



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 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.**

SURNAME:

FORENAME(S):

1	Student Number	PI47607
2	Title of Examination Paper	Network Security
3	Module Code	MTX01701
4	Date and Time of Examination	17/5/2019 12:00 - 2:00
5	Examination Venue	IQ 310
6	Seat Number	G072
7	Number of Answer Books handed in	1

List the numbers of the questions you have attempted	Office Use
1	17
2	18
4	22
Total	57

(Gweler yr ochr arall am y fersiwn Cymraeg)

- a) A security breach happened in Campbell Downes Sedigh Corporation when a frequently visited web site was compromised. This attack installed a trojan code on users workstations by using drive-by downloads. Trojans are malicious code that appear beneficial but once executed can cause ~~damage~~ network damage, or performance issues or compromise data. Drive-by downloads are done when users access specific sites and do not require user input.

The companies anti-virus did not detect this, and this can be ~~attributed~~ due to a number of reasons. The company anti-virus could be out of date or the trojan could be a new variety, which is not located within the anti-virus database. If outdated, the software must be brought ~~be~~ up to date. If the latest version is already used, switching to more advanced software may help.

Additionally, systems ~~can~~ should be periodically scanned to ensure no malicious software are present.

The attackers used the trojan to launch a reverse telnet command that uploaded company data to hacker controlled sites. Telnet transmits all information as clear text and is less secure compared to Secure Shell (SSH). As such, it is advised that the company only utilise

SSH ~~works~~ for remote connections, as this will ensure data is encrypted. The telnet ports should be disabled in order to prevent the usage of this method. Finally, using ACLs which limit what devices can utilise telnet and SSH connections to ~~the~~ specific IP addresses will prevent standard workstations and outside devices from connecting.

The attackers used a port which allowed for outbound HTTPS traffic through the firewall. HTTPS ports are preferred over HTTP for added security. However, these ports are still vulnerable. It is ~~recommended~~ recommended to ensure all unused ports are disabled and those that are in use utilise ~~ACLs and~~ ACLs to limit what can access ~~the~~ or leave the network. In this ~~scenario~~ scenario, ACLs could be used to prevent the download of unauthorised software, which could prevent the trojan download. They can also be used to prevent certain workstations from uploading documents and data to outside destinations. Finally, they can limit SSH and telnet access to and from specific devices, ensuring only security managers can gain access.

X

- b) A security test shows attackers attempting to gain access to the network but have been unsuccessful so far. As it is only a matter of time before they gain access, it is advised to attempt to attract them long enough to trace their movements.

To do this, it is recommended to use honeypots. This is a workstation or location that is heavily monitored and so out of the way that no one should gain access to it. Therefore, any individual who access it is an attacker.

The pros of this are that it is easy to ensure only attackers access this section, it is isolated from the main network and can be easily monitored. Therefore, users who access it can be traced.

The cons, however, are that this method does present a workstation for attackers to access. Also, as this is a new section, finger print scans can be used to check access history. From this, experienced hackers may identify the honeypot which prevents tracing.

As this method is relatively new, there are very few legal issues the company may face. It should be noted that all data gathered from this needs to be considered as private data on the attacker and must not be misused and treated as any other personal data.

② a) i) There are a number of vulnerabilities which can be targeted within a website. Firstly, simple areas such as ports can be targets of attack. If a single port is compromised, ~~as it is~~ it is possible to gain access to the site. Example being from email ports, if the site utilises emails for notifications, this port can be used to upload malicious software to compromise the site.

Other vulnerabilities such as SQL injections can be used to alter site information and compromise data.

Cross-site scripting is another vulnerability that can be used to alter the site code from a client-side position. This can degrade performance and ~~also~~ bring the site down.

Vulnerability to denial-of-service (DoS) and Distributed Denial-of-Service (DDoS) will be examined, as these are popular ~~attack~~ attacks which can degrade ~~performance~~ performance and bring down the site by overloading it with ~~no~~ requests.

Other vulnerabilities can ~~include~~ include cookie poisoning, hidden field manipulation, buffer overflow and man-in-the-middle. While they ~~don't~~ do not specifically bring down a site, they can cause large ~~of~~ amounts of damage and compromise data integrity.

ii) There are many attack tools which can be used to attack ~~as~~ networks and sites. Kali Linux or Parrot are two examples of operating systems with numerous tools for pen testing.

Other tools which can be used for pen testing include:

- ~~W~~ Wireshark, which is used to track inbound and outbound packets.
- recon-ng, which can be used as a reconnaissance tool for identifying ports and other vulnerabilities.
- nmap, which can be used to map a network to identify further vulnerable systems.
- John the Ripper, a decryption tool ~~too~~ for retrieving sensitive information.
- Nikto, a site scanning tool capable of finding specific ~~ad~~ vulnerabilities.
- Metago, which can gain large amounts of information on various areas of a website or network.

/ 5

iii) There are a certain steps involved in pen testing:

1. ~~Conduct~~ Conduct research and reconnaissance of the target. This is done through both scanning software and online research.
2. Identify any weak points or vulnerabilities within the system.
3. Attempt to access these vulnerable systems.
4. Attempt to gain further information from accessed systems if successful. If not, return to step 1.
5. Further Access or into deeper systems or attempt to identify possible attacks.
6. execute potential attacks.

iv) Vulnerability assessment typically looks to identify and assess known vulnerabilities within the system. This can typically be automated and does not require large technical knowledge.

Penetration testing attempts to identify any vulnerabilities and to determine their severity. This method is done by trained individuals or groups with high technical knowledge.



v) Before committing to penetration testing, it is important to have a contingency plan to avoid network damage.

Firstly, ensuring all personal and vital data is backed up will ~~prevent~~ prevent data loss.

Pen testing has the potential of opening areas for others to attack, therefore, isolating the area can reduce this risk.

Ensuring all steps, tools, attacks and outcomes are documented to ensure to ensure the process can be repeated and to ensure all parties are aware of transactions and events.

18

12

Q a) i) Policies ensure all employees are aware of methods to enhance network security. Elements of security policies are:

- Identifying the scope of security methods
- ~~Also~~ Giving guidance of Security to employees.
- Identifying security aspects of the company

ii) Two types of risk analysis in information security are Quantitative and Qualitative ^{analysis} risks.

Quantitative ~~risks~~ analysis is a mathematical approach which ~~details~~ provides higher levels of detail. This method is typically done by trained staff.

Qualitative analysis is done if the company requires quick information, or does not have the resources for a more in depth analysis. This ~~is~~ approach can be done by less experienced individuals.

iii) Identification is the process of identifying an individual or item. This is typically user names, IDs, etc. This simply announces who or what an individual or item is with no concrete proof.

Authentication is the process of confirming the identity of the individual. This is typically done via passwords, or tokens or biometric methods.

iv) Alternative to passwords include token based systems. These utilise physical objects such as cards or tag as a method of authentication.

Biometric systems utilise biological "areas" as a form of authentication. These include iris and retinal scanners, finger print scanning and voice recognition, and to authenticate.

Multimodal Biometrics use multiple forms of biometric qualities to further enhance security. This requires more than one input to complete authentication.

Hybrid methods employ areas of both token and biometric to authenticate. This method requires both a physical token and biometric input.

Finally, physical qualities such as appearance, ~~and~~ height and physical build can be used as a method of authentication.

10

22

22



Complete, fold and seal
(see note 2 below)

FORENAME(S): Elhan

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.**

List the numbers of the questions you have attempted	Office Use
Q1	17
Q2	20
Q4	23
Total	60

(Gweler yr ochr arall am y fersiwn Cymraeg)

80%

Q1a) To secure the network against drive by downloads it is recommended that software solutions be put in place such as an internet filter that prevents employees from accessing certain ~~web~~ webpages. This can also be done on a hardware level with access control lists on a hardware based firewall. To prevent the actions from missing or not detecting the code ~~it is~~ it is recommended that the software is kept up to date with ~~base~~ security patches because the attacker ~~may~~ launched reverse ~~blat~~ attacks it is advised that ~~blat~~ be disabled for a more secure remote management tool such as ~~SSH~~. A port filter should be placed on port 80 / ~~HTTPS~~ to prevent certain information from leaving the network. It is ~~also~~ also wise to ~~disallow~~ JavaScript on the workstations to prevent the execution of ~~drive by~~ drive by downloads on the system.

Q1b) A good way to attract ~~network~~ network intruders is to set up a honey pot which is an isolated system that is designed for analysing attackers procedure and attempts. Whilst an attacker is interested in the honey pot a simple IP trace ~~will~~ would be ~~enough~~ enough to ~~track~~ track their movements. The pros of this is ~~that~~ that they are relatively inexpensive as operating systems and resources would not need to be excessive. They also allow for an in-depth look into how an attacker ~~works~~ works. The downsides are that a trace might not work if they use a VPN or IP masking software. another downside

Is that it might not even attract attention, resulting in a waste of time. There are some legal ramifications, for example it could be seen as entrapment, which in some countries is illegal as it lures people into committing crimes. Wrongful prosecution is another legal risk, while if someone accidentally stumbles on the hang pot, should they be prosecuted for an accident. Hang pots have very little legal precedent in us law as of 2018. (2018 I think)

Q2 a

i) The most common vulnerabilities that could be tested should be common attacks that could cause loss of data or damage. One vulnerability would be cross site scripting (XSS) which involves the injection of malicious code into a ~~static~~ dynamic webpage, this can ~~steal~~ steal the personal information of users that visit the company's site. The next ~~major~~ vulnerability that could be tested is hidden field manipulation which alters the hidden fields in HTML codes that use the GET or POST commands to access servers. This could result in the attacker gaining access to the server. A third ~~major~~ vulnerability to look out for is SQL injection which uses forms on the site to enter certain values that result in the attacker accessing personal information on other customers. Another vulnerability is cookie/session poisoning, which is the process of adding data on a webpage to gain information about the users.

ii) The following tools will be used:

1) Wireshark - allows an attacker to analyze packets being sent between the target and the attackers.

2) Recon - Ng - a reconnaissance tool that gathers information and credentials on a site.

3) Nmap - a port analysis tool but scans for open ports for possible attack vectors.

4) Nikto - a ~~search~~ scanning tool that looks for known vulnerabilities in open systems and hardware / firmware.

5) dmitry - ability ~~scan~~ scans for vulnerabilities ~~to~~ ^{to} ~~by~~ ^{by} ~~can~~ ^{can} attacks such as XSS or SQL injection.

iii)

The steps for the testing are as follows:

- 1) gather data on company and employees (Social engineering)
- 2) ~~search for weaknesses~~ ^{scan the network for information}
- 3) ~~scan~~ ^{scan} for specific vulnerabilities mentioned
- 4) attempt to gain access
- 5) Report findings.

iv) Penetration testing is looking for unknown weaknesses of attack, usually done by a very skilled outside employee. vulnerability testing is

focused around looking at known vulnerabilities and is often an automated task. This is done if budget is an issue.

i) The contingency plan for this attack involves the backing up of vital customer and employer data including Backup images for all operating systems and configurations. Higher up members of staff will be informed in case a sudden system shutdown. Attempts will be made to only focus on isolated systems.

Q4 a

- i) elements of policy:
- perform risk analysis
 - perform classification of assets.
 - create a security board
 - outline user access controls.
 - perform cost analysis

ii) Quantitative risk analysis - the use of mathematical calculations to understand the cost to risk of any system.

Qualitative risk analysis - focused on quality of the procedures to reduce risks (as often the least expensive and less time consuming)

iii) Identification - the process of showing who you are. Think of this as a username or login

authentication - the process of proving who you are with a shared secret. Think of this as a password or pin number.



iv) token based system - using an access card or token as proof of access

biometrics - the physical characteristics of a person to prove who they are. i.e. finger print, Iris/retinal scan, face scanner.

bi-modal biometrics - is the use of numerous biometric scanners as proof of access.

hybrid - the use of both a token base and biometric based system. i.e. access card and thumbprint.

audio - the use of someone's particular voice or phrase to ~~get~~ authenticate access.

10

23

23



Complete, fold and seal
(see note 2 below)

FORENAME(S): DOBRÁV

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.**

List the numbers of the questions you have attempted	Office Use
1	20
2	19
3	7
Total	46

(Gweler yr ochr arall am y fersiwn Cymraeg)

20	20
19	19
7	7

46 46
61%

1 a) First of all one or more of the following should be implemented near to the boundary of the network for example behind the firewall (device $\rightarrow$ firewall $\rightarrow$ Internet).

1. Web Security Appliance (WSA) whose scope is to detect malicious web traffic and/or malware travelling throughout the network. As such, the WSA should prevent the Trojan code from reaching end-user's workstations.

2. IPS (Intrusion Prevention System) or IDS (Intrusion Detection System).

The IPS role is to detect and prevent malicious traffic from reaching the network. It does so by stopping network traffic (packets) from travelling further into the network and analyzing the packets against a large "signature" database. If the packet or series of packets matches a signature known to belong to a malicious type of packet, it disallows it from further travelling into the network. As such, it would possibly detect and prevent the remote Webnet session and/or Trojan code from being established. This device however slows down the traffic rate as it has to analyze every packet with which it comes into contact.

The IDS function is highly similar to that of the IPS except it only detects malicious traffic without preventing it from further travel in the network. It may also be the less

engineering alternatives of the IPS.

As such, implement an IDS, IPS, or IDS+IPS solution depending on the company's budget and traffic rate priorities.

3. Discourage the use of the telnet protocol, and/or out-bound telnet traffic.

4. Implement a firewall policy which prevents out-bound and/or in-bound Telnet traffic.

As all telnet traffic is unencrypted, replace it with that of the SSH protocol which provides more proper authentication and privacy (encryption).

4. Educate employees on what a drive-by download is, how it operates, and ways to avoid it.

5. From the perspective of the internal network, out-bound HTTP traffic may be allowed if it is the starting point of a communication. However, HTTP in-bound traffic should be not allowed unless it comes as a response to a request from the internal network.

6) I implement a "honey-pot" that is a fake web server which pretends to be legitimate and hold legitimate useful information from the point of view of the attacker. I budget and/or time-constraints permit, enlarge the honey-pot to present itself as a legitimate network with highly confidential data.

Pros: - If implemented properly, it could serve as a good trap for the hacker. This involves the use of a program which would record the attacker's movements throughout the network/server.

Cons: - Might be costly, depending on the implementation costs of the honey-pot server and/or network.

- A legitimate user might mistake the honey-pot for a legitimate server/network, thus becoming an unintended victim.

As mentioned above the "unintended victim" factor could make the case of a legal issue.

2) SQL Injection - due to the reason that it is a very common vulnerability, as well as easy to exploit and may result in useful data such as admin user passwords.

Unencrypted session cookie - due to the reason that, if a session cookie is transmitted to the server unencrypted, it could be intercepted and used for malicious purposes. As such, it may result in ~~either extraction of information of an administrator with the help of the~~ intercepted session cookie's value.

Vulnerable servers such as Telnet - due to the reason that the availability of several open ports increases the attack surface and, in turn, number of attack vectors.

Vulnerable OS - due to the fact that, if the server hosting the web-site runs on a vulnerable

8

20

20

OS and/or runs a vulnerable / out-of-date version of the OS. It further increases the number of attack vectors as well as the risk of the impact. If control ~~is not~~ of the entire server is established, then it is possible for one to compromise the entire server and/or network/organisation it belongs to.

II

1. Nmap - network reconnaissance tool. Attempts to find open / filtered and closed ports of its target, as well as OS information (OS fingerprinting).
 2. SQLmap - similar in purpose to Nmap, helps find SQL vulnerabilities as well as help formulate crafted SQL queries for malicious purposes.
 3. OWASP ZAP - scans a web server for vulnerabilities pertaining to the Javascript, PHP, and SQL languages.
 4. Metasploit - An exploit framework tool which comes with its own interactive shell. Serves as a general convenience for ~~exploit~~ activities including exploiting, launching exploits, as well as providing / easy access to exploits found in the exploit database.
 5. Wfuzz - A fuzzing program that is a program that inserts arbitrary but significantly crafted input in a web page and/or certain parts of the URL. Useful for brute-force attacks and/or further reconnaissance of a server and its directory structure. For finding directory information.
- "Burp Suite" is a suitable counterpart similar to Wfuzz.
- III 1. Do network reconnaissance use Nmap to find the server's OS information and open ports.

2. Depending on the information found, perform a search of existing vulnerabilities for each open port, as well as its underlying operating system, with the help of the Internet and/or vulnerability exploit databases.

3. Attempt to use exploits and/or exploit programs to test their feasibility against the server.

4. With the results of the above steps, write a report on the found discoveries, as well as a mitigation plan and vulnerability assessment.

IV Penetration testing ~~is~~ is comprised of the entire process of finding vulnerabilities and/or attack vectors, surfaces. At such, it is a highly odious and practical process.

Vulnerability assessment on the other hand, strives to theorize and formally assess the level of magnitude of risk involved in the presence of one or more vulnerabilities, as well as the process of ~~vulnerability~~ mitigation of said vulnerabilities.

During the process of penetration testing, it shall be assured that:

- Unwarranted loss of data, denial of service, etc will not be engaged into. An malicious processes which may cause a denial of service, shall not be taken as a step of the penetration testing process.

- No un-authorized tampering of recording or theft of data will be taken. At such,

for example, if proven to a court shall well be established, no further action (such as hearings of directors) will be taken.

→ The generation tester will ~~take~~ engage in proper practice with regards to the policies listed above as well as others, so that no loss will be suffered on the part of the organisation and for no ~~profit~~ ~~unwarranted~~ profit gained on the part of the generation tester.

3) a) I ISO 27000 is a standardised security framework with regards to the security aspect of an organisation's IT infrastructure.

II The ISO 27000 standard is composed of a very large number of parts amounting to nearly 400, numbered from 10 to 100. (27000, 27100)

III The rule of an ISMS is to provide a means of managing the IT/information security aspects of the organisation. It helps towards ensuring, maintaining and overruling the proper implementation of information security practices throughout the entire organisation.

IV Organisation can benefit from this universal network through the following ways:

— Security: As the organisation follows a strict security framework, its level of IT security is much higher.

— Risk mitigation: Due to the above reason, the organisation is engaged with a much smaller likelihood of security breaches and thus, of unwarranted data loss, loss of profit,

loss of public image.

→ Inter-operability: Whenever multiple security solutions are employed throughout the organisation, the ISO 27000 framework provides useful information towards their proper functioning. Furthermore, no clash of procedures is present as all of them are taken into account into the framework itself.

b) The "Security Governance" is the formal procedure whereby the proper implementation of security infrastructure and security principles is initiated, checked, maintained and ensured.

(2)

(7)



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 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.**

Complete, fold and seal
(see note 2 below)

SURNAME: CHOWDHURY

FORENAME(S): ROSEN

1	Student Number	P146446
2	Title of Examination Paper	M7x01701 Network Security
3	Module Code	M7x01701
4	Date and Time of Examination	17/9/19 12:00pm
5	Examination Venue	1Q310
6	Seat Number	9066
7	Number of Answer Books handed in	1

List the numbers of the questions you have attempted	Office Use
2	19
3	12
4	6
Total	27-5

(Gweler yr ochr arall am y fersiwn Cymraeg)

50%

2ai) List of vulnerabilities:

open ports, host discovery, security misconfigurations, operating system detection, network mapping, weak passwords, weak user credentials, unsecure logins, External access, code errors, web site scripting errors, database discovery, Network performance discovery in terms of uptime and down time, firewall detection, version type etc.

4

2aii) Metasploit - This is a computer security tool which allows users to carry out security testing with the main advantage being penetration testing. It is command line and provides fast paced implementation. Framework exists mainly on Linux based OS.

NMAP - This is a network mapping tool that allows users to scan a network or system. An active scan provides the discovery of hosts and open ports while looking at other factors such as operating system discovery and firewall detection. It is open source and available on all platforms.

Acunetix - This is an automated security tool which provides the advantage of using pre-defined parameters to carry out security testing. Can discover over 4500 vulnerabilities in terms of weaknesses and vulnerabilities. Full or free version.

Wireshark - This is a network analyser tool which can actively scan a network or system to discover potential vulnerabilities as well as discovering decryption port states. Can sufficiently scan small and large networks and be used in conjunction with other security tools.

Burp Suite - This is a security auditing software tools designed to discover application vulnerabilities. Actively scans an targeted network for variants of discoveries such as port discovery, network hosts detection, web application testing, script detection etc.

XSS - This is a command line interface which is a simple yet powerful tool, provides the user the ability to inject code into the browser's script configuration to test against integrity, authenticity and strength.

2 aiii) Outline steps:

Agreement phase - A mutual agreement between the pen tester and the person in charge of the company could be the security information officer, network admin or even CEO.

Reconnaissance - This stage allows the tester to gather as much information about the intended target as possible to create an conceptual idea of the network while considering the effects of their strategy.



Gaining access - This is where the attacker attempts to physically or virtually gain access to the network system using a variety of tools and strategies. The tester will discover various ways to access the network while considering the discovery of servers, services, network performance, host discovery, mapping etc.

Maintaining access - Once the tester has managed to gain access to the network or system, it is essential that the tester is able to maintain this approach in order to fully carry out the penetration testing. In some cases of losing access after gaining the network can permanently mitigate the threat, therefore will never be able to get in.

5

~~Report & Documentation~~

Exploitation - The main phase of the penetration testing assessment is the attack itself. This is where the tester uses a bundle of security tools within their arsenal to discover the vulnerabilities and weaknesses in the network.

Report & Documentation - After successful exploitation of the network and systems and discovering potential vulnerability, it is essential that all this information is properly documented and sent to the person of authority within the company, so that they may mitigate these vulnerabilities. It is similar to security audits as well.

2aii) Vulnerability ~~scanning~~ ~~assessment~~ assessments scan for discovery of known vulnerabilities while penetration is more of an active exploit which attempts to attack an intended target for the discovery of all potential vulnerabilities and weaknesses.

Vulnerability assessment may only discover known vulnerabilities whereas penetration testing can gather a wide range of exploits such as web application vulnerabilities, port filtration, scripting vulnerability, code errors, security misconfigurations etc.

2aii) Contingency plan - This plan allows the users to create a set of guidelines to cover the areas of the pen test taking into account various factors such as risks, information specific discovery, mitigation, disaster planning etc.

The factors involved could follow as:

Business overview - information about business

Risks involved - Potential damage that can be caused

Gathering potential information prior to the pen test such as network requirements, the severity of the intended attack, the drawbacks etc.

Reconnaissance and scanning

Vulnerability analysis

Documentation

3ai) ISO framework - ~~good~~ International Standard Organisation which provides the assurance that information security is implemented properly within an organisation. It sets out the standard of governance which a company should adopt to protect its assets while complying with the concept of CIA (Confidentiality, Integrity, Availability).

3aii) How many parts - It is composed of 12 different sections covering a variety of information in relation to each aspect of information security towards an organisation.
Business needs - A thorough overview of the effects it has for organisations and what it can provide.

Risk management - What kind of implications it may have ~~have~~ towards the company, while considering factors such as sensitive data and corporate data.

Policies + procedures - the relevant and relevant information in terms of setting policies that outline key implications of the effective information security standards, and the procedures to actually follow them.

3aiii) ISMS - This system governs the concept of the ISO 27000 framework and work through interoperability. With each ISMS contains the relevant assurance that the standards of information security is well outlined within an organisation, while considering factors of protection of sensitive data, corporate data, risk analysis etc. Within the system the relevant security policies + procedures are correctly outlined with the assurance of reliable governance.

3aiv) Benefits -

Business integrity
 Standard at professional
 Information protection
 Risk management strategies
 Security policies outlined
~~the~~ An assurance of data protection
 Confidentiality, Integrity and Availability

3b) Security Governance is the effective
 assurance that ~~an~~ explains protection which
 a company may provide in terms of
 information security, while considering the
 concepts of ethics and policies.

4ai) Policy elements - Procedures, Guidelines, Baselines

4aii) Risk analysis types - Risk analysis is
 thorough in depth review of information
 security for that company. 2. Risk analysis
 for the protection of corporate or
 sensitive data.

4aiii) Identification is the discovery of a person or
 object such as name, date of birth.
 Authentication is the aspect of proving the
 identification, such as passwords. For example
 a credit card, the name would be
 identification and Pin would be authentication.



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

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 the flap 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.

Complete, fold and seal
(see note 2 below)

SURNAME:

Thomas

FORENAME(S):

Ross

1	Student Number	AL66 7661
2	Title of Examination Paper	Network security
3	Module Code	M7X01701
4	Date and Time of Examination	17 th May 2019
5	Examination Venue	SA1
6	Seat Number	301c
7	Number of Answer Books handed in	1

List the numbers of the questions you have attempted	Office Use
2a i	
2a ii	
2a iii	
2a iv	
2a v	
3a i	
3b	
4a i	
4a ii	
4a iii	
4a iv	
Total	35 1/2

17

2 1/2

16

35 1/2

47%

2)

i) The vulnerabilities to exploit are

- / Hidden Fields, This method enables an attacker to discover any hidden files or messages with the ~~HTTP~~ code of the website HTML
- / XSS (Crosssite scripting), this vulnerability will allow an attacker to inject ~~malicious~~ side script into the website to gain information from the webserver. examples of script used are Javascript and ActiveX.
- / Cookies can be exploited also & in order to bypass security. Cookies maintain session state in Stateless HTTP. Once an attacker has done this exploit an injection is done to receive unauthorized information.
- / Buffer overflow, is also an exploit that can be considered as it will allow an attacker to gain full control over a system, simply by changing the address pool for the process.
- / CAPTCHA is also another feature that could be exploited, as it is generally used ~~as~~ an ~~authentication~~ ~~tool~~ validation tool in order to make sure the user is human. If this was attacked it could cause the website to be open to DoS attacks by an attacker.

5

5

2)

i) 1) XSS injection tools could be used in this scenario to inject client side script into the website, which allows the attacker access to unauthorized content.

§

2) Zenmap is a tool that could be used in order to see which ports are open, this tool pushes traffic to the website in the form of an attack to see which ports can and can't be accessed. ~~This~~ This could be considered a reconnaissance tool.

3) Nmap also known as network Mapper, maps the network very similar to Zenmap by mapping the ports that are open, also showing details if they are TCP ports or perhaps SSH ports.

4) Metasploit is another method, however a more advanced network mapper that has a graphical interface that goes in depth by going in different servers and gathering information from them. Once the IP address is gathered it is possible to click on the IP address and dropdown options appear. Allowing you access to mailing, DNS & web servers.

5) SPARTA.



2) iii) There are 4 steps that would be taken.

1) ~~Research~~ - It is important to research the business for any known vulnerabilities prior to attack, as simple one could be apparent before the next step.

2) ~~Recon~~ - This step is the step where tools could be used such as Nmap to gather further info when attacking.

3) ~~Attack stage~~, Once all the info is gathered from the recon it should be possible to ~~attack~~ and gain access, to retrieve info.

4) ~~Evaluation~~, This step is the step to evaluate the unauthorized information that was gathered in the previous stage.

iii) There is one main difference between vulnerability assessment and penetration testing. This difference is that penetration testing ~~requires~~ relies that an attacker is gain access to the network or a users system. whereas vulnerability assessment is the the assessment of the vulnerabilities that could be used to attack and pentest. usually done by web application tools in Kali Linux's metasploitable for which gives the attacker's information as well as pentest capabilities.

2

2)
v)

There are two methods that could be used in order to protect against these threats, for instance a simple backup of the network or even a large scale backup plan where servers are backup in a remote location.

However, other ~~method~~ this does to solve the long term issue. Based on these attacks it would be wise to solve the issues weekly with daily scan for vulnerabilities to make sure developers are keeping up to date with security.

For ~~the~~ A couple of examples:

Hidden field ~~could be~~ Attacker could be stopped by using Steganography. A method to hide secret files or messages in ordinary files. However, this is not a real thing currently but can be seen for future use.

XSS ^{injection} can also be protected against by simple checks and keeping up to date with updates to the web servers security.



3a) i) The ISO 27000 is a collection of standards and policies that must be upheld to the full extent of the law.

1/2

3b) Security governance is set of responsibilities set by the board or executive director for strategic direction. examples can be used so objectives are met, resources are properly used and risks are avoided and dealt with in the correct way.

1

2 1/2

2 1/2

4a)

i) There 10 elements to making a policy work

1. gathering background information
2. Risk assessments must be done
3. Policy reviews
4. Developing an Information security Plan
5. Developing an Information Security policy
6. Implementing standards and policies.
7. Training and awareness
8. Monitoring for compliance
9. Evaluate Performance
10. Modify the policy if needed to ~~the~~ suit the company.

ii) There are Two types of Risk assessment.

- Quantitative risk assessment is used to set a monetary value on assets within a company - for example the price of recovering stolen information.
- Qualitative risk assessments are based of more traditional assessments where it would state whether or not something is low or high risk. This method is usually used if there is a tight budget or needs to be done in a ~~short~~ short period.

iii) An Example can be used for the differences between Identification and Authentication. For example thinking of Identification as someones bank card number or ID, where it holds details about who you are. Whereas Authentication is based on someones bank card pin number for which validates who the person claims to be.

Lead
id

There are many example of alternatives to passwords; simple methods are as listed mainly under biometrics.

- Fingerprint scanners
- Iris scanners
- Voice recognition
- Facial features
- ~~Two step user~~

~~Other examples could also be~~
~~these advanced methods~~

Other methods used could also be token authentication. This could be through the use of RFID Readers, where cards are used to sign someone in rather than passwords.

Other forms of authentication could also be:

- Two step authentication - where you put a password in, however to verify your the right person putting in the password can be verified by an app on your phone.
- Hybrid is also another method, believed to be using both the token method and biometrics to sign a user in.

7

16

16



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 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.**

FORENAME(S):

[illegible]

(Gweler yr ochr arall am y fersiwn Cymraeg)

Q3

- i It is a information security management system framework. Which known as 27000 standard.
- ii It is composed of many parts and the author is going to describe of them which are.

- Security policy ✓
- Risk Assessment ✓
- Compliance ✓
- Access Control ✓
- Asset Management ✓

- The security policy is used to secure the network by complying with security policies that provided by the company.

- The risk assessment is used to assess to make sure to protect a network from vulnerabilities. It's a plan of ensuring network maintained as effectively as possible.

- The compliance is used to provide awareness to the network user to comply with a specific network policies to limit any threats.

- The access control is used to secure network from unauthorized access. This can be done through a logical or physical ways. The logical is such as using software tools whereas, physical is use such as locking door to prevent any access to a room or building.

12

- The asset management is used to protect such as company assets from being damaged from internal or external users. This also allow to maintain the network as effectively as possible.

- ~~The security~~ ^{benefits} ~~organization~~ ^{role} from information security management system is to support or bits information security governance assurance which used to assist both staff as individuals and collectively to provide legal obligation ~~to~~ under protection act and privacy.

- iii - The role of information security system is used to minimize and risk management for organization to maintain the service of businesses as effectively as possible.

- B - The security governance is organizational process that used to provide protection and privacy to the business to protect confidentiality, integrity

Q 2. The vulnerabilities that targeted at the website which are.

- Denial of service
- Man-in-the Middle ~~attack~~ } attacks
- Network Analysis
- Phishing
- Misconfigurations

To defend the above vulnerabilities, it requires number of considerations.

- Use physical ~~with~~ firewall that has latest feature to allow enable the to protect those threats.

- Use website firewall to configure to ensure alert you when there is suspicious activities on the website and inform you.

- Keep up to date the hardware and software to eliminate vulnerabilities.

- Use two-way factor authentication so that the hacker need two credential code to attempt of accessing network. The second key code can be set up to alert you through either email, phone, or message.

ii The attack tools that are going to be recommended for this report are.

- NMAP
- Nikto
- Angry IP Scanner
- ICMP scanning
- John the Ripper
- Wireshark

The nmap is used to discover unused/open ports on a network through zenmap.

The Nikto is used to examine a network and computers on that specific network.

The angry IP scanner is used to discover IP address, network and system on the network to examine the vulnerabilities.

The ICMP scanner is used to discover IP addresses, live network maps.

The John the ripper is used to assess network vulnerabilities to ensure threats are protected.

The Wireshark is used to discover a network real time this includes, time, IP address, threat at that ~~sample~~ moment to ensure action is taken to protect network.

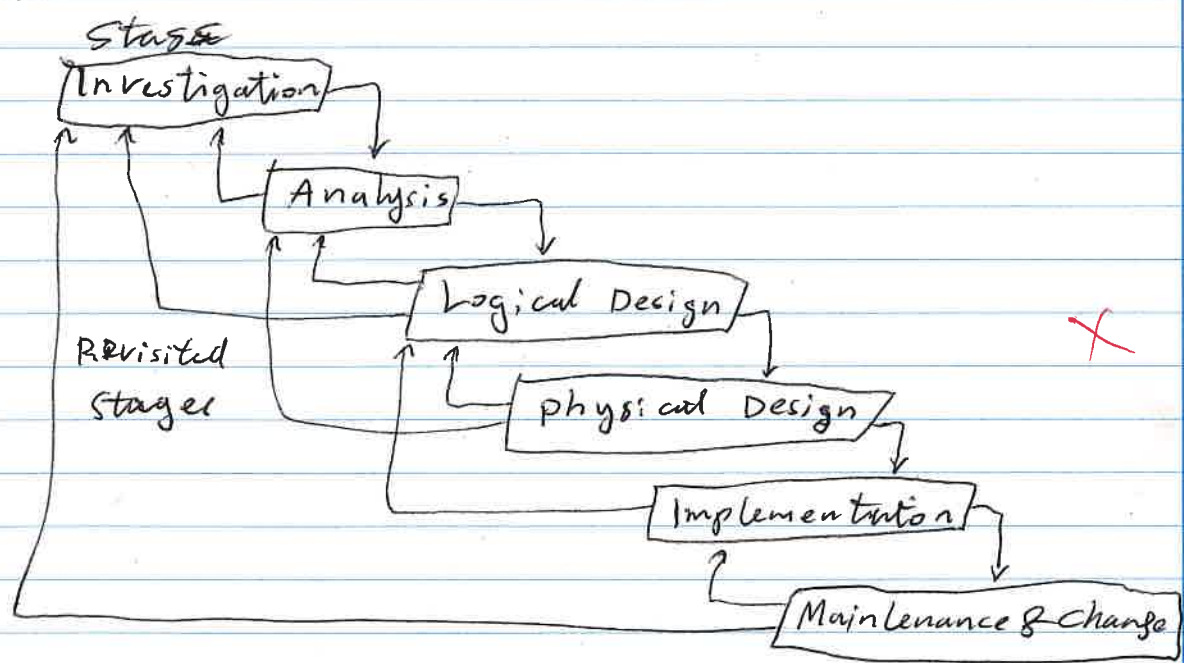
iii • Agreement Phase

- Planning and Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Exploitations
- Evidence collect and report generation

vi The penetration testing is manual process that conducted through combination of hardware and software. The tool such as NMAP and entering IP address manually to start process is the pen testing method.

The vulnerability assessment is method of conducting through automated test which is automatically processed. For example, use of scanning tool that without entering commands. Antivirus software is an example of automated vulnerability assessment.

v The contingency plan is very important as it allow to be aware of risk that could occur or already been occurred. This include the following steps.



The above stages used to ensure the penetration testing is maintained efficiently.

14

14

Q4

- i
- Risk assessment
 - Operation management
 - Industry-recommended practices
 - Implement security policy
 - Compliance
 - Eliminate security risks

ii

- Security needs
- Security operation
- Industry-recommended practices

The security needs used in information security to provide protection to the organization to keep confidentiality, integrity and availability of information from unauthorized access.

The security operation is used to ensure the network maintained as effectively as possible to provide services to the users.

The difference between Identification and authentication is that, the identification is used to identify someone through a unique user ID or password. Whereas, authentication is used to authenticate a user entering password to allow gain access to a network. The identification identify identity of a person and authentication authenticates a person to access into a system.

VI There are number of password systems used in the computer network systems. The method includes,

- AES/3DES
- DES
- Bluefish
- MD5
- IDEA

They all used to encrypt and decrypt communication between the source and destination. The AES uses symmetric algorithm of block cipher to maintain encryption. It uses bits ~~key~~ and one key used for both encrypt and decrypt. The DES uses two keys one for encrypt and second for decrypt. The bluefish uses algorithm to maintain ~~the~~ encryption and MD5 is uses signature which is digital.