니다.		

출제자	이윤기 기술사(제 111 회 컴퓨터시스템응용기술사 / yoonki.lee.pe@gmail.com)
-----	--

1. DDoS 공격의 유형



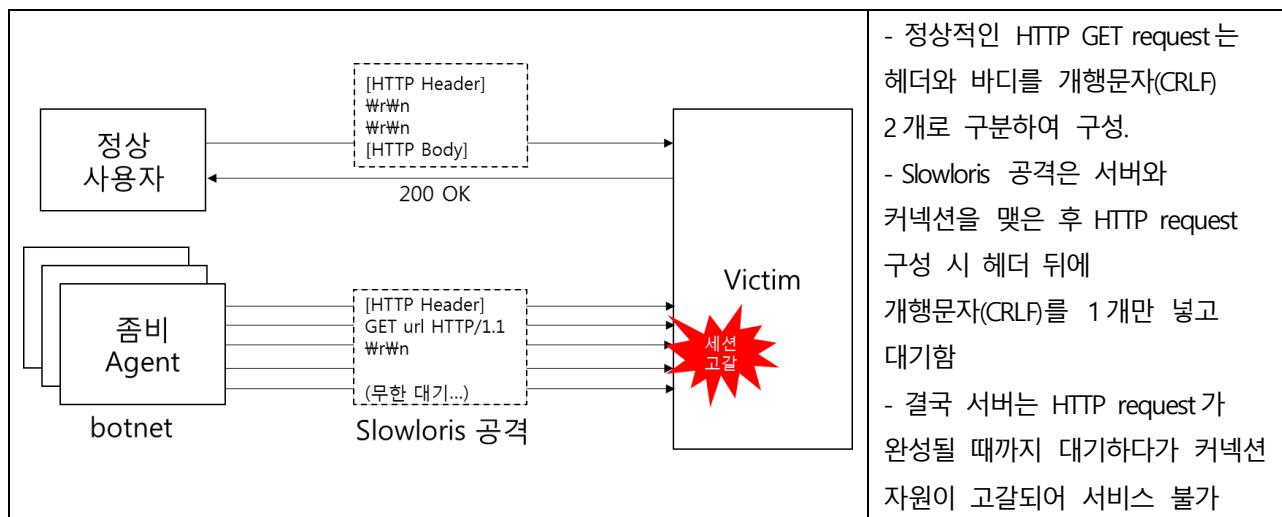
- DDoS 공격: 여러 대의 공격자를 분산적으로 배치해 동시에 한 곳을 공격하도록 하는 형태의 서비스 거부 공격
- DDoS 공격 유형은 크게 대역폭을 고갈시키는 공격과 커넥션을 고갈시키는 공격으로 분류 가능
- Slowloris 와 RUDY는 HTTP 커넥션을 고갈시켜 서비스를 불가능하게 만드는 공격 기법

2. Slowloris의 개념 및 공격원리

가. Slowloris의 개념

- 웹 서버와 다수의 커넥션을 맺은 후 각 커넥션 별로 완료되지 않은 비정상 HTTP 헤더를 전송함으로써 웹 서버의 커넥션 자원을 고갈 시키는 DDoS 공격 기법
- HTTP 프로토콜(RFC 2616)에서 헤더와 바디를 개행문자(CRLF) 2 개로 구분한다는 점을 이용한 공격 방법

나. Slowloris의 공격원리



- Slowloris는 HTTP 프로토콜에 내재된 취약점을 공격하는 기법

3. RUDY의 개념 및 공격원리

가. RUDY의 개념

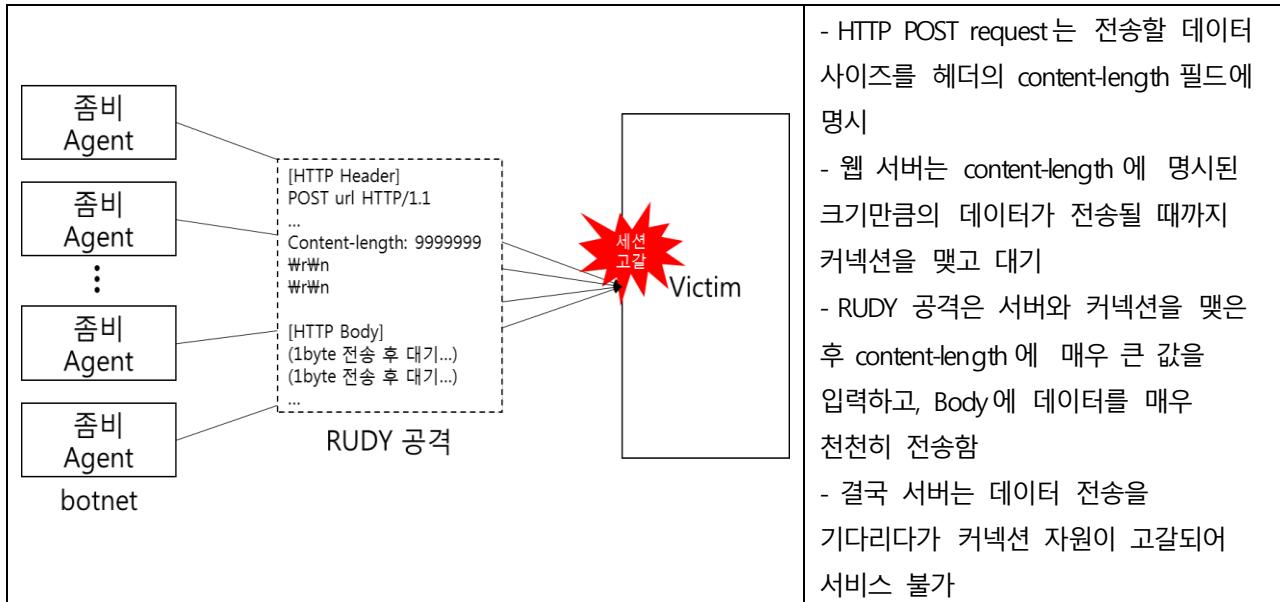
- 웹 서버와 다수의 커넥션을 맺은 후 각 커넥션 별로 데이터를 매우 느리게 전송함으로써 웹 서버의 커넥션

정보관리(2교시)

자원을 고갈시키는 DDoS 공격 기법(RUDY는 R-U-Dead-Yet 의 줄임 말)

- HTTP 프로토콜(RFC 2616)에서 POST method 사용시 헤더에 content-length 를 명시하도록 되어 있는데, 이때 데이터 전송에 대한 제약사항이 없는 점을 이용한 공격 방법
- 큰 데이터를 보낼 예정이라고 명시한 후 작은 단위로 전송하여 커넥션을 점유하는 방식

나. RUDY의 공격원리



4. Slowloris 와 RUDY에 대한 대응

Slowloris 대응	RUDY 대응
<ul style="list-style-type: none"> - HTTP GET 요청에서 CRLF 구분자를 1번만 사용하는 패킷을 원천 차단(시그니처 탐색) 	<ul style="list-style-type: none"> - Content-length 임계치 설정 - Request timeout 설정(실제로 네트워크 상태가 좋지 않아 데이터 전송이 느린 경우도 있으므로 운영 환경에 맞게 설정)
(공통)	
<ul style="list-style-type: none"> - 최대 동시 접속에 대한 임계치 설정 - User-Agent 필드에 알려진 툴이 명시되어 있는지 패턴 매칭으로 사전 차단 - 웹 서버 보안패치 적용 및 최신 버전으로 업그레이드(IIS, Apache 등) 	

- 두 공격방식 모두 많은 패킷을 사용하지 않고도 서비스를 불가능하게 만드는 Application 계층 공격이므로 다양한 측면의 보안 대책 필요. “끝”

Notes

1	DDoS(Distributed Denial of Service)
문제	DDoS(Distributed Denial of Service) 공격유형에 따른 시스템 보호와 방어를 위해 사용하는 자원을 향시 모니터링하고 차단정책 수립하고 적용하는 것이 무엇보다 중요하다. DDoS의 공격 유형별 공격방식을 5 가지 이상 설명하고, 대응 절차와 DDoS 공격유형별 차단정책 적용 방안을 제시하시오.
도메인	정보보안
정의(개념)	DDoS는 네트워크에 많은 에이전트를 분산 배치하여 동시에 '서비스 거부 공격'을 함으로써 시스템이 정상적인 서비스를 제공할 수 없도록 만드는 해킹 방식으로 공격자와 방어자간의 가용성 확보관점의 대응 필요
키워드	체크포인트, 공격유형, 차단정책, 사후조치, 대역폭 소진, 웹 서버 자원소모, DB Connection 부하, 봇, 브라우저 식별 대응, Flooding
목차제시	<ol style="list-style-type: none"> 1. DDoS 공격 개요 및 대응 방향 2. DDoS 공격 유형별 공격방식 3. DDoS 공격 대응 절차 및 공격유형에 따른 대응방안 3. 공격대응 후 사후조치
출제배경	DDoS 공격이 관련 이슈가 자주 등장하며, DDoS의 대응절차 및 대응방안까지 이해
답안작성전략	DDoS 공격에 대한 세부적인 설명과 대응절차 및 대응방안에 정책적인 요소를 감안하여 상세하게 답안 작성
난이도	★★★☆☆ (별 5 개기준)
참고문헌	DDoS 공격대응 가이드, 2012.10, 한국인터넷진흥원
문제풀이	홍성우 PE (제 84 회 정보관리/innoitpe@daum.net)

■ DDoS 공격 유형별 공격 방식

공격유형	공격방식
TCP SYN Flooding	다수의 TCP SYN 패킷을 보내 서버의 연결대기 큐를 고갈시켜 정상적인 서비스 연결 요청에 대해서도 응답할 수 없도록 만드는 공격
UDP/ICMP Flooding	대량의 UDP 또는 ICMP 패킷을 전송함으로써 네트워크의 과부하를 유발해 서비스 접속 장애를 발생시키는 공격
TCP Connection Flooding	다수의 정상적인 TCP 세션을 생성하여 서버 및 네트워크 장비의 CPU, 메모리 자원을 고갈시켜 정상적인 서비스 연결 요청에 대해서도 응답할 수 없도록 만드는 공격
SSL Connection Flooding	다수의 정상적인 SSL 세션을 생성하여 HTTPS 서버 또는 SSL 가속장비의 CPU 및 메모리 자원을 고갈시켜 정상적인 서비스 연결 요청에 대해서도 응답할 수 없도록 만드는 공격
HTTP GET Flooding (1:1, 1:N)	<p>정상적인 TCP 세션을 맺은 후 짧은 시간동안 반복적으로 다양한 웹페이지를 요청하여 서버의 과부하를 유발시킴으로써 원활한 서비스를 불가능하게 하는 공격</p> <p>* 1:1 : 하나의 TCP 세션에서 한번의 요청만을 수행하는 공격</p> <p>* 1:N : 하나의 TCP 세션에서 다수의 요청을 수행하는 공격</p>

HTTP GET Flooding (CC)	HTTP 요청에 캐시 저장 금지 관련 헤더를 설정하여 웹서버가 캐시된 컨텐츠를 재사용하지 못하고 항상 새롭게 응답을 반환하도록 하여 웹캐시 관련 장비 및 내부 실제 웹서버의 과부하를 일으키는 공격
HTTP GET Flooding (Random GET)	웹서버에 실제 존재하지 않는 컨텐츠를 반복 요청함으로써 웹캐싱 매커니즘의 Fail을 유발하여 웹캐시 관련 장비 및 내부 실제 웹 서버의 과부하를 일으키는 공격
DB Query Flooding	정상적인 TCP 세션을 맺은 후 게시판 등 동적 컨텐츠를 요청하여 웹서버 와 통신하는 백엔드 DB 서버의 과부하를 유발시킴으로써 원활한 서비스를 불가능하게 하는 공격
Slowloris	정상적인 TCP 세션을 맺은 후 미완성된 HTTP 헤더를 전송하여 공격 대상 서버가 연결을 유지한 채 계속 대기상태로 머물게하여 추가적인 접속 요청을 받아들일 수 없도록 만드는 공격
Hash Collision	POST 요청시 전달하는 매개변수를 조작하여 Hash 테이블에서 충돌이 발생하게 만들어 CPU 자원을 고갈시켜 원활한 서비스를 불가능하게 만드는 공격
Slow Read	정상적인 HTTP 요청을 보낸 후 응답을 천천히 받음으로써 HTTP 세션을 길게 유지하여 웹서버의 자원을 고갈시켜 원활한 서비스를 불가능하게 만드는 공격

■ DDoS 공격 대응절차

- DDoS 공격 대응은 공격자와 방어자간의 가용성 확보 싸움임
- 방어자는 자신이 관리하고 있는 웹 서버 및 방어시스템 자원의 한계점을 명확히 알고 있어야 함
- 운영자원의 자원 현황 모니터링 및 끊임없는 차단 정책 개선 없이 단순한 장비에만 의존하여 공격을 대응하는 것에는 한계가 존재
- 자원을 항상 모니터링하고 발생하는 DDoS 공격유형에 따른 차단정책을 찾고 적용하는 것이 중요



대응 절차	내용
공격 인지를 위한 체크포인트	웹서비스 관련 이벤트 발생 시 해당 원인이 DDoS 공격으로 인한 것인지에 대한 명확한 판단 필요
DDoS 공격유형 파악	DDoS 공격 유형을 명확히 파악하여 차단정책 설정을 위한 근거로 활용
공격유형에 따른 차단정책 정의 및 대응	공격의 유형과 목적을 명확히 판단하여 차단정책을 설정함으로써 웹 서비스의 가용성 확보

Notes

공격 대응 후, 사후조치	공격 트래픽 분석을 통해 공격 내용을 상세히 규명 추가 발생할 수 있는 공격 대비를 위해 정책을 업데이트, 좀비 PC IP 확보
------------------	--

■ 공격유형에 따른 대응방안

구분	공격유형	정책적용 장비	대응방안
대역폭 소진 공격	UDP Flooding, ICMP Flooding	Anti-DDoS	<ul style="list-style-type: none"> 웹서버 망을 보호하는 방화벽이나 웹서버망 상단에 위치한 라우터에서 해당 프로토콜을 차단하도록 ACL 설정
	TCP Flooding	Anti-DDoS, L7 Switch	<ul style="list-style-type: none"> 비정상적인 헤더 포함여부를 Filtering 하여 차단 대용량 TCP Flooding 공격은 프로토콜 기준으로 차단하는데 한계가 있어 소스 IP(Source IP)별로 PPS 임계치 설정
웹 서버 자원 소모 공격	Syn(Ack/Fin) Flooding	Anti-DDoS	<ul style="list-style-type: none"> 웹서버 OS의 TCP 스택(Stack) 자원을 소모하는 특징 <ol style="list-style-type: none"> 소스 IP 별로 PPS 임계치 설정 패킷 헤더검사를 통해 비정상적인 옵션 필드값을 가진 비정상 패킷 차단
	Slow Header Flooding Slow Data Flooding	L7 Switch	<ul style="list-style-type: none"> Anti-DDoS 장비로는 탐지 및 차단이 불가능 •L7 Switch의 iRule 기능을 이용하여 요청에 대한 차단정책(예: 타임아웃 기능)을 트래픽 분석 데이터를 기초로 도출 및 설정하여 차단 완료되지 않은 연결(Connection) 상태를 지속적으로 유지하는 공격이므로, 하나의 요청에 대해 연결 타임아웃을 설정하고 타임아웃이 지나면 연결을 종료시켜 차단
DB Connection 부하유발	Get Flooding, Post Flooding	L7 Switch	<ul style="list-style-type: none"> 다량의 HTTP 요청으로 웹서버와 DB 연동에 부하를 유발 시키는 것이 특징 Anti-DDoS 장비로는 탐지 및 차단이 불가능하며 L7 Switch에서 Signature 를 이용하여 차단 Source IP 당 요청 가능한 최대 회수를 임계치로 설정하여 차단
봇 vs 브라우저 식별 대응 방안		L7 Switch	<ul style="list-style-type: none"> Anti-DDoS 장비로는 식별이 불가능 L7 Switch에서 특정 코드로 응답하여 반응하는지 여부를 확인하거나 쿠키에 대해 응답하여 반응하는지 여부를 확인하여 차단 일반적인 봇은 브라우저와 달리 웹서버의 응답코드에 반응하여 행동하지 않으므로, 웹서버에서 302 moved temporary 와 같은 코드로 응답하여 봇이 발생시키는 요청을 차단

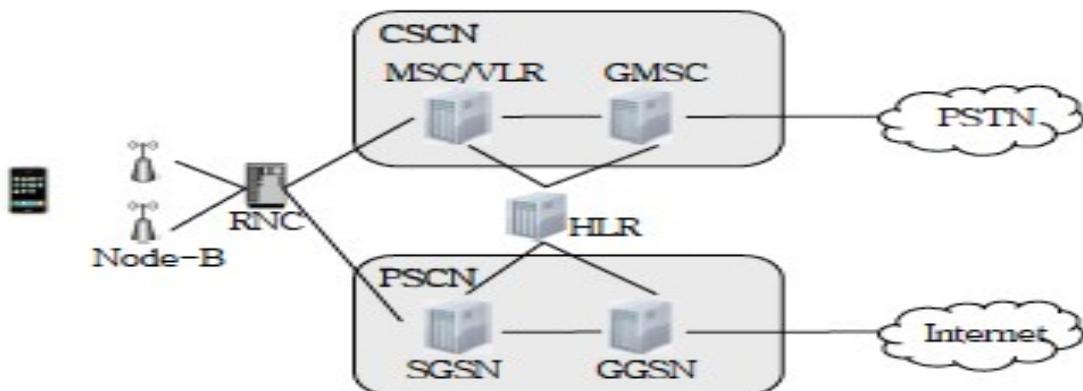
8

DDoS 공격은 여러 기업의 사례를 통해 이슈가 되었다. 이동통신 네트워크에서의 DDoS 공격기술을 설명하고, 이를 대비하기 위한 대응방안을 제시하시오.

출제도메인	보안
주요 키워드	- Address Scanning, 샘플링, Control Plane Attack, Low-rate Flooding Attack
출제배경	- 최근 이슈가 되고 있는 DDoS 공격의 이동통신 응용
난이도	★ ★ ★ ☆ (별5개 기준)
참고문헌	- 정보처리 학회지
출제기술사	최재준 기술사(제84회 정보관리기술사 / cjj329@daum.net)

1. 이동 통신 네트워크 DDoS 공격의 개요

가. 이동통신 네트워크의 구조



- CSCN : 음성 서비스를 위한 코어 네트워크
- PSCN : 데이터 서비스를 위한 코어 네트워크
- 음성 및 데이터 서비스를 위한 통합적 구성으로 진화

나. 이동통신 네트워크 구조 바탕의 취약점

- 1) 반복적인 연결 수립 요청에 무방비
- 2) 소량의 폭탄 패킷에 대한 탐지 방법 미흡
- 3) 이동통신 단말 접속 ID(IP 와 전화번호) 노출

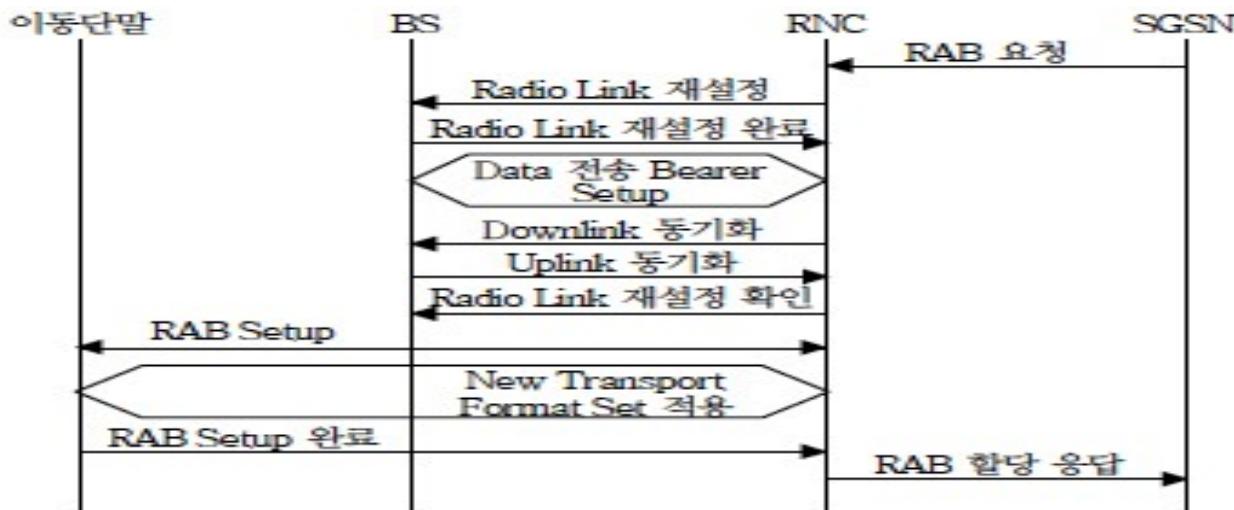
2. 이동 통신 네트워크 DDoS 공격기술

가. 이동통신 네트워크의 DDoS 공격 유형

유형	설명
Address Scanning	이동전화 번호 수집을 위해 인터넷 검색 수행 시스템 해킹 및 유출된 개인정보의 구입
샘플링	자동화된 공격 기술에서 많이 사용 전화번호 체계를 기반으로 한 랜덤 샘플링

나. 이동 통신 네트워크 DDoS 공격기술의 상세

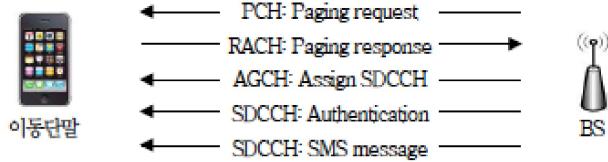
1) 네트워크 제어계 공격(Control Plane Attack)



- 공격 트래픽을 이용, 네트워크 운영을 위한 오버헤드 증가
- 소량의 연속적인 패킷을 주기적으로 전송
- RAB의 반복적인 생성과 삭제를 유발, RNC의 처리 방해

2) 자원 고갈형 공격(Low-rate Flooding Attack)

A. 문자 메시지 공격



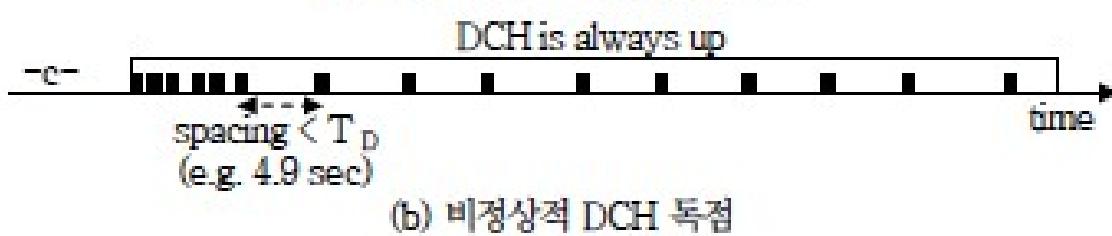
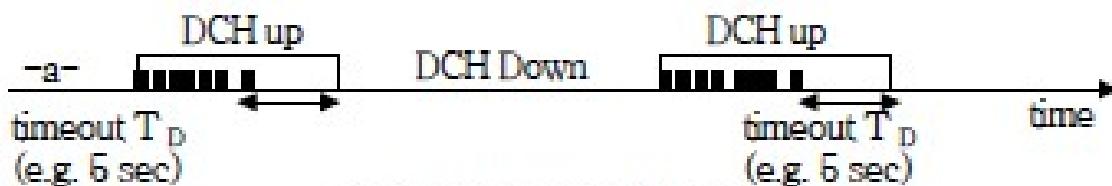
- SDCCH : 소량의 문자 메시지 전송을 위해 사용
- 공격자들은 SDCCH를 포화시키기 위해 메시지 전송
- 수 Mbps의 대역폭만을 사용하여 일반적인 DDoS로 탐지곤란

B. Paging 채널 공격

항 목	상세 내용
Paging 채널의 개념	<ul style="list-style-type: none"> - 상태 : idle(비접속), standby(접속대기), ready(채널 할당, 데이터 송수신 가능) - 이동 단말에 전달할 데이터가 있을 경우, 현재 위치파악 필요 - 해당 routing에 속한 모든 cell에 paging 신호 전달. - 이때 사용되는 무선 채널이 PCH
취약점	<ul style="list-style-type: none"> - PCH는 타 채널에 비해 상대적으로 적은 Band Width를 가진다는 점을 이용
공격 방법	<ul style="list-style-type: none"> - 최소 크기의 UDP 패킷을 주기적으로 전송 - 이동단말을 sub group으로 분류, sub group 별 순차적으로 데이터 전송

- 보안 관리자는 공격 트래픽과 flash crowd 트래픽 구별 곤란

C. 데이터 채널 공격

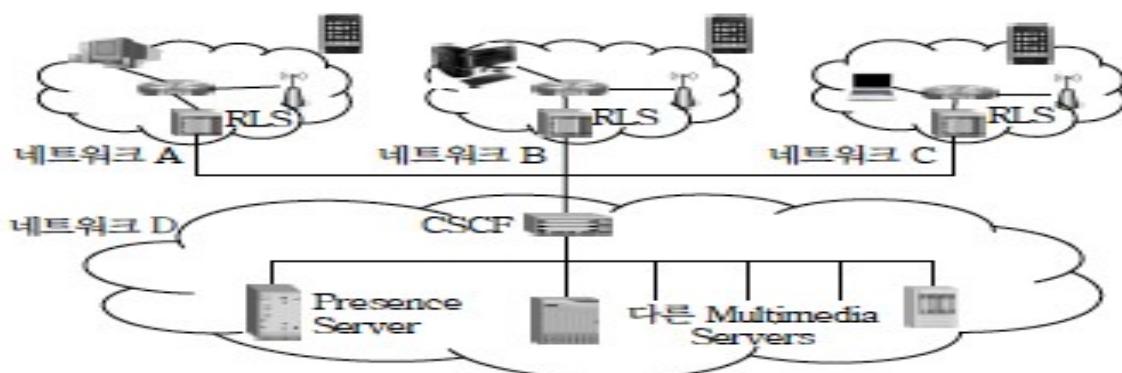


항목	상세 내용
데이터 채널의 개념	<ul style="list-style-type: none"> - 이동통신 네트워크에서 데이터 전송에는 DCH 와 FACH 가 사용됨 - 고속 전송 : DCH, 소량 데이터 전송 : FACH - 할당/전환 : 이동 단말의 상태와 전송 데이터 양에 따라 동적으로 결정됨. - FACH → DCH : 설정된 임계값에 따라 결정 - DCH → FACH : 타임아웃값에 따라 결정
공격 방법	<ul style="list-style-type: none"> - 설정된 임계값보다 조금 큰 값의 데이터 전송 - DCH 반복 직전에 소량의 데이터 전송 - 지속적인 채널 사용을 확보

- 일반적으로 사용되는 타임아웃 값이 약 5 초, 40 byte 소량 패킷을 사용하고 약 500 만 명의 이동단말을 공격한다고 가정할 경우, 약 1 Gbps 이하의 트래픽 만으로 대도시 공격 가능

3) 간접 공격 (Indirect Attack)

A. 인프라의 구조



- 다양한 멀티미디어 서비스를 위한 IMS 를 구축
- IMS 는 서비스 사용자들의 상태를 실시간으로 제공하는 presence service 를 기반으로 하는 특징을 지님

B. 인프라 구조의 문제를 이용한 공격 시나리오

항 목	세부 내용

1 차 공격	<ul style="list-style-type: none"> - 다수의 좀비 PC 를 이용하여 RLS 에 접속 - 복수의 RLS 는 동시에 이용자의 상태 확인 요청 - presence 서버에 요청 메시지 폭증, 서비스 거부
2 차 공격	<ul style="list-style-type: none"> - presence 서버 지연에 따른 재전송 요청 - 재전송 요청에 따른 CSCF 폭주 발생

– SNS 서버에 DDoS 공격 수행, 연쇄적인 네트워크 불통을 유발

3. 이동통신 네트워크 DDoS 공격 대응 기술

대응 기술	설 명	특징
Queue 관리	코어 네트워크의 라우터, 서비스 서버의 큐에 적용	<ul style="list-style-type: none"> - 공격의 효과 경감 - 오탐에 대한 문제 - Packet 손실비율 증가
	보안 게이트웨어 형태 제공 GTP 프로토콜 이상 탐지 트래픽 이상 탐지 제공	<ul style="list-style-type: none"> - 스팸 탐지/대응 가능 - GTP 트래픽 보안 미흡 - 외산 장비 위주

<<예비기술사 결론 시 참고>>

- 이동통신 네트워크가 4G 로 진화하면서 IP 와 연결되어 인터넷의 취약점이 그대로 전가되는 상황.
- DDoS 유형의 공격기술과 대응방안 고민 필요

“끝”

6	IP Spoofing		
문제	IP Spoofing 에 대해 설명하시요		
도메인	보안	난이도	★ ★ ★ ☆ ☆ (별 5 개 기준)
출제의도	최근 악화되고 있는 해킹 및 보안사고에 대한 대비가 강화되고 있고, DDOS 등 해킹사고에 많이 응용되고 있는 , 기본적인 유형인 IP Spoofing 에 대해서 이해 및 관련 기술들을 숙지하고 있는지 확인		
핵심 내용 키워드	Sniffing, TCP SYN Flooding, rsh, rlogin, ACK		
목차예시	<ol style="list-style-type: none"> 1. IP 프로토콜의 인증취약점을 악용한 IP Spoofing 의 개요 2. IP spoofing 의 공격절차 및 대응방안 <ol style="list-style-type: none"> 가. IP spoofing 의 공격절차 설명 나. IP spoofing 의 대응방안 3. IP spoofing 과 ARP spoofing 의 차이점 비교 		
채점 점수 가이드	<ol style="list-style-type: none"> ① IP spoofing의 개념, 이해 부족 (1~2점) ② IP spoofing의 기본 이해 수준 (3~5점) ③ IP spoofing의 정확한 기술 제시 (5~6점) ④ IP spoofing의 추가요소 설명(+α) 		
참고문헌	Spoofing attack (2012. PartPress)		
고득점전략 및 답안작성 가이드	IP Spoofing 의 정확한 개념 및 공격절차의 구성도 및 설명, 대응방법이 풍부하게 설명되면 고득점에 유리하며, 기본 토픽들에 의외로 개념이 정확히 정립인 안된 경우가 많으므로 기본토픽에 충실히 학습계획이 필요함..		
출제자	김보균 기술사 (제 110 회 컴퓨터시스템응용기술사 / robottakwonv@naver.com)		

컴퓨터시스템응용(1교시)

1. IP 프로토콜의 인증 취약점을 악용하는 IP Spoofing 의 개요

인증 : IP의 source Address로 상대를 식별 및 인증

- 암호화 과정이 없고 IP 헤더를 고칠수 있음

세션보호 : IP의 Sequence Number로 세션인증

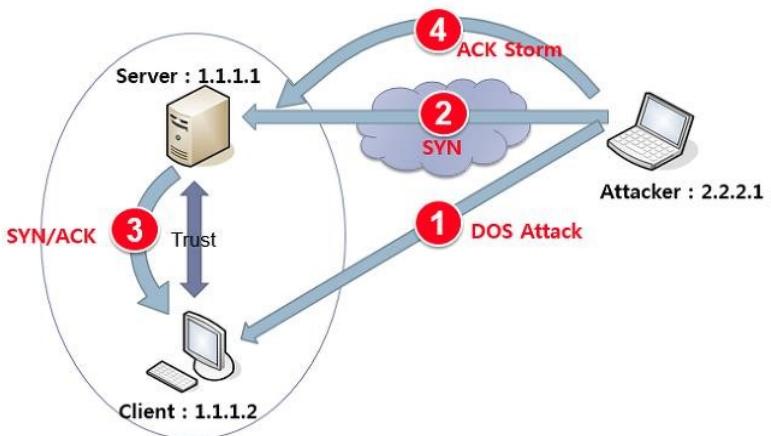
- Sequence Number는 추측이 가능하게 설계됨

IP Spoofing

- IP 프로토콜의 인증취약점을 이용하여 공격자가 자신의 IP Address 를 공격하고자 하는 네트워크의 호스트의 IP Address 로 바꿔 IP 기반의 인증을 무력화 시키는 공격

2. IP Spoofing 의 공격 절차 및 대응 방안 세부 설명

가. IP Spoofing 의 공격 절차



1	공격자는 클라이언트에 TCP SYN Flooding 공격	rsh(513), rlogin(514)
2	공격자는 클라이언트의 IP로 속여 서버에 연결을 요청	Sniffing
3	서버는 클라이언트에서 온 패킷으로 알고 클라이언트에 SYN/ACK 패킷을 보낸다. 하지만 클라이언트는 TCP SYN Flooding 공격 때문에 연결이 이루어지지 않고 서버가 보낸 패킷은 사라지게 되어 SYN/ACK 패킷을 받았는지 확인할수 없게 된다	SYN/ACK 패킷 분실
4	공격자는 클라이언트에서 ACK 패킷을 보낸것처럼 속이면서, IP Spoofing 명령어가 들어있는 패킷을 보내 신뢰관계에 있는 클라이언트라고 속이면 연결이 이루어진다.	IP Spoofing 완료

- 서버와 클라이언트는 신뢰관계(Trusted)에 있으며, Trusted 관계는 서버에 클라이언트가 접속할 때 ID를 입력후 패스워드를 요구하지 않는 관계를 의미함.

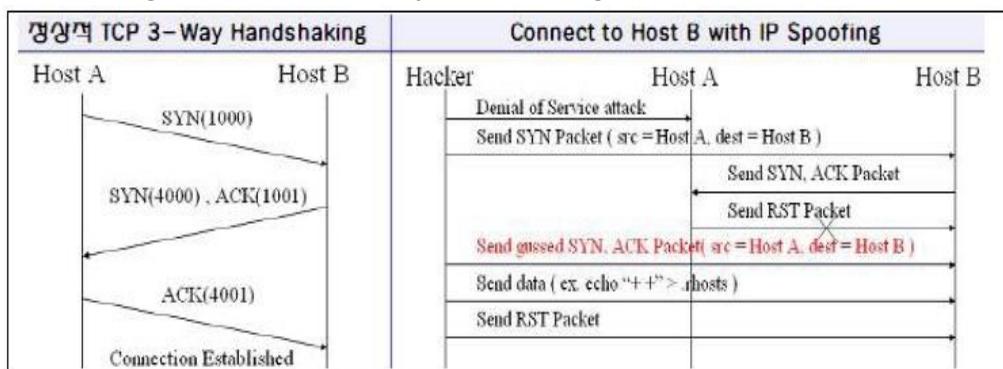
나. IP Spoofing 의 대응 방안

구분	대응방안	설명
Trusted관계	미사용	네트워크에서의 Trusted 관계를 미사용하여 사전 방지
Mac주소지정	Static 설정	부득이 하게 Trusted를 사용할경우 Static으로 지정하면, 공격자가 연결을 끊을수 있으나 클라이언트의 IP로 위장하여 접근하더라도 MAC주소까지는 같을수 없음

Sniffing방지	모니터링	NMS, Packet 모니터링을 통해 Sniffing을 방지하여 원천적으로 IP Spoofing 을 차단할수 있다.
기타	관리적보안	접근제어, DRM, PC(단말)보안

- IP Spoofing 의 유형에는 Packet 을 볼수 있는 Non Blind 형과 Blind 형이 존재함

3. IP Spoofing 과 정상적 TCP-3way Handshaking 과의 비교



- 정상적인 TCP 3-way Handshaking에 IP Spoofing 을 이용해서 attacker 가 접속하게됨

-끝-

6. IP Spoofing에 대해 설명하시오

컴시용

1쪽

번호) IP Spoofing 정의.

정의) IP 프로토콜을 이용해 IP Spoofing의 원리.

1. IP 프로토콜을 이용해 IP Spoofing의 원리.

- 악의적인 공격자가 IP 주소를 그 자신의 실제 주소와 같은 다른 공격자의 주소로 바꿔서 공격하는 기법.

특징 : IP Protocol 특징, 해당 IP 변경 용이.

2. IP Spoofing 공격 개념도 및 실행 과정.

가. IP Spoofing 공격 개념도

나. IP Spoofing 공격 실행 과정.

번호	작업	설명
공격 초기	DDoS	다수의 공격자가 상대방을
	IP Spoofing	별 IP 주소 IP를 위장
Web 접속	SYN.	Web server에 접속
	Ack SYN.	웹 접속 부여자로 표시되도록
	Ack.	공격자가 대신 응답해 연결
결과	결과	결과로 차단해 대응

결과로 차단해 대응으로 차단해 대응

kpc 한국생산성본부

2쪽

번호) IP Spoofing 대응 방법.

- ARP 대처 : MAC 주소 대처로 MAC 주소
- 네트워크 대처 : 외부에서 들어온 IP Null 대처

마지막

kpc 한국생산성본부

2

OAuth (Open Authorization)에 대해서 설명하시오.

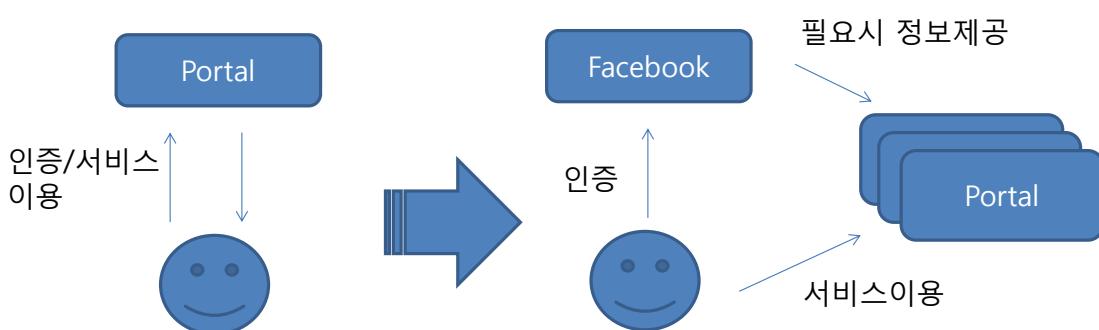
출제도메인	보안
주요 키워드	- users, consumer, service provider
출제배경	- SNS의 확산과 Open API를 활용한 개발에서 포털의 인증 표준에 대한 이해
난이도	★ ★ ★ ☆ ☆ (별5개 기준)
참고문헌	- 위키피디아
출제기술사	서정훈 기술사(제90회 정보관리기술사 / neom3620@gmail.com)

1. 3rd Party 인증, OAuth (Open Authorization)의 개요

가. OAuth (Open Authorization)의 개념

- 사용자의 데이터가 있는 웹 사이트 이외의 웹 사이트에 사용자의 신임 정보(예: 사용자 이름 및 암호)를 노출하지 않고도 하나의 웹 사이트에 저장된 개인용 리소스를 다른 사이트와 공유할 수 있는 **OpenAPI**로 개발된 표준 인증 방식

나. OAuth의 등장배경



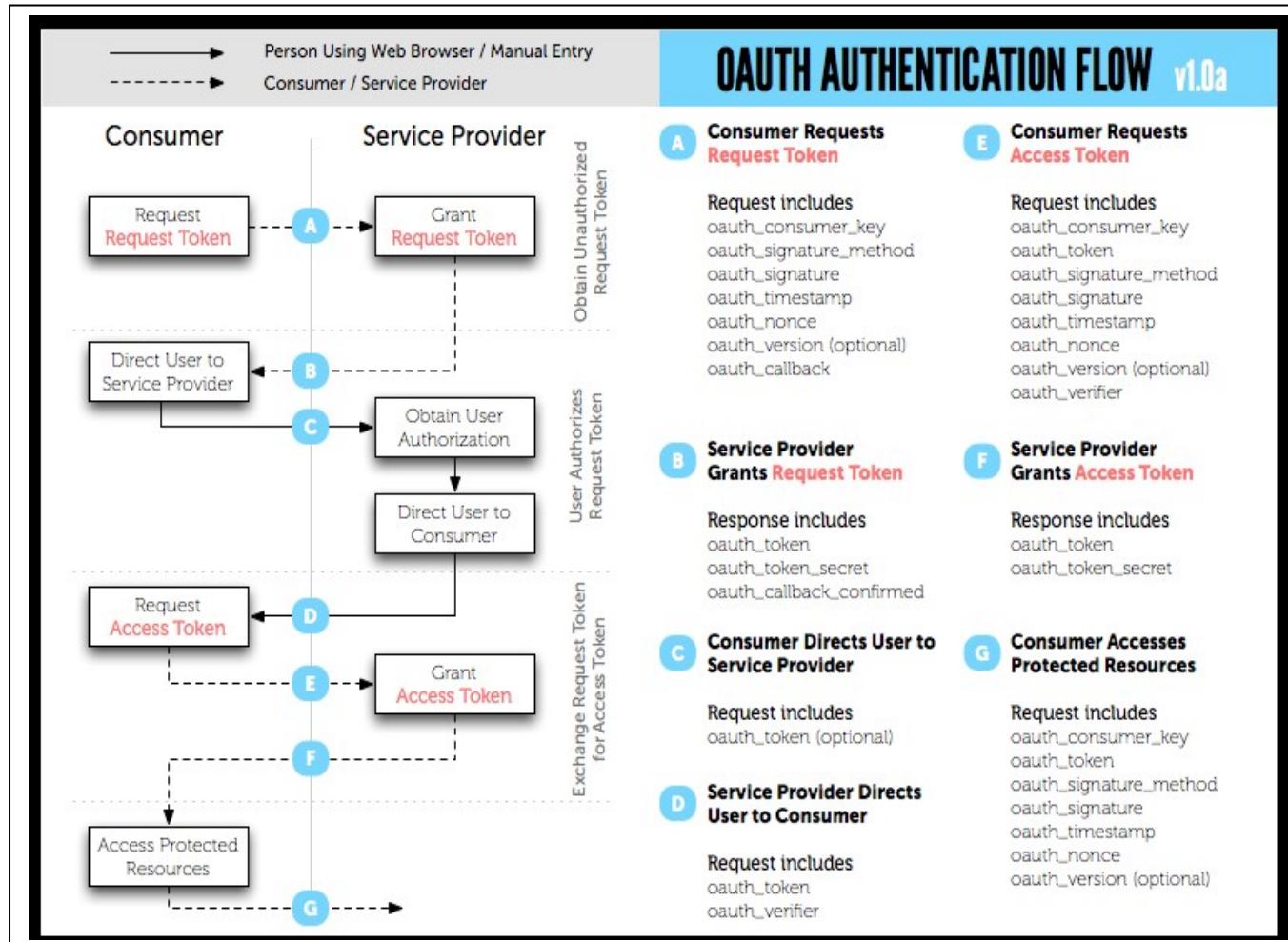
- 과거에는 각 사이트마다 인증 정보를 확인하고 서비스를 이용하는 것이었다면 소셜 네트워킹의 확산으로 Twitter, Facebook과 같은 소셜 네트워킹 웹 사이트를 서로 매쉬업하는 데 필요한 3rd party 인증이 등장
- 보호된 리소스를 노출하는 위험 없이 여러 웹 사이트 사이에서 공유할 수 있도록 지원하는 오픈 프로토콜 등장

2. OAuth 관련 용어 및 인증절차

가. OAuth 관련 용어

항목	내용
사용자(users)	서비스 공급자의 계정이 있는 개인
소비자(consumer)	OAuth를 사용하여 서비스 공급자에 액세스하는 웹 사이트 또는 애플리케이션
서비스 공급자(service provider)	OAuth를 통한 액세스를 지원하는 웹 애플리케이션
소비자 비밀번호(consumer secret)	서비스 제공자에서 소비자가 자신임을 인증하기 위한 키
요청 토큰(request token)	소비자가 사용자에게 접근권한을 인증 받기 위해 필요한 정보가 담겨있으며 후에 접근 토큰으로 변환됨
접근 토큰(access token)	인증 후에 사용자가 서비스 제공자가 아닌 소비자를 통해서 보호된 자원에 접근하기 위한 키를 포함한 값

나. OAuth 인증 절차



처리순서	내용
A	소비자가 서비스제공자에게 요청토큰을 요청
B	서비스 제공자는 요청토큰을 발급하고 소비자 사이트로 리다이렉트
C	소비자는 요청토큰을 받고 콜백과 함께 서비스 제공자로 리다이렉트 사용자는 이 시점에서 서비스 제공자 사이트에 로그인하고, 소비자에게 데이터를 제공 하는데 동의하거나 거부함. 동의하게 되면 요청토큰이 인가됨
D	서비스 제공자에서 소비자로 리다이렉트
E	소비자에서 서비스 제공자로 리다이렉트하면서 접근토큰을 요청
F	서비스 제공자는 접근토큰을 발급하고 소비자로 리다이렉트
G	소비자는 접근토큰을 이용하여 서비스 제공자의 보호되는 리소스에 접근

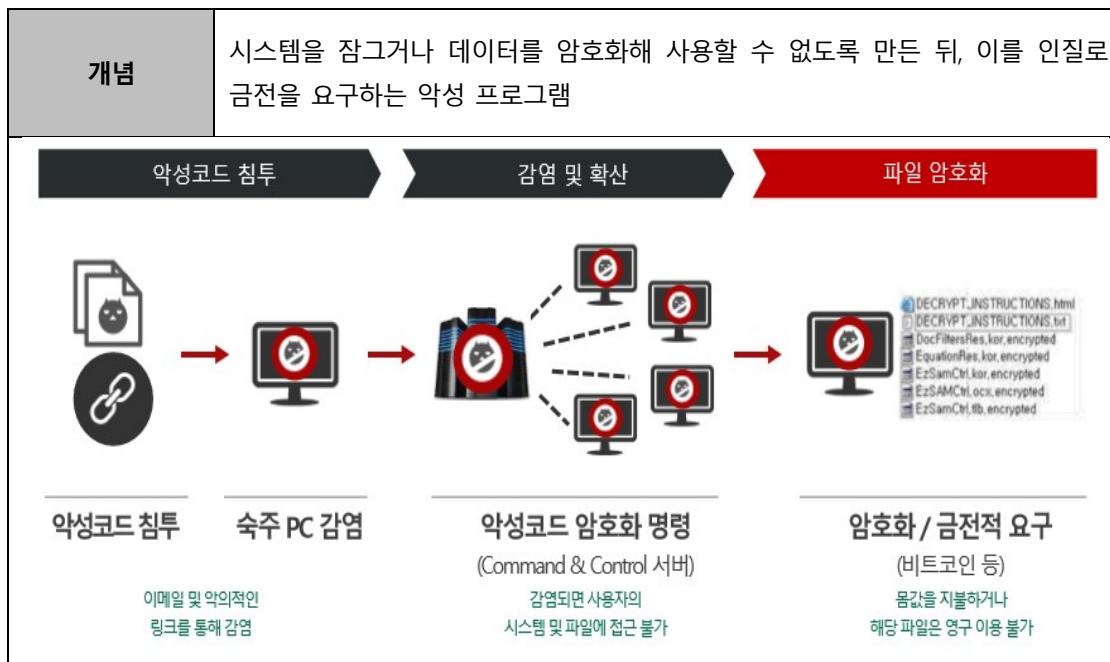
3. OAuth 활용현황

- 1) 국내 : 네이버, 네이트온은 OAuth 1.0 제공
- 2) 해외 : 트위터는 OAuth 1.0, 구글은 OAuth 1.0/2.0, 페이스북은 OAuth 2.0 제공

Notes

3	랜섬웨어
문제	랜섬웨어 공격에 대하여 사전, 사후적 대응방안을 기술적, 관리적 관점에서 설명하시오.
도메인	정보보안
정의	시스템을 잠그거나 데이터를 암호화해 사용할 수 없도록 만든 뒤, 이를 인질로 금전을 요구하는 악성 프로그램
키워드	인질, 금전요구, 드라이브바이다운로드, 유형(크립토락커, 테슬라스크립트, 롤키 등등), 사전사후대책
출제의도분석	상반기 다양한 랜섬웨어 발생으로 사회 이슈가 된 상황에서 기술사로써의 대응방안을 제시할 수 있는지 확인.
답안작성 전략	실제 발생했던 사례, 유형 중심의 랜섬웨어를 간략히 설명 후 다양한 측면의 대응방안 중심의 답안 작성 전략 필요
참고문헌	한국랜섬웨어침해대응센터 http://blog.skinfosec.com/221004087762 ESTSoft 보안 솔루션 소개자료
모범목차	<ol style="list-style-type: none"> 암호화 후 금전요구 피해, 랜섬웨어의 개요 랜섬웨어 공격의 사전 대응방안 랜섬웨어 공격의 사후 대응방안 랜섬웨어 공격에 대비한 물리적 대응방안
풀이 기술사님	박주형 PE (제 111 회 정보관리기술사 / joohyung1002@naver.com)

1. 암호화 후 금전요구 피해, 랜섬웨어의 개요



- 랜섬웨어는 Ransom(몸값)과 Software(소프트웨어) 합성어로, PC 에 있는 중요한 자료를 암호화 후, 피해자에게 돈을 지급하도록 강요하는 악성코드.
- 사전, 사후로 나눠 기술적, 관리적 대응방안이 중요함

2. 랜섬웨어 공격의 사전 대응방안

가. 기술적 관점의 사전 대응방안

대응 방안	설명
원격 Backup 저장	PC 와 분리된 저장소의 백업
파일접근관리	파일의 편성, 등록, 보수, 기밀 유지, 공용이나 파일에의 접근 등을 조작적으로 관리
읽기 전용 권한 설정	읽기 전용 폴더로 변경하여 해당 폴더의 파일이 감염 최소화
문서 중앙화 솔루션 도입	중앙 문서 관리 서버를 통한 백업 및 보안 통제 강화
망분리 적용	내외부 네트워크망 분리를 통한 외부의 접근 제한
백신 소프트웨어 설치	주기적인 악성코드 확인 및 모니터링 진행 최신 백신상태의 유지
랜섬웨어 피해 방지 솔루션 설치	- 랜섬웨어침해대응센터의 솔루션 및 지능형 행위기반 랜섬웨어 탐지 솔루션 설치 - VirusTotal Public API v2.0을 이용한 바이러스, 웜, 트로이 목마 등이 포함된 악성 콘텐츠가 파일과 URL에 포함되어 있는지 분석하는 무료 온라인 서비스
파일 확장자 변경	암호화 대상 문서를 판단하지 못하도록 확장자 변경
이메일 내용 이미지화 수신	수신된 메일을 이미지로 읽어들어 선 확인.

나. 관리적 관점의 사전 대응방안

대응방안	설명
이메일 관리	이메일의 첨부된 파일을 열지 않도록 하고 열게 될시 확인 절차를 걸쳐 파일을 열어볼 수 있도록 대응
파일 송신 확인	- 요청한 자료가 아니면 유선 등으로 발신자와 확인 후 실행. - 메신저나 문자메시지에 첨부된 링크를 무심코 누르거나, p2p 등을 통해 내려받은 파일을 실행할 때도 주의.
OS 및 보안 SW 최신상태 확인	업무 pc 의 보안 SW 가 최신 상태임을 주기적 확인
공유 폴더 관리	최소한의 접근 권한 부여를 통한 공유 폴더 접근 통제 관리
자료 버전관리	백업 및 히스토리 관리를 위한 버전관리
백업정책 마련	주기적 파일을 백업할 수 있는 정책의 마련

3. 랜섬웨어 공격의 사후 대응방안

가. 기술적 관점의 사후 대응방안

대응방안	설명
손실 데이터 복원	백업 서버에 연결을 통한 문서 및 파일의 복구
네트워크 접속 차단	랜섬웨어 진단시 네트워크 자동 연결 차단
자료 반출입에 대한 추적	로그인, 접속 기록 조회를 통한 원인의 판단
시스템 리부팅 옵션 적용	피해 확산을 줄이기 위한 시스템 리부팅 솔루션 적용
실시간 감지 백업	미처 백업하지 못한 데이터에 대하여 실시간 백업 적용

Notes

나. 관리적 관점의 사후 대응방안

대응방안	설명
인터넷선과 PC 전원 차단.	랜섬웨어 발견시 물리적 랜선과 pc 전원의 차단
침해 사례 전파	증거 보존 상태에서 신속한 보고 및 신고
전문 기관과의 상담	평소 해킹 상담, 피해 신고, 원격 점검 등을 한국인터넷진흥원 인터넷침해대응센터를 통한 진행

4. 랜섬웨어 공격 단계별 대응방안



- 랜섬웨어 공격은 점차 상업화, 고도화 될 것으로 보임. 우선적으로 사전 예방책도 중요하지만 피해 규모도 축소 시킬 수 있는 사후 대응책 마련도 고려해야 함.

"끝"

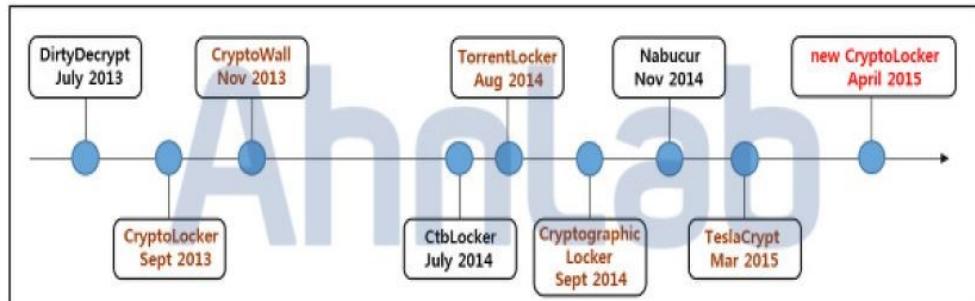
2	랜섬웨어		
문제	<p>최근 랜섬웨어는 다양한 형태의 변종을 중심으로 빠르게 진화하고 있다. 다음에 질문에 대해 설명하시오.</p> <p>가. 변종 랜섬웨어의 종류와 특징 나. 랜섬웨어의 감염경로 다. 대응방안</p>		
도메인	보안	난이도	★ ★ ★ ☆ ☆ (별 5 개 기준)
출제의도	랜섬웨어에 대한 피해가 계속적으로 증가하고 있고 최근 변종 랜섬웨어에 의한 개인 및 기업에까지 그 피해 범위가 확대되고 있음. 110 회에 출제 되었으나, 좀 더 세부적인 내용으로 출제가 가능하기에 변종 랜섬웨어의 종류뿐 아니라 대응방안에 대해 상세히 학습할 필요가 있음.		
핵심 내용 키워드	<ul style="list-style-type: none"> 화면 잠금형 랜섬웨어 및 파일 암호화 랜섬웨어 신종 Locky 이슈화가 된 크립토락커, 원본파일 복구 가능한 테슬라크립토 및 크립트XXX 드라이브 바이 다운로드, 매그니튜드 안티 랜섬웨어툴, 최신버전 패치, 의심되는 이메일 삭제 		
목차예시	<ol style="list-style-type: none"> 신종 사이버 범죄 랜섬웨어의 진화, 변종 랜섬웨어 개요 변종 랜섬웨어의 종류 및 특징 변종 랜섬웨어의 감염경로 진화하는 랜섬웨어 대응방안 		
채점 점수 가이드	<ol style="list-style-type: none"> 개념, 이해 부족 (1~8점) 기본 이해 수준 (9~14점) 정확한 기술 제시 (14~15점) 추가요소 설명(+α) 		
참고문헌	안랩 최신 보안뉴스, 보안신문, 110 회 컴퓨터시스템응용 1 교시		
출제자	이형석 기술사(제 108 회 컴퓨터시스템응용기술사 / ddrseok@naver.com)		

1. 신종 사이버 범죄 랜섬웨어의 진화, 변종 랜섬웨어 개요

가. 변종 랜섬웨어의 개념

기존의 대칭키 알고리즘이 아닌 비대칭키 알고리즘을 사용하여 대응을 어렵게 만든 악성소프트웨어

나. 변종 랜섬웨어의 동향



- 랜섬웨어 중 크립토락커는 2013년 9월 처음 발견, '크립토월', '토렌트락커', '테슬라크립트' 등의 이름으로 변형들의 지속적인 유포. 2016년 록키의 등장.

2. 변종 랜섬웨어의 종류와 특징

가. 변종 랜섬웨어의 분류

화면잠금형 랜섬웨어	파일 암호화형 랜섬웨어
바탕화면 전체를 사용 불가능 상태로 만들고 금전을 요구. 안전모드로 부팅하여 백신 등으로 치료하거나 원도우 시스템 복원을 통해 이전을 원복 가능. 단, 감염되기 전 복원 기능을 사용하고 있어야 가능.	사용자의 파일이 암호화된 사실을 텍스트파일, HTML 파일 등으로 알림. 다른 시스템을 사용할 수 있으나 각종 문서파일이나 개발소스, 데이터베이스 등 주요한 사용자 파일을 암호화 하므로 정상적으로 실행 불가.

나. 변종 랜섬웨어의 종류 및 특징

구분	랜섬웨어 설명	특징
Locky(록키)	해당 압축 파일 내에 Locky 랜섬웨어를 다운로드하는 JavaScript 파일이 존재하며 이를 실행할 경우 랜섬웨어 실행 파일을 다운로드 하며 시스템 감염을 진행.	JS파일 존재 확장자.locky
Cerber(서버)	PE 파일의 리소스 영역 안에 미리 RSA 공개키를 보관 함. 또한, 감염 대상, 감염 방법 등도 함께 저장되어 있어 따로 C&C 서버와의 실시간 통신이 필요없음.	비주얼 베이직 스크립트를 생성해 경고문구를 직접 음성으로 읽음.
CryptLocker(크립토락커)	exe파일을 생성하며 레지스트리에 등록하여 재부팅시 자동 실행을 수행.	확장자.encrypted. Tor 네트워크 사용
TeslaCrypt(테슬라크립트)	%APPDATA% 경로에 생성한 악성코드 실행을 통해 감염됨.	Key.dat로 파일 복원가능 AES 암호화의 CBC사용

3. 변종랜섬웨어의 감염경로

구분	감염경로	사용기술
Locky(록키)	주로 이메일 첨부파일에 가짜 송장 파일이나 급여 명세서와 같은 파일을 통해 감염	스피어피싱
Cerber(서버)	유포 경로는 주로 광고 서비스의 정상적인 네트워크를 이용하여 악성코드를 유포함.	멀티타이징
CryptLocker(크립토락커)	IT 커뮤니티인 클리앙 광고배너를 통해 유포되어짐.	웹 기반의 DBD(Drive-By-Download) 방식.
TeslaCrypt(테슬라크립트)	%APPDATA% 경로에 생성한 악성코드 실행을 통해 감염됨.	스피어피싱, DDOS

- CryptXXX 의 경우 웹을 통해 DLL 형태로 유포되고 정상적인 프로세스를 호출하게 하여 동작.

4. 진화하는 랜섬웨어 대응방안

가. 감염원인에 따른 예방방안

감염원인	원인 및 예방방안	공통 예방방안
드라이브바이다운	바이러스토털(virustotal.com)과 같은 안내 사이트를	

컴퓨터시스템응용(2교시)

로드	활용하여 사전 확인	중요 자료 백업과 취약점 보안패치 안티랜섬웨어 툴 사용하여 보호 폴더 설정하여 문서파일 사전 보호
스크립트 실행	게시자를 확인할 수 없는 소프트웨어 실행 금지	
플래시	플래시 차단 (브라우저 수준에서 차단가능)	
멀버타이징 (광고배너 클릭)	- 광고 배너 클릭 금지 - Sandbox 솔루션 사용	

- 근본적인 예방 방안은 중요 데이터에 대한 충분한 보안과 백업이며, 시스템 운용 시 최대한 확인되지 않은 외부환경에의 노출을 최소화 해야 함.

나. 감염 후 조치방안

조치방안	설명	조치 시 확인내용
시스템 복원	시스템에 설정되어 있는 복구 시점으로 돌아가서 해당 시점으로 데이터 복원	시스템 복구 영역이 존재하는지 확인 필요
암호화 해제	암호화 된 파일들을 복호화 - 디크립토락커(decryptcryptolocker.com) 사이트에서 복호화 가능여부 확인 - 안랩 Cryptxxx 복구툴 전용백신 사용	랜섬웨어의 종류에 따라 복호화가 불가능한 경우 있으므로 확인
제거툴 사용	윈도우 PC 의 경우, 부팅 시 F8 키로 command line 모드로 부팅하여 cryptolocker removal tool 적용	도구 적용 후 데이터 손실이 발생할 수 있으므로 적용 시점을 선택해야 함

- 기본적으로 감염 후에는 인터넷 연결을 차단하여 연결된 네트워크를 통한 2 차 감염을 막아야 함

고득점 전략 및 학습가이드	계속 업데이트 되고, 새롭게 등장하고 있는 랜섬웨어들에 집중해서 풀이 해야 합니다. 특히 최근의 랜섬웨어는 개인을 타겟으로 하기보다는 기업의 구성원들을 타겟으로 하는 추세입니다. 고득점을 위해서는 최근 보안 이슈나 뉴스에 관심을 갖고 문제가 되는 세부 랜섬웨어 기법에 대해서도 숙지함은 물론 최근의 경향도 짚어주면 좋을 것 같습니다.
----------------------	--

11. 랜섬웨어(Ransomware)의 공격방식과 대응방안에 대해 설명하시오.

정보관리

번호 문제) 랜섬웨어의 공격방식과 대응 방안		
답)	65	
I. 컴퓨터내의 데이터를 악으로하는 유품요. 랜섬웨어가요 - 공격자의 악성 프로그램이 사용자 PC에 설치되면 데이터를 암호화하여 이를 해제하기 위한 금전 요구공격 - Drive by download 방식, 금전요구, 크립토월, AES		
II. 랜섬웨어의 공격 방식 가. 랜섬웨어 공격 전차도		
- 사용자가 랜섬웨어 설치·설정시 암호화하여 피해당함		
나. 랜섬웨어 공격 전차 세부 설명		
전차	세부 설명	설명
공격·설치	Drivebydownload Exploit	사이트 접근 시 다운로드 취약점 이용 공격
암호화·금품요구	암호화 금품요구	AES 기반암호 수행(암호화) Bitcoin이나 대출통장암호
학습	암호화해제 다른공격	암호화 해제 요구 도박 추가 공격 대상

III. 랜섬웨어 (Ransomware)의 대응방안		
대응방안	세부방안	설명
악성Site	Safe URL	안전한 사이트 확인 후 접속함. 접두사인 .kr/.net/.com
접근금지	브라우저설정	파일 다운로드 무분별하기 되는 것을 방지하는 설정
백업	Data백업	데이터는 주소로 백업하여 감염되었을 경우 되돌림
폐지	OS·APP	OS·Application의 주약점 폐지 수행으로 예방
- 사용자 스스로 보안의식을 가지고 대응·예방 중요!		

6. 사이버공격이 지능화됨에 따라 다양한 방법으로 공격이 되고 있다. 최근 이슈가 되는 DBD(Drive by Download)와 랜섬웨어에 대해 설명하고 각각의 대응방안을 설명하시오. 그리고 사이버공격에 대한 보안강화 및 능동적 대응을 위한 보안 네트워크를 구성하시오.

시스템응용

~~문제 6) DBD / 랜섬웨어 심포지엄 대응방안~~

사이버 공격 대응 모임 간라 대응 세 구조

I. 자동화된 사이버 보안 대응의 흐름식

① 사이버공격에 대한 대응
② 자동화된 보안 대응

II. 사이버 공격의 저작자, 그로 인해 따라
는 결과, 가능한 사이버 보안 대응이 있다.

II. 가능한 공격 기법. DBD 설명.

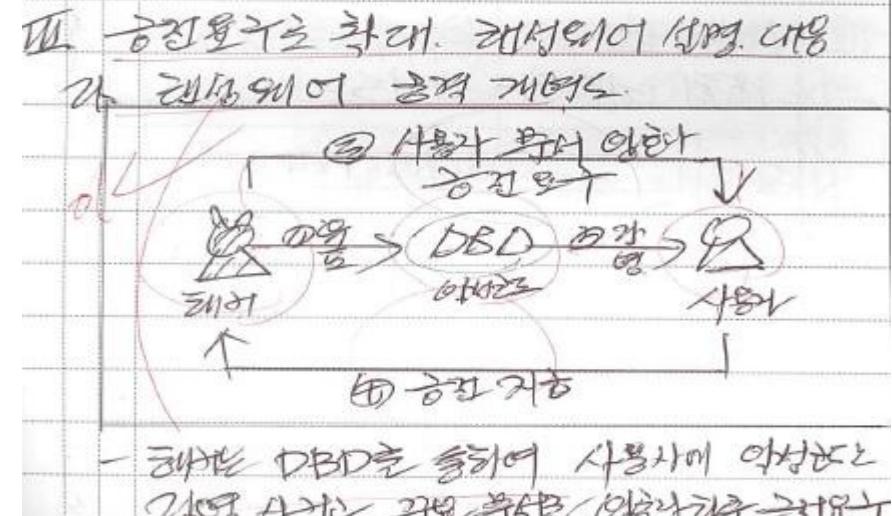
가) DBD 공격 원리도

① 사용자
② 애플리케이션
③ 네트워크
④ 후花园

- 사용자가 민족화한 상태에서 웹사이트를
인수하는 경우가 가능이 되는 악성 공격 기법.

번호	내 DBD 주제 대응 방안	구 분	방 법	비 용
1	보안 제작 - KBSNS, DBNS 등	서 비	서비스	- 일상 강간자, 암호화
2	설정 - 사용자 설정, 보호자 설정 등. 균형	설정	설정	- 주기적 등의 취약점
3	운영 관리 - 보안수칙 체계 마련	운영 관리	운영 관리	- 기관 내부 정부는
4	감시 체계 - 개인정보 수집 및 이용	감시 체계	감시 체계	- 개인정보 수집 및 이용
5	PC 미처방 - 초기화 미처방	PC 미처방	PC 미처방	- 초기화 미처방
6	사용자 교육 - 유타 카드, 전문 유도	사용자 교육	사용자 교육	- 유타 카드, 전문 유도

정부 예산 GAO 설치, 개인정보와 사용권

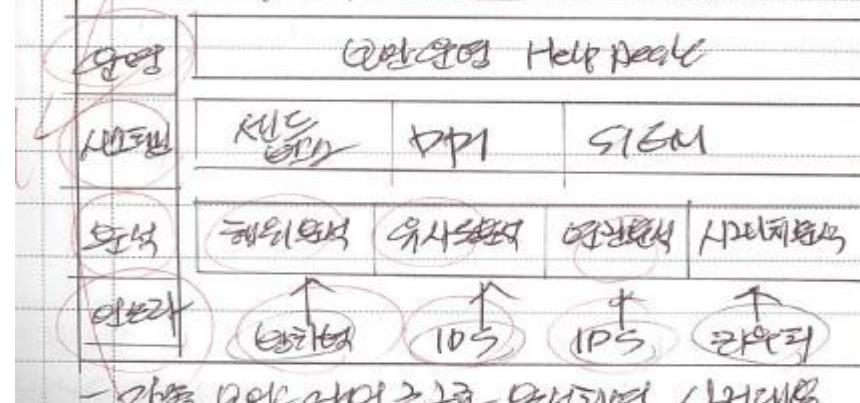


6. 사이버공격이 지능화됨에 따라 다양한 방법으로 공격이 되고 있다. 최근 이슈가 되는 DBD(Drive by Download)와 랜섬웨어에 대해 설명하고 각각의 대응방안을 설명하시오. 그리고 사이버공격에 대한 보안강화 및 능동적 대응을 위한 보안 네트워크를 구성하시오.

시스템응용

나. 랜섬웨어 대응 방법		
구분	해석 내용	내 용
방지적 대응	해킹수행 중인 부서는 즉각 차단 勒索 하여 사용	
방지적 대응	악성사이트 이용을 막아야 하는 경우 인터넷 사용 주의	
방지적 대응	DDoS - 트리플리, OS 등 폐지	제한된 대상에 대해서만 가능
방지적 대응	인터넷 이용에 기반 인터넷으로	인터넷 사용 가능
방지적 대응	- 사용자 관점에서 악성화 사용이 중단	

가) 사이버 공격 보안 강화 및 능동 대응 보안 네트워크
는 QoS 네트워크 구조 구현도



번호	나. 랜섬 대응을 위한 주제 구현도	구 분	내 용
		제한적 대응	- 가상영역에서 악성코드 실행 방지
		제한적 대응	- 전파로 내화까지 확장하는 시스템
		제한적 대응	- 지능형 전파구조(CDC, Adaptive)
		제한적 대응	- 악성 행위를 모니터링하여 발생 가능한 모든 행위 예상
		제한적 대응	- 유사 네트워크 DB, 지도이용
		제한적 대응	- AI와 함께하는 AI 네트워크 모니터링
		제한적 대응	- 미래 QoS 설정 예측
		제한적 대응	- 각국 최대 경비 감소
		제한적 대응	- 운영과 동시에 제작되는 저작권을 보호하는 방식
		제한적 대응	- 보안 강화 확장
		제한적 대응	- 미래 시장에서 구축
	- QoS 설정을 위한 24X7 의사 결정기구화 및 예상 개선 2회, “설”		

3	랜섬웨어(Ransomware)
문제	<p>최근 랜섬웨어에 의한 기업 피해가 증가하고 있다. 이와 관련하여 다음 질문에 답하시오.</p> <p>가. 랜섬웨어의 침투 경로 및 공격 기법 나. 기업보안 관점에서의 랜섬웨어 대응 방안</p>
도메인	정보보안
출제배경/의도	최근 증가하고 있는 랜섬웨어 피해와 관련해서 기업 보안 담당자 측면에서의 랜섬웨어 대응 방안 제시 능력 및 기술사적 관점 보유 검증
키워드	<ul style="list-style-type: none"> ● 금전요구, Drive by download, 사회공학적 기법 ● 임직원 보안 교육, 주기적 백업
목차예시	<ol style="list-style-type: none"> 1. 금전 갈취를 목적으로 하는 악성 프로그램, 랜섬웨어의 개요 2. 랜섬웨어의 침투 경로 및 공격 기법 3. 기업보안 관점에서의 랜섬웨어 대응 방안 4. 기업보안 방안 수립시 고려사항
채점 점수 가이드	<p>① 랜섬웨어 및 대응 방안에 대한 개념, 이해 부족 (5~9점) ② 랜섬웨어 및 대응 방안에 대한 기본 이해 수준 (10~13점) ③ 랜섬웨어 및 대응 방안에 대한 정확한 기술 제시 (14~15점) ④ 기업보안 관점에서의 추가요소 설명(+α)</p>
난이도	★ ★ ☆ ☆ ☆ (별 5개 기준)
학습 가이드	랜섬웨어에 대한 침입 경로, 공격 기법에 대한 정확한 지식은 물론 기업 보안 측면에서의 대응 방안을 제시할 수 있는 폭넓고 높은 관점이 필요합니다.
참고문현	국내 타깃 랜섬웨어의 현황 및 대응방안(한국인터넷진흥원) 안랩 보안이슈(www.ahnlab.com)
출제자	박병선 기술사(제 110 회 정보관리기술사 / deepb1ue@nate.com)

1. 금전 갈취를 목적으로 하는 악성프로그램, 랜섬웨어의 개요

가. 랜섬웨어의 정의

- Ransom(몸값) + Ware(제품)의 합성어
- 사용자 컴퓨터의 화면을 잠그거나 문서 등을 암호화 후 사용자에게 해독용 프로그램 전송을 미끼로 금전을 요구하는 악성프로그램

나. 랜섬웨어의 기업피해 현황

- 2015년 기준 국내 랜섬웨어 감염 피해는 5만 3천건, 총 피해금액 1천 90억 원 규모 (한국랜섬웨어침해대응센터 조사)
- 기업 5곳 중 1곳은 랜섬웨어 공격으로 보안사고를 겪었으며 이 중 중소기업의 경우 5곳 중 1곳은 대가를 지불했지만 데이터를 복구하지 못함 (카스퍼스키랩코리아 조사)
- 대가 지불을 포기할 수 있는 개인의 경우와 달리 기업의 데이터는 백업 여부에 따라 반드시 대가를 지불하지 않으면 안되는 경우가 있어 그 피해 수준이 심각함

2. 랜섬웨어의 침투 경로 및 공격 기법

가. 랜섬웨어의 침투 경로

침투 경로	설명	연관 기법
신뢰할 수 없는 사이트	- 단순 홈페이지 방문만으로도 감염 가능	- Drive by download
스팸메일	- 이메일 내 URL 링크 또는 첨부파일을 통한 악성코드 유포	- 사회공학적 기법
파일공유 사이트	- P2P 사이트를 통해 동영상 등의 파일을 다운받고 이를 실행할 경우 악성코드에 감염	- 익명 네트워크

- 랜섬웨어는 개인에 비해 기업을 대상으로 피해를 입혔을 때 훨씬 많은 금액을 요구하므로 기업에서는 랜섬웨어 침투 경로에 대한 철저한 대비 필요

나. 랜섬웨어의 공격 기법



▶ 익명네트워크 및 가상화폐를 이용한 주적 회피

공격 기법	사용 기술	설명
침입/배포 기법	- Drive by download	- 해커가 유도한 사이트에 접속하면 악성코드를 즉시 다운로드 시켜 사용자의 PC를 감염시킴
	- 멀버타이징 (Malvertising)	- 인터넷 사이트의 광고를 가장하여 클릭을 유도 - Drive by download 기법과 혼용하여 사용
	- 사회공학적 기법	- 업무 관련 메일인 것처럼 가장하여 피해자가 스팸 메일을 열어보도록 유도하는 기법
데이터 암호화 기법	- 단방향 암호화	- 피해자의 데이터를 복구할 수 없도록 단방향 암호화 하여 피해자는 대가를 지불하더라도 구제받을 수 없음
	- 양방향 암호화	- AES/RSA 등을 이용하여 데이터를 암호화하고 대가 지불시 복호화 할 수 있는 키 또는 별도 프로그램을 전송
금전 탈취 기법	- 비트코인	- 가상화폐를 통한 대가 지불을 요구하여 금융 추적을 회피
	- 토르 네트워크	- 복구 프로그램 배포시 익명 네트워크를 사용하여 배포자의 위치를 알 수 없도록 은닉

- 랜섬웨어에 의해 금전적 지불을 할 경우 또 다른 랜섬웨어를 만드는 자금으로 사용될 것을 우려하는 시선이 있으나 기업 입장에서는 중요 데이터에 대한 피해를 입었을 경우 대가 지불을 회피하기 어려움

3. 기업보안 관점에서의 랜섬웨어 대응 방안

가. 기업보안 관점에서의 랜섬웨어 대응 전략



- 사전 예방, 실시간 대응, 사후 복구 등의 랜섬웨어에 대한 전방위적 기업 보안 대응방안 마련 필요

나. 기업보안 관점에서의 랜섬웨어 대응 방안

구분	대응 방안	설명
사전 예방	- 최신 보안 업데이트 적용	- OS, 브라우저, 오피스 프로그램 등을 최신 보안 업데이트로 유지 - Agent를 이용하여 임직원의 업데이트 상태를 관리
	- 중요파일 주기적 백업	- 파일의 중요도를 고려하여 주요 파일은 주기적으로 백업
	- 임직원 보안 교육	- 랜섬웨어에 대한 경각심 고취 위한 주기적 임직원 보안 교육 실시 - 모의 해킹 메일을 발송하여 반응하는 임직원 대상으로 추가 교육 실시
실시간 대응	- 스팸 메일 실시간 감시 및 차단	- 메일 솔루션을 활용하여 스팸메일을 실시간으로 차단
	- 샌드박스 통한 첨부파일 검증	- 악성코드 전용 샌드박스를 이용하여 신속하게 악성 코드 여부를 판단
	- 의심 파일 실행 보류	- 샌드박스 검증이 완료될 때까지 의심파일은 실행을 보류시키는 기능을 추가
사후 복구	- 전용 Anti-Virus 백신 치료	- 전용 Anti-Virus 백신을 이용하여 랜섬웨어를 제거 - 랜섬웨어는 제거되지만 데이터 복구는 불가능
	- 백업된 파일 복구	- 백업된 데이터를 이용하여 감염된 파일을 복구

- 랜섬웨어에 효과적으로 대응하기 위해서는 랜섬웨어에 감염되더라도 언제든지 최신의 데이터로 복구가 가능하도록 철저한 데이터 백업이 중요

4. 기업보안 방안 수립시 고려사항

고려사항	설명
최신 보안기술 유지	- 공격 기법은 날로 진화하므로 기업 보안 시스템을 최신의 상태로 지속적으로 유지해야 함
보안 정책적용의 일관성	- 정책 적용에 예외사항이 적용될 경우 악용의 소지 발생 - 인적 사고를 방지하기 위하여 일관된 보안 정책 적용 및 철저한 감사 체계 구축
적절한 비용 투자	- 중요 정보와 그렇지 않은 정보를 구분하고 투자를 집중하여 비용 효율적인 정보보안 체계를 구축

- 기술적 대응방안 수립도 중요하지만 대부분의 기업보안 사고는 인재에 기인하므로 조직 관점에서 임직원 보안 의식 향상 및 유지가 핵심

"끝"

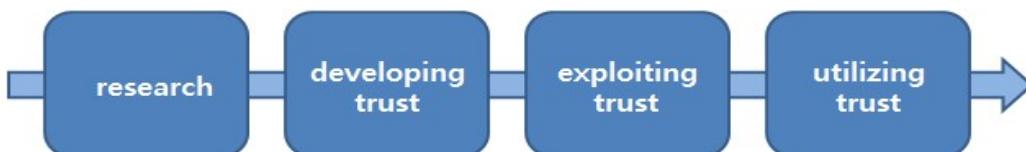
12	보안학적 측면에서의 사회공학(Social Engineering)
문제	보안학적 측면에서의 사회공학(Social Engineering)
도메인	보안
정의	기술적인 방법이 아닌 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여 정상 보안 절차를 깨트리기 위한 비기술적 침입 수단
키워드	인간관계, 신뢰, ROI, 사회공학사이클, 사회적관계, 공격적위협, 보안의식 포렌식, 유대관계기반, 컴퓨터기술 기반
출제의도분석	다양한 악성코드들이 보안이 철저한 시스템을 공략하는 것보다 대인관계를 이용한 사회공학적 방법을 이용하는 경향이 증가하고 있음에 따른 출제
답안작성 전략	기본적인 사회공학의 공격 절차 및 이에 대한 상세 기법을 서술하고, 다양한 관점에서 대응방안을 작성
참고문헌	사회공학적 해킹의 변화양상(KISA) http://blog.lgcns.com/1330 https://blog.naver.com/isacastudent/150187546768 KPC 110 회 대비 합숙해설집 1 일차
풀이 기술사님	김유성 기술사 (제 113 회 정보관리기술사 / yousungkim1216@gmail.com)

1. 보안학적 측면에서의 사회공학(Social Engineering)의 개념

- 기술적인 방법이 아닌 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여 정상 보안 절차를 깨트리기 위한 비기술적 침입 수단
- [특징] 1) 접근권한 담당자와 신뢰형성 2) 타겟의 약점과 도움을 이용

2. 보안학적 측면에서의 사회공학(Social Engineering)의 공격절차 및 공격유형

가. 사회공학의 공격절차



공격절차	세부특징	설명
Research	<ul style="list-style-type: none"> - 관계 형성 - 타겟 정보수집 	<ul style="list-style-type: none"> - 다양한 모임을 통해 공격 대상에 대한 정보수집 - 수집한 정보들은 관계형성을 위해 사용
Developing Trust	<ul style="list-style-type: none"> - 접근, 유대형성 - 주요인물 식별 	<ul style="list-style-type: none"> - 도움이 필요하거나 중요한 인물에게 접근 - 유대관계 기반 공격과 컴퓨터 기반 공격 가능
Exploiting Trust	<ul style="list-style-type: none"> - 감정에 호소 - 결정 요구 	<ul style="list-style-type: none"> - 사소한 요청에서 큰 요청으로 발전 - 충분한 신뢰 형성 이후에 수행
Utilizing Trust	<ul style="list-style-type: none"> - 책임회피 - 목적 수행 	<ul style="list-style-type: none"> - 공격자는 타겟의 도움으로 시스템에 침투 성공 - 타겟은 직접적 실행을 통해 피해 발생시킴

- 지속적인 탐색 및 신뢰 형성을 통해 시스템의 보안을 내부자의 도움으로 회피함

나. 사회공학의 공격유형

공격유형	상세기법	설명
유대관계 기반 사회공학	- 직접적인 접근 - 도청 - 훔쳐보기 - 휴지통 뒤지기 - 설문조사 - Piggybacking	- 권력이 있는 사람에게 접근하여 친분을 쌓고, 동정심에 호소하거나 가장된 인간관계 이용 - 도청장치 설치 및 휴대폰 감청 - 공격대상의 어깨너머에서 정보 획득 - 파쇄하지 않은 문건에서 정보 획득 - 신원확인된 앞사람과 함께 들어가는 유형
컴퓨터 기반 사회공학	- 포렌식 - 악성코드 전송 - 크롤링 - 피싱 - 파밍 - 토렌트 seed	- 디지털 핑거프린팅 활용 - 고객사 및 파트너사 위장하여 악성코드 배포 - 웹상에 존재하는 정보에 대해 관계기반 수집 - e-mail or SMS 를 활용하여 개인정보를 불법적으로 도용 가능 - P2P 공유사이트 내부 seed 활용하여 악성코드 배포

- 시스템이 아닌 사람을 대상으로 하기 때문에 100% 방어는 불가능. 인력/조직, 프로세스/기술 측면에서 대응체계 구축 필요

3. 보안학적 측면에서의 사회공학(Social Engineering)의 대응방안

구분	대응방안	설명
인력 및 조직 측면	- 지속적 교육 - 보안 거버넌스 - 내부통제 - 상호 인증	- 핵심 인력들에 대한 주기적인 교육과 함께 보안 거버넌스 수립 요구 - 접근 권한 및 2factor 인증 수행 - 공격에 대한 레퍼런스 주기적인 공지
기술 및 프로세스 측면	- DRM/DLP, UTM - ACL, 접근제어 - 모니터링 - 비식별화	- 방화벽 및 중요정보의 암호화, 내부자원에 대한 통제 리스트 작성 및 수행. MAC/DAC/RBAC 정의 - Audit 기능 활성화, K/L/T 비식별화로 주요정보 보호 - 패스워드의 주기적 변경 및 validation 수행

- 사회공학 기법의 지능화에 따라 개인이 아닌 다양한 관점에서 대응

"끝"