



SURNAME: MILNE

FORENAME(S): JOHN-PAUL

12 Pages

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 may require the script to be 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	1705837
2	Title of Examination Paper	Network Security
3	Module Code	M7X01701
4	Date and Time of Examination	12/1/18 12 PM
5	Examination Venue	Gym
6	Seat Number	9031
7	Number of Answer Books handed in	1

List the numbers of the questions you have attempted	Office Use
3	19
4	14.5
2	20
Total	53.5

(Gweler yr ochr arall am y fersiwn Cymraeg)

3 Penetration Testing is the simulated attack on a system from an attacker's perspective. Its purpose is to highlight vulnerabilities before they are exploited by an attacker.

External testing is performed from outside the company. Simulates external attacker.

Internal testing is performed from inside the company's network. It is used to check that network segmentation is correctly implemented and checks that users within the company can only access what they are supposed to access. Simulates rogue/disgruntled employee.

External testing focusses on security measures that protect the network from internet - firewall, IDS/IPS etc.

Black box testing is where the tester has no prior knowledge of the company network. Information gathering makes up a large initial aspect of black box testing.

White box testing is where the tester is given information about the network by the company prior to testing. This can allow for certain aspects of the company to be tested with a higher level of scrutiny + detail.

Announced testing is when the IT department have full prior knowledge of testing schedules. IT systems + network is being tested.

Unannounced testing is where only upper management have prior knowledge of testing schedules. This test not only tests systems + hardware, but also the response to attack by the IT department - procedural testing.

Automated testing uses software tools to perform large scale testing in a systematic + consistent manner. Reporting tools can produce detailed reports for review. Needs to be regularly updated.

3 Manual testing is a more labour intensive process. It is therefore usually more expensive, and takes a longer period of time. Zero day exploits can be tested. Most penetration testing would use a combination of automated testing tools and ~~on some~~ manual testing. False positives need reviewing and reporting needs a manual review process. Manual testing can be used for testing processes within the company, not just IT systems.

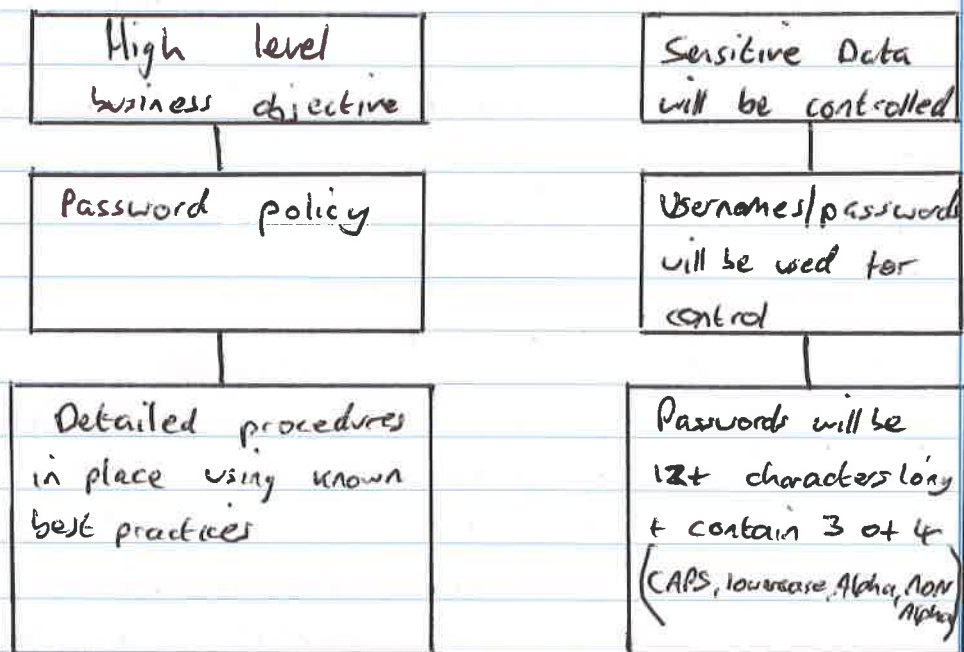
Service Level Agreement is a requirement for penetration testing. It needs to clearly define the following:

- Goal of penetration testing project
- Full scope of works
 - what systems are included in project?
 - what systems are NOT included in project?
 - what time schedule is available for testing?
- Who is responsible for fixing any problems that arise from testing process?
- what time requirements need to be considered for fixing a problem - have online in 30 mins / 2hrs etc?
- contact details for all parties in case of emergency.

SLA is a legal contract between all parties - company, pen tester, contractors. It needs to clearly state all aspects of project. Needs to be in place before testing commences



- 4 Policy mapping allows for high level company objectives to be defined and policies put in place to implement these objectives. These can be regulatory in nature - ie, if there is a legal compliance aspect.



Security Policy should contain the high level goals + objectives of the company with regards to Information Security. This can be broken down into more detailed + specific sub policies that target specific areas, ie. password complexity policy, VPN policy. Policies should make use of known best practices within the industry. Policies need to be regularly audited for compliance + renewed at regular intervals, updated + amended as required. Needs to include Management + technical expertise. Management need to ensure policies + procedures are adhered to.

Always assume that policies + procedures need regular review and updating, it is not a one-time only process. Never assume that because a policy is in place, the problem has gone away. Management need to ensure there is a culture that encourages + promotes following policy.

- 4 Always assume human error will occur. People will make mistakes and measures need to be in place to detect + act when necessary.

2

Ten step approach to writing a policy.

Pre 3

Write 2

Do 2

review 3

Pre	{	Perform background research ✓ Carry out risk assessments ✓ Create policy review panel ✓
Write	{	Write Information Security Plan ✓ Write Information Security Policies + Procedures ✓
Do	{	Implement Plan, policies + procedures ✓ Awareness + Training ✓
Review	{	Gather feedback from implementation Perform regular audits to ensure compliance Review + update policies + procedures ✓

8

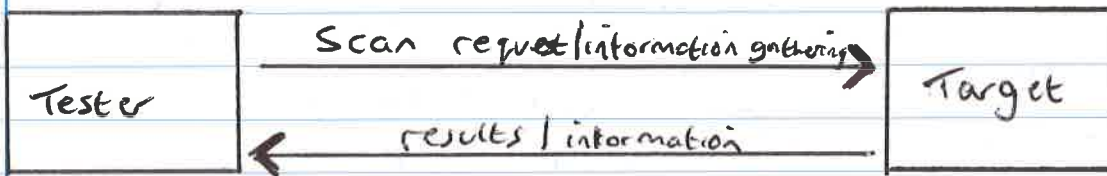
The above ten steps to writing a policy is a well known structured method to developing correct policies. Initial steps are based around gathering the relevant information. This can then be used to write plans + policies. When these are rolled out, awareness + training need to be prioritised to ensure staff know they need to follow these new policies. The last stages are important as they monitor compliance with these policies and allow for feedback to be gathered which can be used for amendments to improve policies. These steps can be repeated as required.



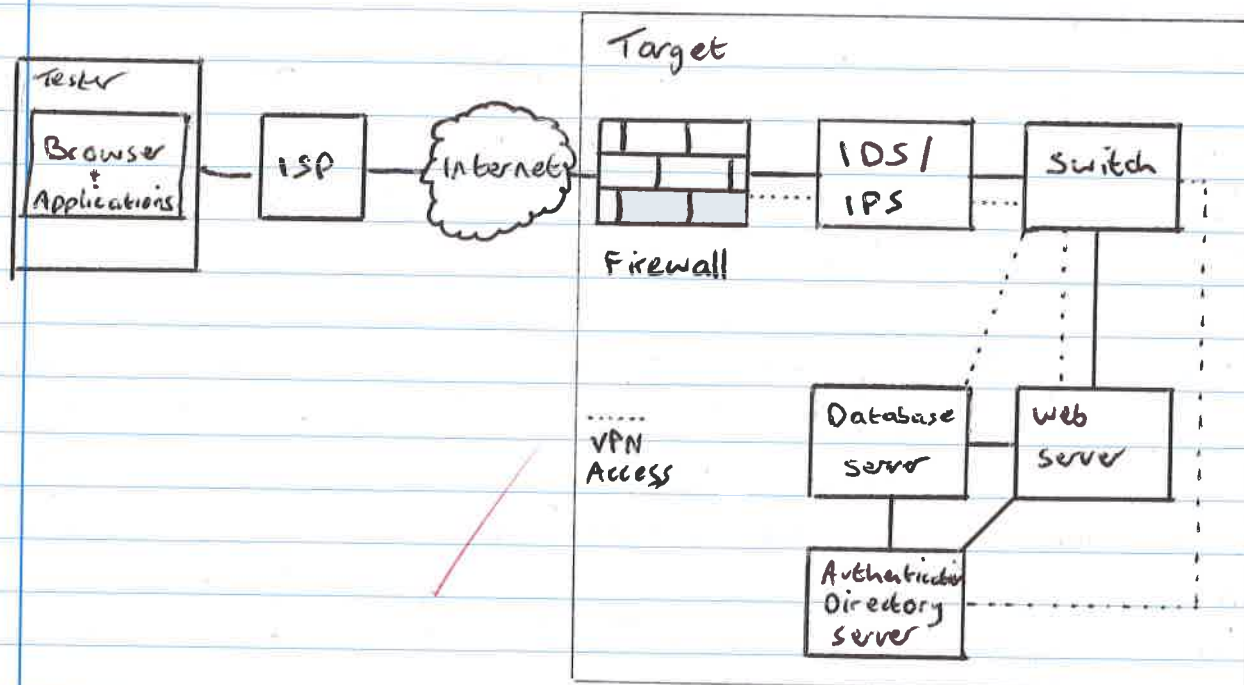
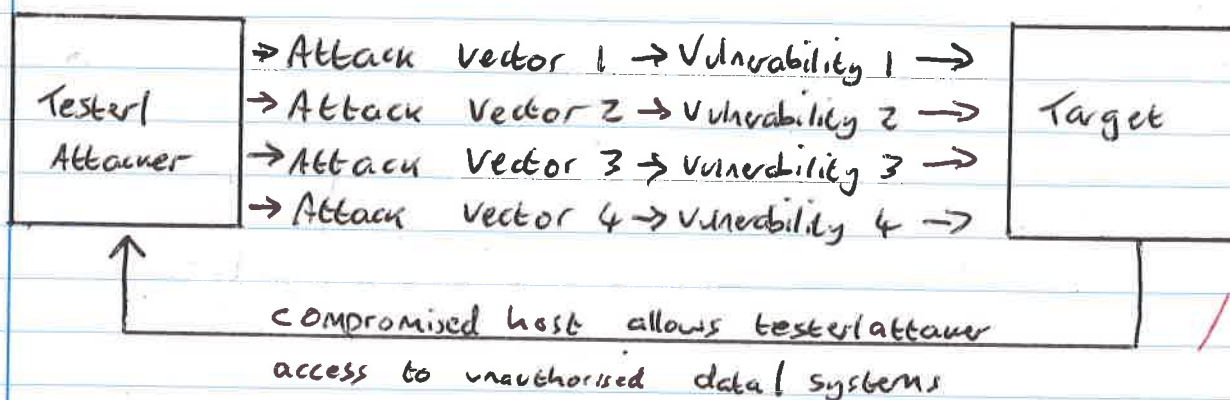
2. Penetration Test on CUPSTC.COM - External Test.

Test will be broken down into four high level steps.

- Gather information
- Scan for vulnerabilities
- Attempt to exploit vulnerabilities
- Report findings.



- NMap is a port scanning tool. It can probe the target and report on any ports that are open on the host. Misconfigured ports can be targeted by an attacker. It can also detect OS + Application version numbers.
- Nmap is a vulnerability scanner. It cross-references against lists of ~~well~~ known vulnerabilities in applications, OS, firmware etc.
- OWASP ZAP is another vulnerability scanner. It is important to use more than one. No automated scanner is 100% guaranteed. They can find known vulnerabilities - they cannot find unknown vulnerabilities hence need regular updating.
- Dirbuster is a file/folder recursing software. It uses dictionary files to traverse through a server to find files/folders that have mistakenly been left exposed. This can be useful to an attacker as they can find log files or passwords etc. which could allow them to compromise / attack the site.
- John the Ripper is a password cracking tool. It uses a brute force attack method. It is a time consuming process.



External test will be performed and initial target will be the web server. Open ports will be checked and any known vulnerabilities checked. ~~using this information~~ Directory structure of web server will be interrogated.

This information will be used to attempt to gain ~~large~~ ~~information~~ access to any database server that are connected to the web server. Additionally access to any authentication server will be attempted. If possible, extraction of username and password data will be carried out. Using John the Ripper offline password cracking will be attempted to try and gain VPN credentials which would allow direct access to the database server and AD server.

Penetration Testing looks for vulnerabilities in a system and attempts to exploit them to gain access.

Vulnerability assessment is an audit of a system to check against lists of known vulnerabilities. Actions are generally not performed to exploit any findings.

Both cases generally involve creation of a detailed report with findings.

Contingency plan needs to be in place before any testing work is carried out. It is a legal document that needs to be signed by all parties. It needs to clearly define the goals & objectives of the pen test, and must contain details of the systems within scope of the test. Any systems that must be excluded from the test must be stated. Contact details must be included for ~~both~~ all parties so any problems can be rectified. It must be clearly stated who has responsibility for fixing any problems that arise from testing. Any specific requirements for fixing issues within a given timescale must be stated. Data backups must be taken immediately prior to any testing.

2

20