جامعة بيرزيت

BIRZEIT UNIVERSITY

Name: Jumana Abu Murra Day: Wednesday

ID:1220594 Date: 2.JUN.2023

Dr: Asem Kitana section:2

Assignment#2

Question 1:

What is the output of the switching function in S-DES algorithm, if you know that the plaintext is (00111011) and the key is (1010010010)? Show the details of your answer.

Key: 1010010010

P10:1000001101

LS-1:0000111010 (deployed on both halves of P10)

P8:10100101 (represents k1)

Round 1

Plaintext:00111011

IP:00101111

R-half:1111

l-half:0010

EP:11111111 (deployed on R-half)

XOR: 01011010 (EP XOR K1, which represent substitution)

S0:0101 (left half of XOR deployed on S-Box 0)

row = 01 (decimal 1)

column = 10 (decimal 2)

output =01 (row 1 and column 1 of S0)

S1: 1010 (right half of XOR deployed on S-Box 1)

row = 10 (decimal 2)

column =01 (decimal 1)

output =00 (row 2 and column 1 of S1)

S0S1:0100

P4:1000 (deployed on S0S1)

XOR:1010 (P4 XOR L-half)

Result:10101111 (XOR + R-half)

End of round1

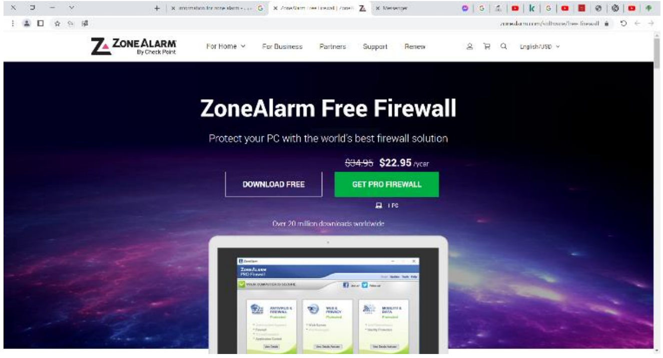
SW: 11111010(swapping the two halves of Result

Question 2:

Consider the approach of host-based security. Search for a free firewall tool/software. Visit the manufacturer website; look up the product description, such as the installation process, setting up the product process, and the process of creating firewall policies. Your task is to install the firewall software on your personal computer, then to create TWO firewall policies.

You should submit different screenshots that show your process, with a brief description on each screenshot.

1)Here we can see the firewall software main website with the download for free option or upgraded protection with pay per year

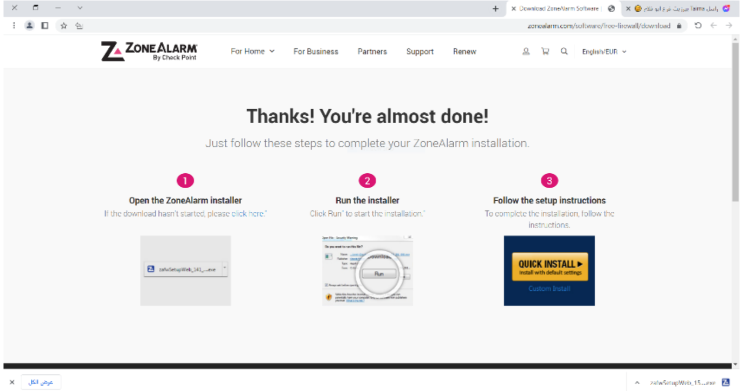

ZoneAlarm Free Firewall

Protect your PC with the world's best firewall solution

~~$34.95~~ $22.95 /year

Over 20 million downloads worldwide

2)After pressing download this is the page we see and the software starts downloading



Thanks! You're almost done!

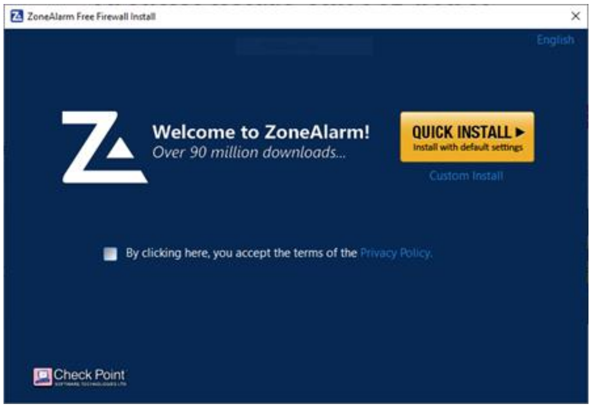
Just follow these steps to complete your ZoneAlarm installation.

1 Open the ZoneAlarm installer
If the download hasn't started, please click here."

2 Run the installer
Click Run" to start the installation."

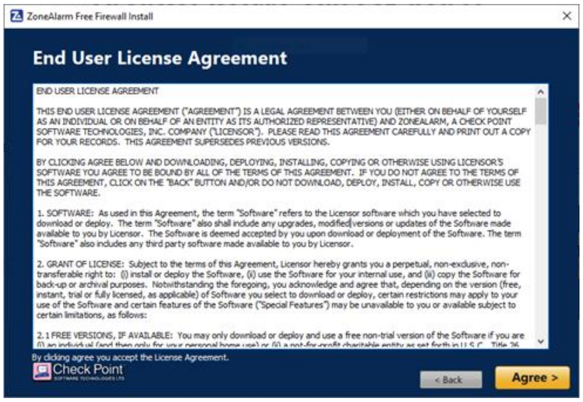
3 Follow the setup instructions
To complete the installation, follow the instructions.

3)The downloading and installing progress of the software


ZoneAlarm Free Firewall Install
English
QUICK INSTALL ▸
Install with default settings
Custom Install
Check Point
SOFTWARE TECHNOLOGIES LTD

Welcome to ZoneAlarm!
Over 90 million downloads...

□ By clicking here, you accept the terms of the Privacy Policy.



End User License Agreement

END USER LICENSE AGREEMENT

THIS END USER LICENSE AGREEMENT ("AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER ON BEHALF OF YOURSELF AS AN INDIVIDUAL OR ON BEHALF OF AN ENTITY AS ITS AUTHORIZED REPRESENTATIVE) AND ZONEALARM, A CHECK POINT SOFTWARE TECHNOLOGIES, INC. COMPANY ("LICENSOR"). PLEASE READ THIS AGREEMENT CAREFULLY AND PRINT OUT A COPY FOR YOUR RECORDS. THIS AGREEMENT SUPERSEDES PREVIOUS VERSIONS.

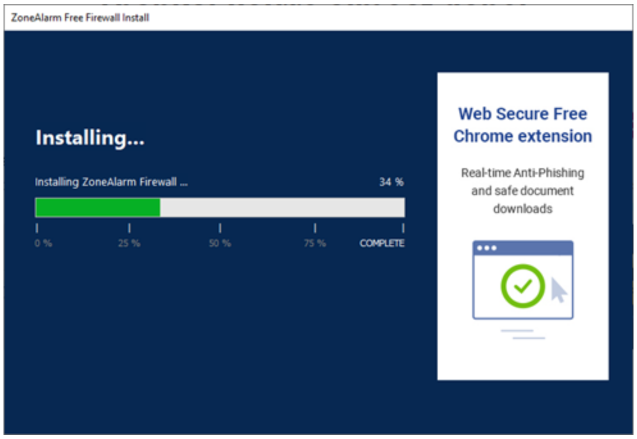
BY CLICKING AGREE BELOW AND DOWNLOADING, DEPLOYING, INSTALLING, COPYING OR OTHERWISE USING LICENSOR'S SOFTWARE YOU AGREE TO BE BOUND BY ALL OF THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, CLICK ON THE "BACK" BUTTON AND/OR DO NOT DOWNLOAD, DEPLOY, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1. SOFTWARE: As used in this Agreement, the term "Software" refers to the Licensor software which you have selected to download or deploy. The term "Software" also shall include any upgrades, modified versions or updates of the Software made available to you by Licensor. The Software is deemed accepted by you upon download or deployment of the Software. The term "Software" also includes any third party software made available to you by Licensor.

2. GRANT OF LICENSE: Subject to the terms of this Agreement, Licensor hereby grants you a perpetual, non-exclusive, non-transferable right to: (i) install or deploy the Software, (ii) use the Software for your internal use, and (iii) copy the Software for back-up or archival purposes. Notwithstanding the foregoing, you acknowledge and agree that, depending on the version (free, instant, trial or fully licensed, as applicable) of Software you select to download or deploy, certain restrictions may apply to your use of the Software and certain features of the Software ("Special Features") may be unavailable to you or available subject to certain limitations, as follows:

2.1 FREE VERSIONS, IF AVAILABLE: You may only download or deploy and use a free non-trial version of the Software if you are (i) an individual (and then only for your personal home use) or (ii) a not-for-profit charitable entity as set forth in U.S.C. Title 26

By clicking agree you accept the License Agreement.



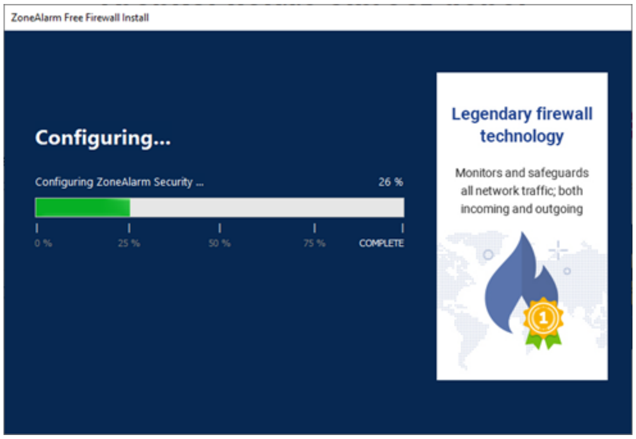
ZoneAlarm Free Firewall Install

Installing...

Installing ZoneAlarm Firewall ... 34 %

Web Secure Free Chrome extension

Real-time Anti-Phishing and safe document downloads



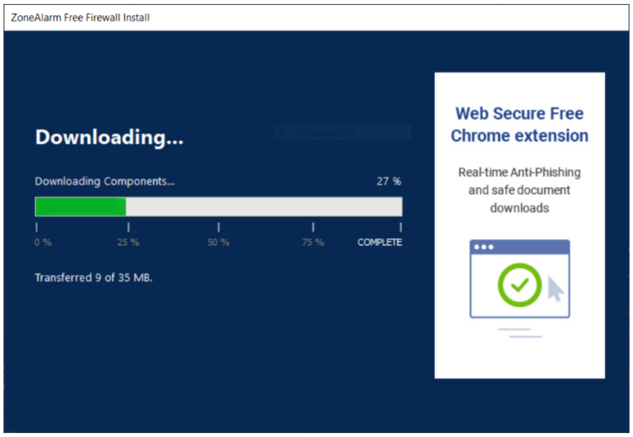
ZoneAlarm Free Firewall Install

Configuring...

Configuring ZoneAlarm Security ... 26 %

Legendary firewall technology

Monitors and safeguards all network traffic; both incoming and outgoing



ZoneAlarm Free Firewall Install

Downloading...

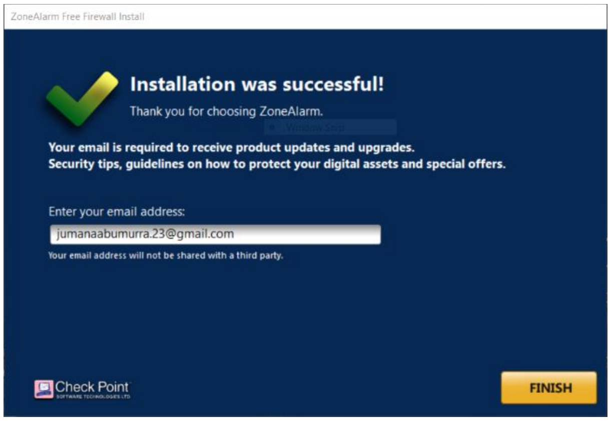
Downloading Components... 27 %

Transferred 9 of 35 MB.

Web Secure Free Chrome extension

Real-time Anti-Phishing and safe document downloads

,



Installation was successful!

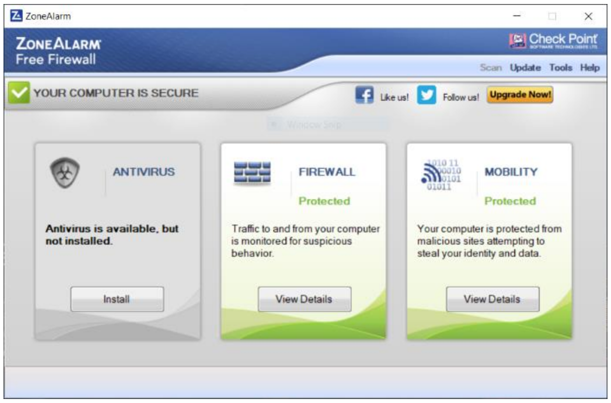
Thank you for choosing ZoneAlarm.

Your email is required to receive product updates and upgrades.
Security tips, guidelines on how to protect your digital assets and special offers.

Enter your email address: jumanaabumurra.23@gmail.com

Your email address will not be shared with a third party.

4)After installing and running the program we are greeted by the interface of it



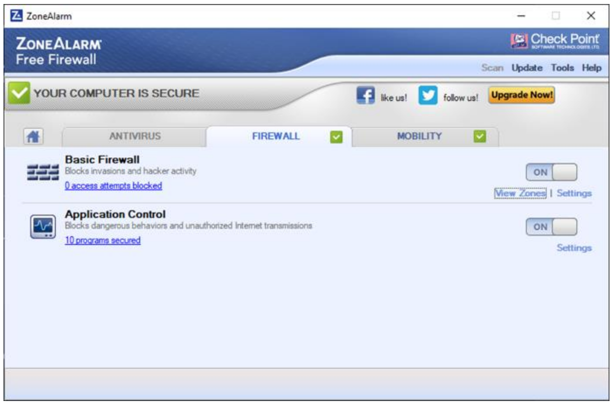
YOUR COMPUTER IS SECURE

ANTIVIRUS: Antivirus is available, but not installed.

FIREWALL: Protected. Traffic to and from your computer is monitored for suspicious behavior.

MOBILITY: Protected. Your computer is protected from malicious sites attempting to steal your identity and data.

5)After clicking on firewall we see 2 options are previewed

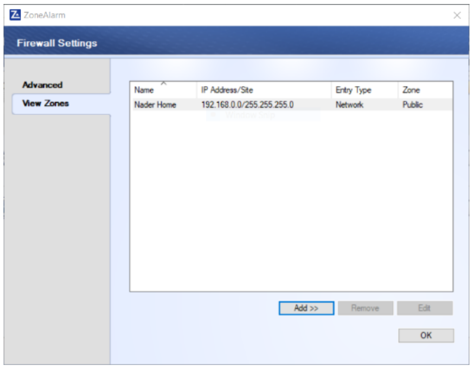


YOUR COMPUTER IS SECURE

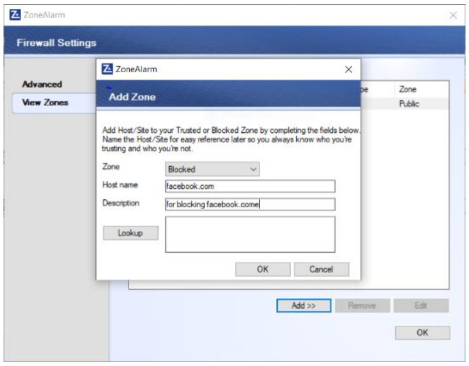
Basic Firewall — ON
Blocks invasions and hacker activity
0 access attempts blocked

Application Control — ON
Blocks dangerous behaviors and unauthorized Internet transmissions
10 programs secured

6) These are the default policies that are set up for the software with trusting both of them



Name	IP Address/Site	Entry Type	Zone
Nader Home	192.168.0.0/255.255.255.0	Network	Public



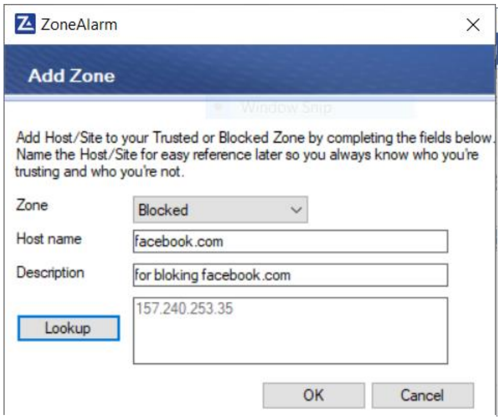
Add Host/Site to your Trusted or Blocked Zone by completing the fields below. Name the Host/Site for easy reference later so you always know who you're trusting and who you're not.

Zone: Blocked

Host name: facebook.com

Description: for blocking facebook.come

7)After putting in the host name the software provides a lookup feature that finds the ipaddress of the domain.



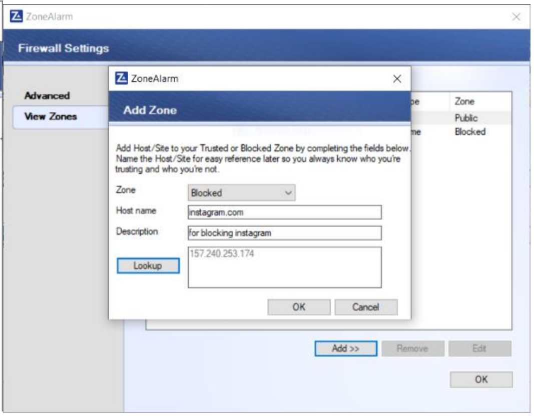
Add Host/Site to your Trusted or Blocked Zone by completing the fields below. Name the Host/Site for easy reference later so you always know who you're trusting and who you're not.

Zone: Blocked

Host name: facebook.com

Description: for bloking facebook.com

157.240.253.35



Add Host/Site to your Trusted or Blocked Zone by completing the fields below. Name the Host/Site for easy reference later so you always know who you're trusting and who you're not.

Zone: Blocked

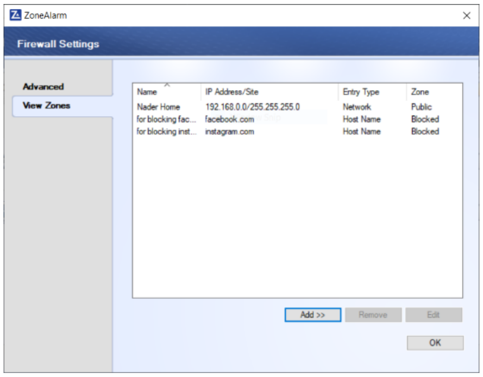
Host name: instagram.com

Description: for blocking instagram

157.240.253.174

Zone
Public
Blocked

8)The 2 policies that i added (For testing purposes) and blocked access to these sites

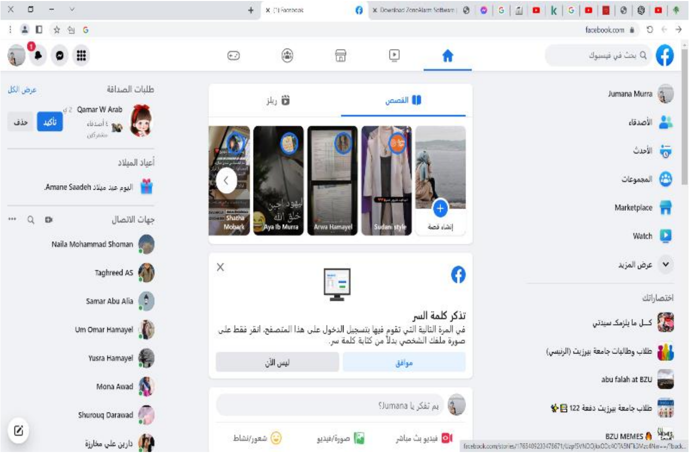


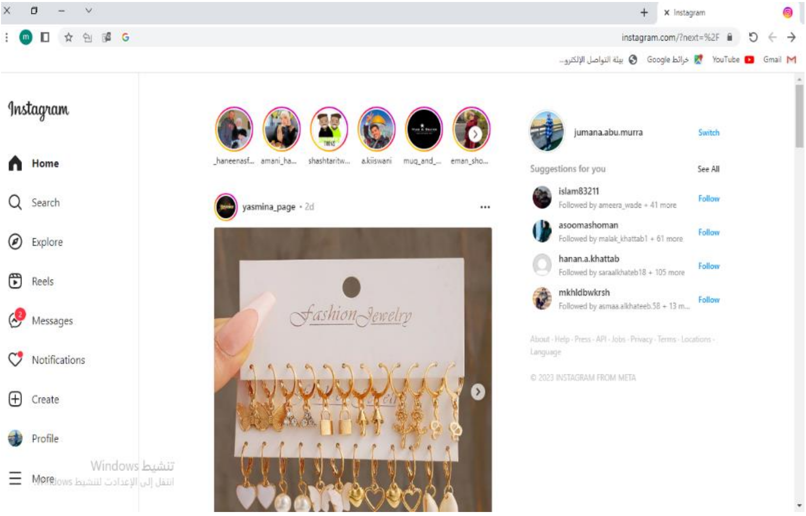
ZoneAlarm

Firewall Settings

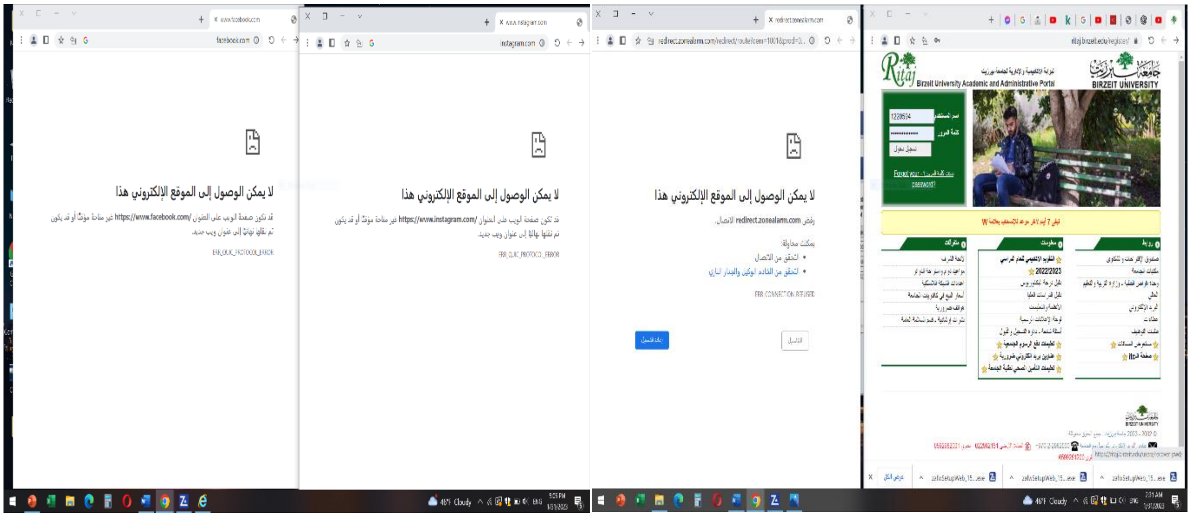
Name	IP Address/Site	Entry Type	Zone
Nader Home	192.168.0.0/255.255.255.0	Network	Public
for blocking fac...	facebook.com	Host Name	Blocked
for blocking inst...	instagram.com	Host Name	Blocked

The 2 sites before the policies were configured





After the 2 policies were added these sites no longer open and another site opens like normal for proof.



لا يمكن الوصول إلى الموقع الإلكتروني هذا

قد تكون صفحة الويب على العنوان https://www.facebook.com/ غير متاحة مؤقتًا أو قد يكون تم نقلها نهائيًا إلى عنوان ويب جديد.

ERR_QUIC_PROTOCOL_ERROR

لا يمكن الوصول إلى الموقع الإلكتروني هذا

قد تكون صفحة الويب على العنوان https://www.instagram.com/ غير متاحة مؤقتًا أو قد يكون تم نقلها نهائيًا إلى عنوان ويب جديد.

ERR_QUIC_PROTOCOL_ERROR

لا يمكن الوصول إلى الموقع الإلكتروني هذا

رفض redirect.zonealarm.com الاتصال.

يمكنك محاولة:

- التحقق من الاتصال
- التحقق من الخادم الوكيل والجدار الناري

ERR_CONNECTION_REFUSED

Question 3:

List the three main advantages of deploying a honeypot, and list two practices that could be used to enhance the reality of deploying a honeypot.

Three main Advantages are:

- Divert an attacker from accessing critical system
- Collect information about the attacker’s activity
- Encourage the attacker to stay on the system long enough for administrator to respond

Two practices that could be used to enhance the reality of deploying a honeypot:

- Fill the honeypot server with some information that may seems critical so the hacker gets happy and doesn't think that he entered a honeypot
- Increase the security and defenses level on the honeypot so that it doesnt look like a decoy to the hacker

Question 4:

What is a zero-day attack? Which one of the IDS categories is the most suitable system for protecting against such an attack, and why?

Zero-day: a broad term that describes later discovered security vulnerabilities that attackers can use to attack systems. The term "zero day" refers to the fact that at this point the seller or developer has learned of the defect - meaning they have no "days" to fix it. A zero-day attack occurs when hackers exploit a flaw before developers have had a chance to fix it.

The most suitable IDS class system against such an attack is Anomaly Detection IDS because it analyzes a set of system properties and compares its behavior against a set of expected values. It reports an intrusion when there is a deviation from the expected behavior, so it is able to detect any new intrusions so that administrators know there has been an intrusion and when the hacker takes no action, it is likely zero-day. Attack becomes very high, it may also be a new normal since abnormality is detected IDS False positive rate is very high.

Question 5:

Explain in details the Smurf attack, and list two practices to protect from such an attack.

- The smurf attack broadcasts a ping to all of the machines on a local network.
- It forges (spoofs) the return address of the ping packet to be that of the victim.
- All of the machines receiving the broadcast ping then send reply packets to the victim.

Computers and networks can help prevent themselves from being used as intermediaries in the attack.

- Computers do not reply to broadcast pings.
- Block broadcast packets at router.