|  |
| --- |
| **[514126] 컴퓨터네트워크** |
| **실습 #04 문제 및 보고서** |

|  |  |
| --- | --- |
| **이름** | 정수현 |
| **학번** | 20185290 |
| **소속**  **학과/대학** | 전자공학과 |
| **분반** | 02 (담당교수: 박찬영) |

<주의사항>

* 개별 과제 입니다. (팀으로 진행하는 과제가 아니며, 모든 학생이 보고서를 제출해야 함)
* 각각의 문제 바로 아래에 답을 작성 후 제출해 주세요.
* 소스코드/스크립트 등을 작성한 경우, 해당 파일의 이름도 적어주세요.
* SmartLEAD 제출 데드라인:
* 다음 실습시간 전날 23:55까지
* 데드라인을 지나서 제출하면 0점
* 주말/휴일/학교행사 등으로 인한 데드라인 연장 없음
* 부정행위 적발 시, 원본(보여준 사람)과 복사본(베낀 사람) 모두 0점 처리함
* SmartLEAD 에 아래의 파일을 제출해 주세요
* 보고서(PDF 파일로 변환 후 제출을 권장하나, WORD로 제출해도 됨)
* 보고서 파일명에 이름과 학번을 입력해 주세요.
* 소스코드, 스크립트, Makefile 등을 작성해야 하는 경우, 모든 파일 제출(또는 본 문서에 소스코드 화면 캡처해서 붙여넣기)

<개요>

이번 과제는 네트워크 모니터링 실습입니다. 네트워크에서 획득할 수 있는 다양한 정보를 이용해서 네트워크 모니터링, 특정 호스트 모니터링, 패킷 모니터링 등을 수행하는 실습으로 구성되어 있습니다.

<실습 과제>

|  |
| --- |
| **[Q 0] 요약 [배점: 10]**  이번 과제에서 배운 내용 또는 과제 완성을 위해서 무엇을 했는지 2~3문장으로 요약하세요. |

답변:

nmap명령어를 통해 원격 호스트의 정보를 알아낼 수 있고 hydra, tcpdump, wireshark, telnet을 통해 원격 접속을 해서 파일을 들여다보는 방법을 배웠습니다.

|  |
| --- |
| **[Q 1] nmap [배점: 10]**  ‘nmap’은 원격 호스트의 포트 정보, OS 정보 등을 스캔하여 알아내는 명령어입니다. 간단한 사용법은 다음과 같습니다. 210.115.230.145 번 IP를 가진 호스트가 실행중인 서비스 및 포트번호 정보를 가져오는 방법은: $nmap -v 210.115.230.145 (혹시 이게 안되면, $nmap –p ssh 210.115.230.145)  문제 1) 위 명령어를 실행하고, 결과 화면을 캡처하여 아래에 첨부하세요  문제 2) SSH 서비스가 몇 번 포트를 통해 서비스되고 있는지 답하세요 |

답변 1)



답변 2)

22번

|  |
| --- |
| **[Q 2] hydra [배점: 20]**  Kali 리눅스에는 hydra 라는 프로그램이 기본으로 설치되어 있습니다. ‘hydra’ 명령을 사용하면 무차별 로그인 시도를 해 볼 수 있습니다. 아래와 같은 상황을 가정합니다.   * 210.115.230.145 서버에는 test 라는 계정이 있음 * ‘test’ 계정의 비밀번호는 숫자 4개로 이루어져 있는데, 처음 두개 숫자는 84임 * ‘test’ 계정으로 로그인 하면 ‘secret-message.txt’ 라는 텍스트 파일이 있는데, 파일에 기록된 내용이 매우 중요한 내용임   ‘pwd-atk-test’ 라는 디렉토리를 만들고, 디렉토리 안으로 이동하세요.  ‘logins.txt’ 라는 파일을 만들고, 그 안에 test 라고 입력하세요  ‘targets.txt’ 라는 파일을 만들고, 그 안에 210.115.230.145 이라고 입력하세요.  ‘pws.txt’ 라는 파일을 만들고, 파일 안에 84로 시작하는 4자리 숫자에 해당하는 모든 조합을 입력하세요. 하나의 행에는 하나의 숫자만 입력하세요 (8400 부터 8499까지 총 100개의 숫자가 100개의 행으로 입력된 텍스트 파일을 생성)  터미널에서 다음과 같이 입력하세요: $sudo hydra -L logins.txt -P pws.txt -M targets.txt ssh (포트번호를 20022로 바꾸려면 –s 20022 이라고 마지막에 입력)  ‘test’ 계정의 비밀번호를 알아낸 후, 해당 호스트에 ssh로 연결하세요 (22번 또는 20022 포트로 접속하세요)  문제) secret-message.txt 에 적힌 내용은 무엇인가요? |

답변)

I like Coca Cola

|  |
| --- |
| **[Q 3] tcpdump [배점: 20]**  ‘tcpdump’는 터미널에서 사용 가능한 패킷 모니터링(패킷 캡처) 도구입니다. 네트워크에서 돌아다니는 패킷을 모니터링 할 수 있으며, 네트워크 프로토콜 개발 시 디버깅 목적으로 사용하거나, 네트워크 상태를 진단하는데 사용합니다. Kali 리눅스에는 기본적으로 설치되어 있습니다.  Kali 가상 머신을 종료하고, 네트워크를 ‘어댑터에 브릿지’로 설정한 후 가상 머신을 시작하세요. 터미널에서 $sudo tcpdump 라고 입력하세요. 조금만 기다리면, 네트워크에서 오고 가는 모든 패킷을 볼 수 있습니다. 패킷의 내용을 ASCII 형식으로 보려면 $sudo tcpdump -A 라고 입력하세요.  터미널 2개를 실행하세요. 터미널 1에서 $sudo tcpdump src 210.115.230.145 -A 라고 입력하고 실행하세요. 이제 터미널 2에서 $curl 210.115.230.145 이라고 입력하세요. 터미널 1에는 210.115.230.145 웹 서버에서 보낸 결과를 캡처한 내용이 출력됩니다.  문제 1) 위의 과정을 모두 수행하고, 터미널 1의 화면을 캡처하여 아래에 첨부하세요  문제 2) 웹 서버가 보낸 응답에는 어떤 메시지가 포함되어 있나요? (힌트: Hello 로 시작하는 문장입니다)  문제 3) $curl 210.115.230.145 명령은 어떤 동작을 하는지 설명하세요. |

답변 1)



답변 2)

Hello world, Chanyoung Pack

답변 3)

해당 ip주소의 서버와 통신

|  |
| --- |
| **[Q 4] wireshark [배점: 20]**  ‘tcpdump’와 유사한 기능을 하지만 GUI 인터페이스를 가지고 있는 프로그램이 Wireshark 입니다. Kali 리눅스에는 기본적으로 설치되어 있습니다. 터미널에서 다음과 같이 입력하세요  $sudo wireshark &  **문제 1)** 명령어 끝에 & 라는 기호를 붙였습니다. 무엇을 의미하는 것인가요?  메인으로 사용하는 인터페이스 카드를 이용해서 패킷 캡처를 시작하세요. **필터**를 다음과 같이 입력하세요: ip.addr == 210.115.225.177 (이 IP 주소는 [www.hallym.ac.kr](http://www.hallym.ac.kr/) 웹 서버의 주소 입니다.) \*\* 아래의 그림에서 초록색으로 표시된 텍스트 입력란을 ‘필터 입력란’이라고 하겠습니다.    <필터 입력란에 필터값 입력하기>  웹 브라우저를 시작하고, [www.hallym.ac.kr](http://www.hallym.ac.kr/) 주소로 이동하세요. Wireshark로 돌아가 보면, [www.hallym.ac.kr](http://www.hallym.ac.kr/) 웹 서버와 주고받은 모든 패킷이 캡쳐되어 있습니다.    초반에는 [SYN], [SYN,ACK], [ACK] 패킷을 교환하고, 다음으로 [GET ...] 요청 패킷이 전달되는 것을 알 수 있습니다.  Wireshark를 제대로 사용하기 위해서는 필터를 어떻게 설정하는지를 잘 알고 있어야 합니다!!  **문제 2)** tcp 프로토콜에 해당하는 패킷만 필터링 하려면, 필터 입력란에 무엇을 입력해야 하나요?  **문제 3)** 송신측 IP 가 10.20.30.40 인 패킷만 필터링 하려면, 필터 입력란에 무엇을 입력해야 하나요?  **문제 4)** (송수신측 구분 없이) IP 주소가 10.10.10.10 이고, TCP 포트 80을 통해서 전송되는 패킷만 필터링 하려면, 필터 입력란에 무엇을 입력해야 하나요? |

답변 1)

wireshark를 백그라운드 작업으로 사용한다.

답변 2)

tcp

답변 3)

ip.src eq 10.20.30.40

답변 4)

(ip.addr==10.10.10.10)and(tcp.port eq 80)

|  |
| --- |
| **[Q 5] telnet을 사용하지 않는 101가지 이유 [배점: 20]**  옛날 옛적에는 원격 접속을 위해서 telnet 을 사용했습니다. 하지만, telnet은 서버-클라이언트 간에 전송되는 메시지를 암호화 하지 않고 전송했고, 이로 인해 보안상 취약했습니다. 현재는 telnet 대신 ssh 를 사용하고, ssh는 서버-클라이언트간 메시지를 암호화 하기 때문에 wireshark 등으로 패킷을 캡쳐해서 (훔쳐) 보아도 어떤 내용이 오가는지 알 수 없습니다. 이번 문제는, Kali 리눅스에 telnet 서버를 설치하고, 호스트 컴퓨터에서 Kali 리눅스에 telnet 으로 로그인 할 때, wireshark로 패킷을 캡쳐하고, 이를 통해 로그인 계정 (아이디, 비번)을 알아내는 과제 입니다.  Kali 리눅스 가상 머신을 ‘어댑터에 브릿지’로 설정하여 호스트 머신이 Kali로 telnet 접속을 할 수 있도록 하세요. 윈도우10의 경우 기본적으로는 telnet 명령이 터미널에서 인식되지 않는데, 인터넷 검색을 통해서 telnet 명령을 활성화 하는 법을 검색하세요.  아래와 같은 순서로 진행하세요.  [1] Kali 가상 머신에 telnet 서버 설치 (인터넷 검색 고고)  - $sudo apt update $sudo apt install xinetd $sudo apt install telnetd /etc/xinet.d 폴더 아래에서 xinetd.conf 파일 또는 telnet 파일을 아래와 같이 수정하세요 서비스 재시작 $sudo systemctl restart xinetd 텔넷 서비스가 시작되었습니다 (상태확인: $systemctl status xinetd 로 확인해서 active/running 인지 체크)    [2] Kali 에서 신규 사용자 생성 (아이디: test, 비번: 1234로 설정)  - $sudo useradd test $sudo passwd test 해서 1234로 패스워드 설정  [3] Kali 에서 telnet 서버 실행 ([1]번에서 이미했음)  [4] Kali 에서 wireshark 패킷 캡쳐 시작 (23번 포트로 오가는 데이터만 캡처)  - 필터 입력란에서 tcp.port == 23 이라고 입력  [5] 호스트 머신에서 터미널을 열고, Kali 서버로 telnet 접속후, test 계정으로 접속\  - 텔넷 클라이언트가 설치되어 있지 않으면, 인터넷 검색해서 설치  [6] 호스트 머신에서 telnet 접속(로그인)이 완료되면 Kali 에서 wireshark 종료  [7] wireshark에서 캡쳐한 패킷을 보고, 로그인 계정(ID 및 비번) 알아내기  문제 1) 어떻게 wireshark에서 로그인 계정 및 비번을 알아낼 수 있었는지 설명하세요.  문제 2) test 사용자의 ID(=test)와 비밀번호(=1234)가 보이는 wireshark 화면을 모두 캡처하여 아래에 첨부하세요. 즉, wireshark 를 통해서 ID와 PWD를 확인할 수 있었다는 것을 증명해보이세요. |

답변 1)

telnet접속을 통한 원격접속을 해서 패킷을 암호화하지 않고 송수신했기 때문이다

답변 2)

















**끝! 수고하셨습니다**