



Examination Answer Books

12 Pages

Instructions to Candidates

1. Please give the information requested in the boxes below.
2. Enter your name in the space provided to the right, fold over and seal down (using the label provided) to hide your name.
3. The answers must be legibly written. The Examiners can either ignore illegible script or have it typed and the expense of typing charged to the candidate.
4. Write your answers in ink.
5. Begin each answer on a fresh page. Do all rough work in the answer book and cross it through.
6. No part of this book is to be torn out; it must be handed in complete.
7. If more books than one are used, fasten them together using the tags available from the invigilator(s).
8. Every book must be handed in. In no circumstances may answer books, used or unused, be taken out of the examination venue.

1	Student Number	1708232
2	Title of Examination Paper	NETWORK SECURITY
3	Module Code	M7X01701
4	Date and Time of Examination	12/1/18 12:00AM
5	Examination Venue	TOWN HILL
6	Seat Number	G030
7	Number of Answer Books handed in	2

Complete, fold and seal
(see note 2 below)

SURNAME:

PACE

FORENAME(S):

CHRISTOPHER

List the numbers of the questions you have attempted	Office Use
1a	2
1b	18
2a i	2
2a ii	2
2a iii	19.5
2a iv	2
2a v	2
3 i	2
3 ii	22
Total	59.5

79%

① TCP PORT 25 / ~~TCP~~ PORT 110

~~This~~ This port is used by an email application for sending of emails.

The security implications of this port being used is that the network becomes susceptible to attack rendered via email (i.e. hidden within an attachment ~~or~~ or via a malicious URL)

TCP 42 / ~~TCP~~ ~~42~~ / TCP 53

These two ports are used for DNS. These leave the system susceptible to hijacking DNS.

TCP/80 + TCP/1027 + TCP/1025 + TCP/593

This is used for WWW access, there is a webserver running. This leaves open the chance for attack ~~of~~ of the web application held on this server.

TCP/88

This port is used for security, much like TACACS/RADIUS. The system could be attacked via brute force on this port.

TCP/135 + TCP/445 + TCP/139

These ports are used in Windows file access, these can be used to traverse viruses through a network (i.e. WANNACRY)

1a) TCP/389 + TCP/636 + TCP/3268 + TCP/3269

THESE ARE USED FOR COMMUNICATION ~~BETWEEN~~
~~A USER~~ TO AND FROM AN ACTIVE
DIRECTORY INSTANCE. INTERCEPTION OF
THIS TRAFFIC MAY ENABLE A HACKER TO
REPLAY THIS TRAFFIC TO IMITATE A GENUINE
USER.

TCP/464

THIS IS USED FOR PASSWORDS.

1b) PORT SCANNING TOOLS

1) NMAP

THIS TOOL CAN BE USED TO PERFORM NUMEROUS TYPES OF SCANNING PORT TECHNIQUES. SUCH AS (ACK, SYN, XMAS, NULL)

2) ZENMAP

THIS IS JUST A FRONTEND FOR NMAP, MAKING USE OF NMAP, ALLOWING FOR MUCH EASIER SCANNING OF A TARGET.

3) ANGRY IP

MUCH LIKE NMAP THIS IS ABLE TO PERFORM ALL TYPES OF PORT SCANS. CAN PRIMARILY BE USED TO PERFORM PING SWEEPS OF A NETWORK.

4) PORTQUERY

THIS TOOL CAN BE USED TO QUERY IF A PORT IS OPEN, RESULTS FROM THIS TOOL INDICATE WHETHER A PORT IS FLUERING OR LISTENING.

1b) TYPES OF PORT SCAN.

- 1) ACK ✓
- 2) SYN ✓
- 3) XMAS ✓
- 4) NULL ✓
- 5) CONNECT:

ACK SCAN.

THIS SCAN WILL SEND AN ACK MESSAGE TO THE TARGET. IF THE PORT IS OPEN THEN NO RESPONSE WILL BE RECEIVED, THIS IS DUE TO THE TARGET OR FIREWALL IN FRONT OF THE TARGET HAS RECOGNISED THAT THERE IS NO EXISTING CONNECTION FOR THIS FLOW. (I.E. OUT OF STATE.)

IF THE PORT IS CLOSED THE TARGET WILL RESPOND WITH A RST PACKET TO END THE CONNECTION. NO TRACE OF SCAN IS LEFT.

SYN SCAN.

THIS SCAN WILL SEND A SYN MESSAGE TO THE TARGET. IF THE PORT IS OPEN A SYN-ACK WILL BE SENT BACK. IF THE PORT IS CLOSED THE TARGET WILL RESPOND WITH A RST PACKET TERMINATING THE CONNECTION. NO TRACE OF SCAN IS LEFT.

XMAS SCAN

THIS SCAN IS WHEN ALL THE URG, PSH, NULL FLAGS ARE SET. THIS LIGHTS UP THE PACKET LIKE A XMAS TREE, HENCE THE NAME.

- 16) THIS COMBINATION OF FLAGS IS ILLEGAL, AND WILL BE DROPPED BY THE TARGET, ~~AND~~ THEREFORE NO RESPONSE INDICATES THE PORT IS OPEN. A RST PACKET WILL BE SENT BY THE TARGET IF THE PORT IS CLOSED. TRACE OF SCAN IS LEFT.

NULL SCAN.

MUCH LIKE THE XMAS SCAN, AN ILLEGAL FLAG COMBINATION IS SENT TO THE TARGET (I.E NULL FLAG SET).

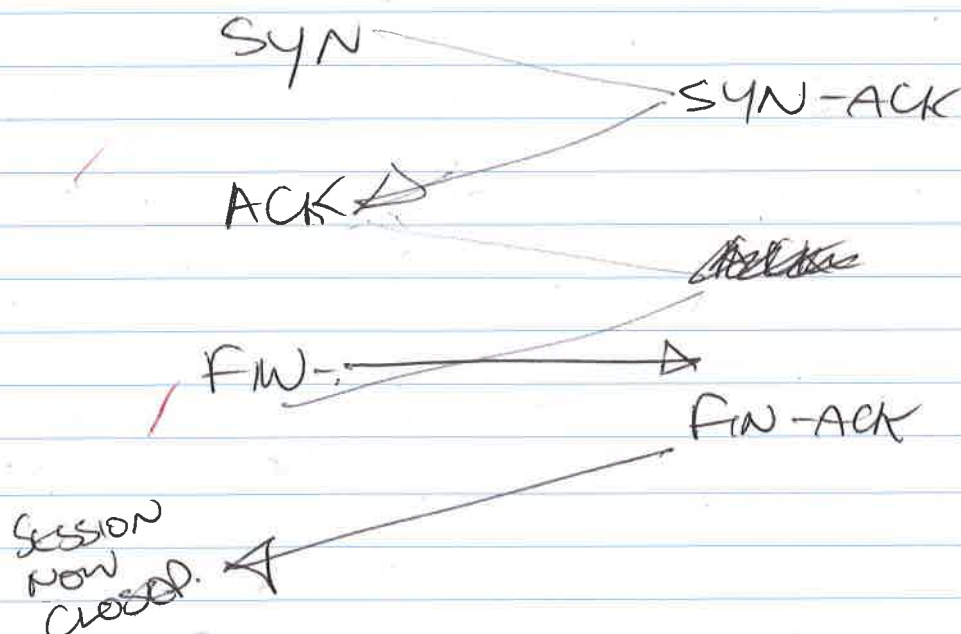
IF THE PORT IS OPEN, NO RESPONSE WILL BE RECEIVED AS THE PACKET WILL BE DROPPED, IF CLOSED A RST PACKET WILL BE RECEIVED. TRACE OF SCAN IS LEFT.

CONNECT SCAN

THIS TYPE OF SCAN TRIES TO ESTABLISH A 3 WAY HANDSHAKE WITH THE TARGET.

SCANNER

TARGET.



15) THIS TYPE OF SCAN LEAVES A TRACE OF THE SCAN.

18

- Q2) i) 1) SQL INJECTION ✓
2) XSS INJECTION ✓
3) SECURITY MISCONFIGURATION ✓
4) INFORMATION DISCLOSURE ✓
5) SOCIAL ENGINEERING. ✓

SQL INJECTION

MANY BACK-END DATABASE CONFIGURATION IS INADEQUATELY SECURE. SIMPLE SQL INJECTION COMMANDS CAN BE ENTERED TO MANIPULATE THE BACK END DATABASE INTO RUNNING MALICIOUS COMMANDS, COMPROMISING THE INTEGRITY OF THE WEB APPLICATION.

XSS SCRIPTING.

THIS TYPE OF VULNERABILITY CAN ALLOW AN ATTACKER TO INTERCEPT COMMUNICATION WITHIN THE WEB APPLICATIONS LOGIC. THIS CAN ALLOW THE ATTACKER TO MANIPULATE THE TCP STREAM TO GAIN ACCESS TO UNAUTHORISED DATA.

SECURITY MISCONFIGURATION

THIS VULNERABILITY CAN BE EXPLOITED TO ALLOW AN ATTACKER TO ACCESS NOT INTENDED. PASSWORD PROCESS CAN BE TESTED TO SEE IF ANY INFORMATION REGARDING USERS ARE PRESENT. ALSO PASSWORD RESET FUNCTIONS CAN BE EXPLOITED TO RESET A USER'S PASSWORD ILLEGALLY.

2i) Information Disclosure.

WEB APPLICATION CAN BE SEARCHED FOR INFORMATION ON THE BACK END CONFIGURATION OF THE WEB APPLICATION. THIS MAY THEN ALLOW THE ATTACKER TO PERFORM A MORE FOCUSED ATTACK ON THE WEB APPLICATION

~~Information~~

SOCIAL ENGINEERING.

INFORMATION GATHERED FROM ONLINE RESOURCES SUCH AS GOOGLE, OR OBTAINED DIRECTLY FROM THE WEBSITE CAN BE USED TO STRUCTURE AN ATTACK DIRECTLY AT THE WEBSITE OWNER. (I.E. PHONE CALL, EMAILS.) WHERE FURTHER INFORMATION CAN BE GAINED TO HELP PERFORM A MORE STRUCTURED ATTACK. ALSO MALICIOUS CODE CAN BE EMBEDDED INTO AN EMAIL TO GAIN ACCESS TO THE WEB OWNERS PC.

2ii) NMAP

THIS CAN BE USED TO PERFORM PORT SCANNING ON A TARGET TO GAIN AN INSIGHT INTO WHAT TYPE OF APPLICATIONS ARE RUNNING ON A TARGET.

IDSERVE

THIS CAN BE USED TO IDENTIFY/ENUMERATE THE INNER WORKINGS OF A WEB SERVER. (I.E. APACHE, IIS)

NETSPARKER

~~THIS CAN BE~~ THIS IS AN AUTOMATED TOOL TO SCAN FOR VULNERABILITIES ON A WEBSITE, ALTHOUGH CAN FLAG UP FALSE POSITIVES.

NETCAT

THIS IS A UTILITY THAT CAN BE USED TO SEND AND RECEIVE TCP/UDP PACKET, AS WELL ~~AS WELL~~

5

BURP SUITE

THIS IS A MULTI FUNCTIONAL PROGRAM, BUT CAN BE USED AS A PROXY BETWEEN ~~A~~ A WEB BROWSER AND THE TARGET WEB APPLICATION. TRAFFIC IS INTERCEPTED BY THE PROXY ALLOWING MANIPULATION OF THE TRAFFIC BEFORE SENDING TO THE TARGET.

2 iii) PLANNING + RECONISANCE ✓
SCANNING.

GAINING ACCESS ✓

MAINTAINING ACCESS

ANALYSING THE RESULTS

PLANNING + RECONISANCE

THIS STAGE IS USED TO PLAN THE TYPE OF ATTACKS INTENDED TO BE USED IN THE PEN TEST. IT WILL ALSO BE USED TO PERFORM RECONISANCE (I.E. GAINING INFO ON THE TARGET OWNERS/USERS)

2 iii) SCANNING

THIS STAGE WILL BE USED TO SCAN THE TARGET FOR POTENTIAL VULNERABILITIES AND TYPES OF SERVICES RUNNING ON THE TARGET. ENUMERATION OF THE TARGET WILL ALSO BE PERFORMED AT THIS STAGE.

GAINING ACCESS

THIS STAGE WILL BE USED TO GAIN ACCESS TO THE TARGET, UTILISING THE VULNERABILITIES AND SERVICES IDENTIFIED IN THE SCANNING STAGE.

MAINTAINING ACCESS

THIS STAGE WILL BE USED TO SET OUT ACTIONS TO ENABLE TO PERSISTENCE OF THE PEN TEST (I.E. ABILITY TO CONTINUE THE TEST).

ANALYSIS OF RESULTS.

THIS STAGE WILL BE USED TO COLLATE ALL THE INFORMATION IDENTIFIED IN ALL PREVIOUS STAGES, WITH THE INTENTION OF CREATING A REPORT TO GIVE TO THE WEB APPLICATION OWNER.

2iv) VULNERABILITY ASSESSMENT

A VULNERABILITY ASSESSMENT IS THE IDENTIFICATION OF KNOWN VULNERABILITIES WITHIN A NETWORK.

PENETRATION TESTING

THIS IS ~~THE~~ THE EXPLOITATION OF A VULNERABILITY (I.E. GAINING ACCESS DUE TO A VULNERABILITY).

2v) CONTINGENCY PLAN

- 1) DATES/TIMES AGREED WITH WEB APPLICATION OWNER WHEN TESTS CAN BE CARRIED OUT.
- 2) AGREEMENT THAT ANY INFORMATION OBTAINED DURING THE TEST WILL NOT BE DISCLOSED TO THIRD PARTIES AND WILL BE DESTROYED.
- 3) ONLY QUALIFIED SECURITY TESTERS WILL BE USED DURING THE TEST.
- 4) NO INFORMATION WILL BE DESTROYED ON A ~~WEB~~ APPLICATION DURING THE TEST.
- 5) IF A MAJOR VULNERABILITY IS DISCOVERED THIS WILL BE NOTIFIED TO THE OWNER INSTANTLY.
- 6) CONTACT INFORMATION OF TESTERS WILL BE MADE AVAILABLE TO OWNERS.
- 7) OWNERS WILL NOT PREVENT THE PEN TEST BEING PERFORMED (I.E. BLOCKING ACCESS).

1/2

5

2) 8) LIABILITY OF ANY FAILURES WILL BE HELD WITH THE OWNER.

~~6/7~~

Q3) i) EXTERNAL TESTING

THIS IS WHEN THE TEST IS PERFORMED FROM OUTSIDE OF A NETWORK, NOT KNOWING THE INNER LAYOUT OF A NETWORK.

INTERNAL TESTING

THIS IS WHEN THE TEST IS ACTUALLY PERFORMED WITHIN THE NETWORK, KNOWING THE TARGETS. THUS PERFORMING A MORE FOCUSED ATTACK ON THE SYSTEM ITSELF, NOT THE LAYERS OF SECURITY PROTECTING IT (I.E. FIREWALLS)

ii) BLACK BOX TESTING

THIS IS WHEN NO INFORMATION IS GIVEN TO THE ATTACKER. IT IS THE RESPONSIBILITY OF THE ATTACKER TO USE PEN TESTING TECHNIQUES TO GATHER THE INFORMATION NEEDED TO PERFORM THE ATTACK.

WHITE BOX TESTING

THIS IS WHEN THE ATTACKER IS GIVEN ALL THE RELEVANT INFORMATION ON A TARGET, ALLOWING THEM TO PERFORM A MORE STRUCTURED / FOCUSED ATTACK ON A SYSTEM.

Q3) (iii) ANNOUNCED TESTING.

THIS IS WHEN KNOWLEDGE OF THE TEST IS KNOWN. SECURITY PERSONNEL INVOLVED IN THE TARGET ORGANISATION ARE ABLE TO MONITOR THE TEST AND ADVISE THE PEN TESTERS OF ANY INFORMATION DISCOVERED BY THEM, THUS NOT SILENCING OF THE PEN TESTERS ACCESS.

ON ANNOUNCED TESTING.

THIS IS WHEN THE TESTING IS NOT KNOWN BY THE SECURITY PERSONNEL WITHIN THE TARGET ORGANISATION. HIGHER LEVELS OF MANAGEMENT WILL BE TOLD. THIS TYPE OF TEST ALLOWS FOR THE SCROUTINY OF THE SECURITY PERSONNEL TO THEIR REACTIONS TO THE BREACHES OF SECURITY.

Q4) (i) AUTOMATED TESTING.

THIS IS WHEN ~~AS~~ AUTOMATED TESTING TOOLS ARE USED TO ATTEMPT TO PENETRATE A NETWORK. THESE CAN BE USEFUL FOR TESTING LARGE AMOUNTS OF TARGETS, BUT CAN ALSO PRODUCE FALSE POSITIVES.

MANUAL TESTING.

THIS IS THE OPPOSITE OF AUTOMATED TESTING. THIS IS WHEN A PEN TESTER USES HIS/HER SECURITY KNOWLEDGE TO PERFORM TESTS. ADJUSTING THEIR ATTACKS ACCORDING TO THE OUTCOME OF PREVIOUS TESTS.

BOTH MANUAL AND AUTOMATED CAN BE USED IN CONJUNCTION. USING MANUAL TESTING TO CONFIRM RESULTS GATHERED FROM THE AUTOMATED TESTER.

Q3b) THE PENETRATION SLA IS AN AGREEMENT BETWEEN THE PENESTER AND TARGET ORGANISATION. IT IS A LEGAL DOCUMENT FILED BETWEEN THEM OUTLINE THE LEGAL STANCE ON THE IMPLICATIONS OF THE PENTEST.

WITHIN THIS DOCUMENT INFORMATION WILL BE CONFIRMED ON TIME SCALES, RESPONSIBILITIES AND OUTCOMES OF SITUATIONS.

THIS DOCUMENT WILL BE USED IF ANY ISSUES ARISE FROM THE PENTEST.