



## 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.**

Luxbon

**FORENAME(S):**

Soder

|   |                                  |                  |
|---|----------------------------------|------------------|
| 1 | Student Number                   | 939822           |
| 2 | Title of Examination Paper       | Network Security |
| 3 | Module Code                      | M7x01701         |
| 4 | Date and Time of Examination     | 12/1/2018        |
| 5 | Examination Venue                |                  |
| 6 | Seat Number                      |                  |
| 7 | Number of Answer Books handed in | 1                |

[illegible]

## Netowrk security exam

Q1 What services are running and security implimentations.

Fig1 demonsttates the use of Nmap being utilised to target the IP address 192.167.0.2  
(www.insecure.org.nmap)

The scan ran 1646 port tests which resault in all bar those present on the screen found to be closed.

The scan found the common ports were tested and found to be in use, for example the SMTP(Simple Mail Transfer Protocol) port was open which is no neccesary for the server unless it is hosting a email server. The reprocuissions of port 25 being open is that if the port is open to the server and there are no custom tools, firwalls, IDS(Intrusion Detection System)/IPS(Intrusion Prevention System) and hardend security features internally introduced on the system then it can be easily exploited. This would be in the form of packet forming creating packets that when are through the port and are analysed, pivot and release a worm or virus. In addition port 80 is being utilised form common HTTP(Hyper Text Transfer protocol) however this in its self is a insecure protocol due to the face that it is succceptable to a number of attacks thus resaulting in the server and the clients being effected by viruses and worms. However more specifiially with HTTP the webpage can be effected by css/xss (Cross site-scripting) and injection attacks(Java) which change the intetion of the webpage so the users as stated can have trojans and keyloggers implimented into there systems if they are not secured and patched. The main dissadvantage to HTTP especialy for users these days and the abundance of WI-FI(Wireless Fidelity) is that MITM(Man in the Middle) attacks are easy to impliment and stable to replicate. THis is also seen within wired networks through proxys which change the code implimenting advertising as an example or change the advertising implimenting stenography. Meaning the implimentation of malicios code into digital application and objects such as advertising pictures and word documents to download. Therefore nmap in this instance demonstrates a simple implimentation of TLS2.0 or SSL(Secure Socket Layer) encryption could be added to remedy the problem.

An exampele of the code change could be

HTML.xss

head = "insecure.org"

body = "xyz"

Href = "1nsecure.org/PDF"

so changing the l in insecure to a one 1.

Other services that are un-neccasry are direct connection to the LDAP services on ports 389, 3268 and 3269 which are suseptable to LDAP injection effectively like MySQL injection changing the data wthin the directory database. Outside connection to these ports should not be visible or at the very least

overscated with proxy access and VPN(Virtual Private Network)/IPSEC(IP Security).

In addition just by the scan we know what the server is running IIS which is microsoft systems for web servers and internet applications. This again should not be that easy to interpret and should be closed. Effectively the remaining ports that should be left open are POP3 on port 110, the updates inclusion of port 443 HTTPS and a RDP or a VPN link that the webserver should be expeling. The remaining ports should be closed or atleast have custom rules and firewall exceptions in addition to network implimentaiton of IDS and IPS to analyse and prevent attacks. In addition the server could be protected behind services such as cloudfares WAF (Web Application Firewall) protecting the identity of the server and preventing DDOS (Distrobuted Denial of Service) attacks in the future preventing services to run. 9

Q1.b four port scanning tools, port scanning types such as SYN,ACK,FIN.

In order to diversify the way in which the company scanning tools are analysed to see the different results encountered the use of a variety of applications such as OWASP ZAP, Shodan, Microsoft Netscan for IIS utilities and wordpress-analyser are discussed below.

The OWASP Zap utility is a tool developed by OWASP that utilises open source technology inherited from programs such as NMAP however developed in different paths and different modifications analysing and provoking responses from the searches in different ways.

Owasp ZAP is a tool that develops the simple scanning of ports then correlated that to the data gained from the ports such as the application used on the server or the server OS its self. From that a determination of kernel version can be made or patch version to see if the systems are up to date and what are the known effects against the data presented in the OWASP ZAP application. The database using CVE determines for instance if the server has kernel vulnerabilities and if so how many and what level of exploitation and operation it is at meaning the effectiveness of the attacks that can be assaulted on the server. OWASP ZAP also checks the sessions of the website in question and then spiders through the links meaning that all the links in the webpages are analysed to see if any are susceptible to attack and exploitations such as session hijacking and client side configuration to the server. Therefore the use of common search parameters SYN, ACK, FIN, XMAS are searched but added modifications means the searches are not so protocol specific but use the same strategy of querying the database and analysing the results. 7

Shodan is a multi tier independent analyser that looks into all the available connection on the webserver, this means that for instance all the ports are scanned and then the chain of servers connected to the webserver in question are highlighted. This proves especially helpful when for instance there is a website on a godaddy webserver and you want to attack the cPanel parameter thus change the webpage and all the configurations on the website such as email. The scanning parameters therefore check for open ports and all connected links to the servers and domain names/server names. This presents a great map from which to read if you wanted to get an overall perspective of links in the network chain and see where the 16

weaknesses could be exploited from that.

Microsoft Netscan is a developed scanning tool by Microsoft that is built for the sole purpose to detect its own systems and analyse exactly what version is running and the way how to update and it specifically. This applications tool is primarily for the purpose of highlighting patches that should be deployed onto the systems and the repercussions if they were not. This scan as a result is a proprietary focused application specifically looking at updating the systems.

Lastly Wordpress analyser is an open source application that develops the CVE database and others that determine all known weaknesses on Wordpress webpages. This can result for instance in analysing themes that people implemented onto the web servers and the other Wordpress application addons that are not frequently updated and easy to exploit. This however is solely useful when detecting Wordpress sites meaning that other website scanning tools should be researched into if that is not utilised.

(16)

Q2

i.

In my approach towards detecting and analysing vulnerabilities which I wish to target then I would use the most commonly susceptible attack parameters first which have a proven track record of success.

- SQL injection meaning that the SQL database behind the website via a PHP website script could be queried and exploited changing the parameters of data and fields.
- XSS/CSS cross-site scripting is the process of effectively changing the website's contents that could be malicious in nature when passing through an encrypted channel of communication to advantages proxies and MITM attacks.
- DDoS attacks which if not properly defended behind sites such as Akamai and Cloudflare will result in the website being taken down and the millions of requests received across the distributed internet from end devices. This will result in the website being unable to serve its services.
- LDAP injection meaning that the web server might be hosted where the LDAP is attackable and so therefore the exploitation of this service may result in changing data fields and processes on the server causing the website not to function.
- Session hijacking is another method where by if a user is logged in and a session cookie is detected and taken by the attacker then they could potentially be mistaken by a system administrator and having in some cases the field prefilled such as passwords. As a result of the cookie containing this data meaning the website can be taken down from the primary control board such as cPanel.

4

ii.

The 5 primary attack tools that would be deployed in order to test many different vectors and resources belonging to the company would be as followed.

- Nessus, this is an extremely advanced and trusted application used by millions of people around the world to test their systems. The tool can detect a variety of things such as the basics like port scanning. Then it can diversify by modifications looking for tools developed by the NSA and internal kernel exploitations in addition to webserver exploits all packaged and ready to go having an effected pre-assembled attack strategy configured within the software once the site has been analysed.
- Kali Linux is the open source operating system that hosts the widest variety of tools seen within the cybersecurity world taking on packages such as Jack the Ripper and Wi-Fi detect and packet sniffer, all having specialised uses to bruteforce, detect and interpret/hack the available target resources.
- Google search, this is the most simple method however can be the most effective by simply finding information on the site, the owners, the WHOIS information etc and see exactly as a perspective on all the elements exactly where the website could be effected and therefore the business. This could mean simple details on the software used to host the website or the cPanel tool not hidden.
- Human interface is a tool in its self using your own skills via social engineering to communicate via telephone or email. Through this technique you can persuade and overcome people's natural tendency to help thus gaining access to private data and confidential details. This could be ringing up the office finding out the boss's telephone and sending him a picture via SMS, through which steganography could be deployed to keylog and capture all the data on the boss's phone as a result of the software virus.
- Shodan is the other primary attack tool because it provides an extremely well detailed insight into the communication structure between servers in addition to the ports, addresses and cryptographic details in addition to the location of the place. The use of metadata and scanning tools on the website mean that simple breakdowns mean that a logical path can be developed within the systems querying and analysing for weaknesses.

4/2

iii.

The penetration testing approach can be broken down into three sections pre-attack, attack and post-attack. This means that a methodological approach should be taken in order to attack the website in the most effective means possible. The result of which can simply be expressed as above so the identification of the target should be made firstly, determining the scope of the project, who runs it, how big is the company etc. This determination can often resemble the skill required when attacking

company websites as smaller independent businesses may not have the money to afford the extra services such as WAF or could false DDOS protection and analysis. This means that the determination of time and resource should be accomplished in the first stage.

No.2 the analysis of the research should then be broken down into active engagement with the servers and communication parameters and processes. So using social engineering or active probing of the network and its the scanned results will deliver the details about exactly what the system are running and from there the best way to attack them.

No.3 Is to attack the site now trying to probe through the systems of control which when broken will result in access to the command and control systems required to take down and effect the site. However if this can not be achieved then DDOS would be another method of attack if all communication was to be halted.

No.4 is when the attack is successful through the methods stated, what should be done from there, e.g a worm on the network or keyloggers on machines, cryptowall trojan the devices. This stage concludes in the part of an attacker a successful mission.

No.5 if this was a trial testing method then the negotiations within contingency policy and AUP acceptable use policy would come into effect showing the quantitative data gained through the search and a report summarised.

iv.

A vulnerability assessment is when an assessment is to be made on the components within the company network such as misconfigured devices or improper security protocols and defences and patch analysis. The vulnerability assessment is therefore a focused look into the systems for errors and updates that should be undertaken to improve the company's security stability. The downside to the assessment is that it is relevant only at the time of writing as new malware etc come out all the time so a new assessment would have to be written.

Pen testing looks into the entire company structure searching for weaknesses and vulnerabilities assessing all the components and providing suggestions on how to overcome and improve the company's structure. This could be through social engineering or actual application exploitation.

v.

The contingency plan would consist of AUP policy, risk analysis and company availability to conduct such test as to not effect the services. The plan would result in only at certain times of day under particular conditions when the test could be attempted. In addition the limitations to the test would be set so to not interfere with the company. The configuration of a SLA which would have lines of conduct which the pentesters must abide by in order for the company to have the proper level of verification of security whilst also not receiving the appropriate level of analysis.

Q3

i.

Testing can be broken down into many levels, internal, external grey, black or white hacking.

The external testing would depend on the situation and would mean varying level of information so a black or grey hat attack so the pen testers have some or no information on the systems from the outside. They then use and develop the information gained in order to attack the site remotely. Internal testing is the same again however being any of the hat flavours black, grey or white however the advantage to internal testing is that there is the possibility to have physical access to the machines unlike that seen with external source who are purely in contact digitally or via proxy using phishing and tricking people into turning off the machines or attaching devices to the servers or switches.

ii.

Black box testing is when the pen testers or hackers have no knowledge of the target company systems and depending on the interpretation potentially malicious in intent. This means that all attacks and reconnaissance conducted would be from scratch and a report assembled would be developed to as the research and attacks were being conducted on the company. Again depending on the interpretation from there a black box tester/ hacker may then sabotage or sell the data gained from the attack whilst a white hat hacker will report the problem and hopefully get a bug bounty. A white box tester is a person who has insider knowledge of the target systems and knows all the data and structures. This results in easier analysis of results not having to waste time on searching for names and features. However this can mean in white box testing that because it is assumed that everything is known about the system that certain elements shouldn't be tested. This results in missed and improperly analysed and assessed results which may cost the business down the line.

iii.

Announced testing is when the company is aware of the penetration testing that is going on, they have either paid specialist to conduct the scans or have allowed a company to attempt to break their systems. This is seen as an effective way by businesses to encourage hackers to invest time and money into cracking the resources such as the messaging app telegram that actively encourages users to attack the application. This means that the company is prepared and structured in the event of an attack or from this announced testing will create one as a result. Unannounced testing is when the company is either in the state they paid a company to attack them however not give notice and so to keep the security team and systems at an effective level. However it can also be interpreted as general testers analysing the systems scanning and testing for things actively without the company's knowledge.

iv.

Automated testing is when the applications have a the organisers of the testing pre assembled a process

and procedure to attack and test systems, the automation is adapted so that it actively and independently assaults the target. This automation means that whilst an application is actively engaged in testing the deployment of other vectors may be utilised. Manual testing is when the testers have to do the applications and configurations by their own ability therefore there is a specific use and application at work which may have to be implemented incrementally as the object application may be unstable or not fully developed requiring the users to implement the process as they are conducted.

3

b.

The penetration service level agreement is when there are agreed parameters through which the company should be tested. This could be the time of day, the place and application and the extent to which they test. The longevity of the tests would also be under review, through that the agreement would enact policy and redundancy procedures which would be carried out if attacks were successful. The SLA would develop multiple areas of qualitative, quantitative risk analysis the accountability, authorisation and access controls given in addition to the confidentiality, integrity and availability of the systems. This covers ISO 27001 and ISMS procedures to make sure that company and client private data is not leaked. The SLA defines parameters therefore through which they can operate. Those components therefore allow the company to recover and be in the best position to develop from the knowledge gained or be in a time and place where the recovery of systems will not interrupt business.

3

14/2

Symmetric

Asymmetric

Hash

WEP ~~AES~~ 128bit ~~key~~ block 24bit IV, 128bit key RC4

WPA RC4 + 256bit TKIP key 48bit IV

WPA2 AES & CCMP encryption & Authentication.

AES Asymmetric, 128bit block cipher

RSA Asymmetric, 1024bit key, POP & Email

DES 3 x 56bit keys, Symmetric

Blowfish replaces DES up to 448bit key, Symmetric

Omnidirectional 360 Antenna

Unit directional PCP Antenna

Web APP

SQL Injection

Session Hijacking

XSS Cross Site Scripting

MySQL Injection

DDOS Attack

LDAP Injection (I'm my input in search)

ISMS = Information <sup>Security</sup> ~~System~~ Management System

ISO 27001

Qualitative risk analysis

Quantitative risk analysis

A, A, A

Accounting, Authorisation, Access control

C I A

Confidentiality

Integrity

Availability

Brute force, ~~password~~ Dictionary etc.

pre-Attack, Attack, post-Attack method).

Identify the target

Analyze / research the target

Attack the target

Exploit the target.

Vulnerability Assessment = looking at the different components on the network (checking for human error, configuration problems, patches & updates etc).

Down side to the Vulnerability Assessment is they have to be done frequently to assess the network accurately as the report is only relevant at the time of making it. e.g. viruses come out the week after the assessment is up'd.

Pen testing looks at the whole process of the target company with human targets (email/phone phishing) to devices. The security structure therefore.

5 Altair tools

Kali Linux

recon

google search engine

Shodan search

Human intelligence (phishing / email, phone).

Contingency plan

Acceptable use policy

Risk Analysis

(Qual / Quant)

procedures / limitations to testing

depends on the type (Black/gray/white)  
Hacking.