CYBS 3323

Test 2

Fall 2024

|  |  |
| --- | --- |
| Name: | Daren Diaz |
| Student ID: | 113487126 |

**Instructions.** You have 150 minutes to complete this exam. You can access any resources of information, including calculators, electronic devices, textbooks, or notes. It would be recommended to solve the problems by yourself. In case of hand-writing, please write your answer clearly. If we cannot read your writing, it may be difficult to be graded.

**Academic Integrity Pledge.** This course operates under the rules of the Office of Academic Integrity at the University of Oklahoma. Your signature endorses the pledge below. After you finish your exam, please sign on the line below:

*I have neither given nor received aid on this examination, nor have I concealed any violations of the Academic Integrity.*

|  |
| --- |
|  |

1. Logic Gate in the Digital Logic Circuit:

Please complete the truth table and answer the followings:

(a). 1-input NOT gate

|  |  |  |
| --- | --- | --- |
| Symbol | Truth Table | |
|  | Input1 | Output |
| 0 | 1 |
| 1 | 0 |
|  |  | |

(b). 2-input NAND gate

|  |  |  |  |
| --- | --- | --- | --- |
| Symbol | Truth Table | | |
|  | Input1 | Input2 | Output |
| 0 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |
|  |  | | |

(c). 2-input NOR gate

|  |  |  |  |
| --- | --- | --- | --- |
| Symbol | Truth Table | | |
|  | Input1 | Input2 | Output |
| 0 | 0 | 1 |
| 0 | 1 | 0 |
| 1 | 0 | 0 |
| 1 | 1 | 0 |
|  |  | | |

(d). 2-input XOR gate

|  |  |  |  |
| --- | --- | --- | --- |
| Symbol | Truth Table | | |
|  | Input1 | Input2 | Output |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Circuit | Truth Table | | | |  |
| A diagram of a nand  Description automatically generated | S | R | Q |  |  |
| 0 | 0 | Q (no change) |  | No change |
| 0 | 1 | 0 | 1 |  |
| 1 | 0 | 1 | 0 |  |
| 1 | 1 | 0  1  (undefined) | 1  0  (undefined) | Invalid |

(e). 2-input S-R Latch with NAND gates circuit

(f). What is the purpose of circuit in the Problem 1.(e) above?

The purpose of a 2-input S-R latch with NAND gates is to store and maintain a binary state (0 OR 1) based on two control inputs: Set (S) and Reset (R). Here are the key functions it serves:

1. **Memory Storage:** It holds a single bit of information, effectively functioning as a memory element in digital circuits.
2. **State Control:** The Latch can be set to a high state (1) or reset to a low state (0) based on the input conditions, enabling simple control mechanisms in sequential logic.
3. **Stability:** It provides a stable output that can hold its value indefinitely until changed by the inputs, making it useful in applications requiring state retention, such as flip-flops and other memory devices.
4. **Event Triggering:** The latch can be used to trigger actions in circuits based on input changes, allowing for synchronized operations in more complex digital systems.

Overall, the 2-input S\_R latch with NAND gate is fundamental in building more complex memory structures and sequential logic circuits.

(16 Points)

2. IP Piracy and Hardware Trojan (HT):

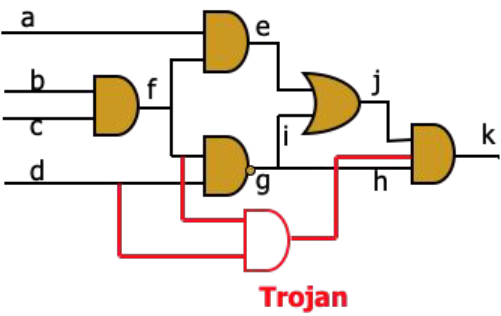
Please answer the followings:

(a). What is Intellectual Property (IP) Piracy in digital circuit design, and how can it be prevented?

Intellectual Property (IP) piracy in digital circuit design refers to the unauthorized use, replication, or distribution of proprietary designs, circuits, or technology that are legally protected by copyright, paten, or trade secret laws. In context of digital circuit design, this typically involves: unauthorized duplication, counterfeit components, and design theft.

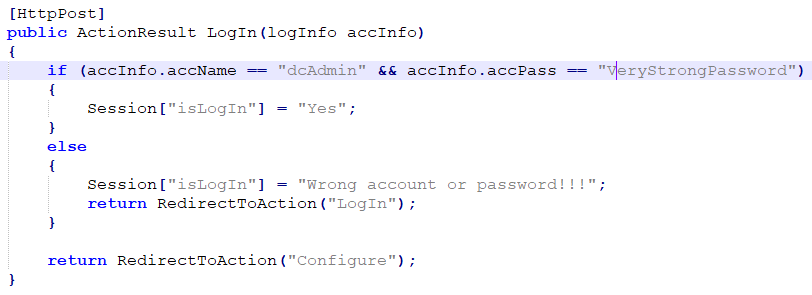
It can be prevented through various strategies, including legal protections like patents and copyrights, design encryption, watermarking, access control, and clear licensing agreements. Additionally, educating designers about the importance of IP rights and conducting regular audits can further safeguard against piracy, fostering a culture of respect for intellectual property.

(b). Find the triggers from HT inserted circuit as follow:



(c). In the back-end web application code (using ASP .net MVC) for login to the configuration below, insert a Trojan code, which redirects to the “HoneyPot” web page (when a password is “WinnieThePooh” without a case sensitive) instead of being back to “LogIn” web page or going to “Configure” web page.

You may need to make a condition for accept all the variations of “WinnieThePooh”, “winniethepooh”, “WINNIETHEPOOH”, and so on.



A computer screen shot of a program

Description automatically generated

(d). From Problem 2.(c) above, what is a trigger and payload for a web Trojan code?

A **trigger** is an event or condition that activates the Trojan code. In a web context, triggers can include:

* **User Input**: For example, entering a specific password or visiting a particular URL.
* **Time-based Events**: Executing at a specific time or after a certain period.
* **System Events**: Actions like system startup or when a specific application is launched.

The **payload** is the actual malicious action that the Trojan executes once triggered. This could involve:

* **Data Exfiltration**: Sending sensitive information (like passwords, personal data) to an attacker's server.
* **Redirecting Users**: For instance, sending users to a malicious website or a "HoneyPot" page.
* **Installing Additional Malware**: Downloading and executing further malicious software on the victim's system.
* **Creating Backdoors**: Allowing unauthorized remote access to the compromised system.

(18 Points)

3. Cybersecurity Job Interview Questions:

Please answer the followings:

(a). What is the Port Number, and what layers in the OSI model does it belong to?

A port number is a numerical label assigned to specific processes or services on a computer network. It helps to distinguish between different services running on the same device. Port numbers are part of the Transport Layer (layer 4) of the OSI model, where protocols like TCP (transmission control Protocol) and UDP (user datagram protocol) use them to identify specific applications.

(b). What are the default Port Numbers for HTTP and HTTPS?

The default port for HTTP is 80.

The default port number for HTTPS is 443.

(c). What are black hat, white hat, and grey hat hackers?

Black Hat Hackers: These individuals exploit vulnerabilities for malicious purposes, such as stealing data, damaging systems, or spreading malware. They operate outside the law.

White Hat Hackers: Also known as ethical hackers, they use their skills to improve security. They work with organizations to identify and fix vulnerabilities legally and ethically.

Grey Hat Hackers: these hackers fall somewhere between black and white hats. They may exploit vulnerabilities without malicious intent but without permission from the organization. They often inform the organization afterward, which may lead to legal or ethical dilemmas.

(d). What is the Honeypot in the Network and Cybersecurity?

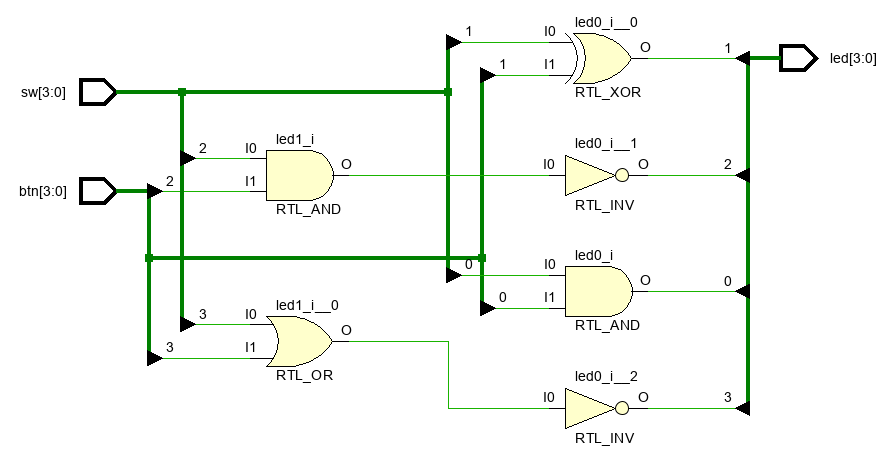
Honeypot is a security resource that is set up to attract, detect, and analyze unauthorized access or attacks on a network. It acts as a decoy, mimicking real systems to lure attackers. By monitoring interactions with the honeypot, security professionals can gather information about attack methods and motives, helping to improve security measure for real systems. Honeypots can be used for research, threat intelligence, and as a distraction for attackers.

(12 Points)

4. Chip Architecture:

Please answer the followings:

(a). Refer the netlist schematic below, complete the RTL Verilog code for AND, XOR, NAND, and NOR operations

  
<Netlist Schematic>

`timescale 1ns / 1ps  
  
module LGates2(  
 input [3:0] sw, // 4-bit input for switches  
 input [3:0] btn, // 4-bit input for buttons  
  
 output [3:0] led // 4-bit output for LEDS  
 );

//LED0 = sw[0] AND btn[0]  
 assign led[0] = sw[0] & btn[0];

//LED1 = sw[1] XOR btn[1]  
 assign led[1] = sw[1] ^ btn[1];

//LED2 = ~(sw[2] AND btn[2]) (NAND operation)  
 assign led[2] = ~(sw[2] & btn[2]);

//LED3 = ~(sw[3] OR btn[3]) (NOR operation)  
 assign led[3] = ~(sw[3] | btn[3]):

<Verilog source code>

(b). Refer the Verilog source code below, please draw the netlist schematic of the 4-bit calculator using Verilog code following?

<Verilog source code>

`timescale 1ns / 1ps  
  
module calculator(  
 input wire[3:0] x,  
 input wire[3:0] y,  
  
 output wire[4:0] add,  
 output wire[4:0] sub,  
 output wire[7:0] mul,  
 output wire[3:0] div  
);  
 assign add = x + y;  
 assign sub = x - y;  
 assign mul = x \* y;  
 assign div = x / y;  
  
endmodule

x[3:0] --->

4-bit

adder

4-bit divider

8-bit

multiplier

4-bit

subtractor

y[3:0] ---> ----------- ------------- --------------

Div[3:0]

Sub[4:0]

Add[4:0]

Mult[7:0}

(c). What is the final stage in the back-end of IC design and manufacturing, where the individual semiconductor chips (die) are encased in a protective housing?

The final stage in the back-end of IC design and manufacturing, where individual semiconductor chips (die) are encased in a protective housing, is known as **packaging**.

* **Purpose**: Packaging protects the die from physical damage and environmental factors, facilitates electrical connections, and aids in heat dissipation.
* **Types of Packages**: There are various packaging types, such as Dual In-Line Package (DIP), Surface-Mount Device (SMD), Ball Grid Array (BGA), and Chip-On-Board (COB).
* **Process**: The process typically involves attaching the die to a substrate, connecting it with wire bonds or flip-chip methods, and then encapsulating it with materials like epoxy or plastic.

This stage is crucial for ensuring the reliability and performance of the integrated circuit in its intended application.

(15 Points)

5. Simple Codes/Scripts:

Please answer the followings:

(a). When we’re using the web browser on the systems with a keylogger, what information can the keylogger get?

- Go to chase.com with typing “chase.com” on the address bar

- Click the Username line and type account name “tonystark”

- Enter the Password “ActorIsRobertDowneyJr.”

When using a web browser on a system with a keylogger, the keylogger can capture a variety of information based on the user's interactions. Here’s what a keylogger would typically log in the scenario you described:

1. **URL Typed in the Address Bar**:
   * The keylogger would record the URL chase.com when you type it in the address bar.
2. **Form Inputs**:
   * **Username**:
     + When you click the Username line and type tonystark, the keylogger would capture this input as well.
   * **Password**:
     + When you enter the password ActorIsRobertDowneyJr., this would also be captured by the keylogger.

* **URL**: chase.com
* **Username**: tonystark
* **Password**: ActorIsRobertDowneyJr.

(b). With the Python socket programming code below, what server and service port we can access?

# Import socket module

**import** socket

# Create a socket object

s **=** socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

# Define the port on which you want to connect

port **=** 2553

# connect to the server on local computer

s.connect(('216.249.138.55', port))

# receive data from the server and decoding to get the string.

print (s.recv(1024).decode())

# close the connection

s.close()

In the provided Python socket programming code, you are attempting to connect to a server at the IP address 216.249.138.55 on port 2553. Here’s a breakdown of the relevant components:

* **Server IP Address**: 216.249.138.55
* **Service Port**: 2553

Port 2553 does not have a well-known or standardized service associated with it like HTTP (port 80) or HTTPS (port 443). Instead, it is considered a user-defined port that may be used by specific applications or services.

Since port numbers above 1024 are often used for custom or proprietary applications, the specific service running on port 2553 would depend on the application developed for that server. To determine what service is running on that port, you could:

You can access a service on the server 216.249.138.55 using port 2553, but the specific nature of that service would require further investigation. If you're developing or debugging, ensure you have the correct service specifications or documentation for that port.

(c). Recall your homework #4, and add a client Python code to print the socket information, and connect to the server with TCP/IP port 8192. Please show the screen shot on connection.

A computer screen with text and images

Description automatically generated



(15 Points)

6. Cryptography:

Please answer the followings:

(a). In a configuration file of one Cisco switch, we can see some information below, find the user account and password from it

username tonystark password 7 0815444B3D0B10031A221F4A64650D293E1C301C093B020F

Building configuration...  
Current configuration : 3637 bytes  
! No configuration change since last restart  
!  
version 12.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname DC236SW001  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$wLbr$Sly9SiIsF7mgnyfl8LFi5.  
!  
username tonystark password 7 0815444B3D0B10031A221F4A64650D293E1C301C093B020F  
!  
no aaa new-model

--More--

(b). From Problem 6.(a) above, how can we secure the user account login instead of Cisco type 7 passcode?

* Ensure that passwords are complex, using a combination of uppercase letters, lowercase letters, numbers, and special characters.
* The enable secret command uses a stronger hashing algorithm (MD5 or SHA) compared to the older enable password command.
* Ensure that you use enabled secret to set the privilege mode password instead of enable password.

**enable secret <your\_secure\_password>**

* Enable AAA for centralized authentication and management:

**aaa new-model**

* Configure a RADIUS or TACACS+ server for user authentication:

**aaa authentication login default group radius local**

* Define local user accounts with strong passwords:

**username tonystark secret <strong\_password>**

* Use SSH for remote access instead of Telnet, which is insecure and sends data in plaintext

**line vty 0 4**

**transport input ssh**

* Make sure to generate RSA keys:

**crypto key generate rsa**

* Disable any unused services and ports to reduce potential attack surfaces:

**no service tcp-small-servers**

**no service udp-small-servers**

Implement ACLs to restrict access to the switch's management interfaces.

Keep your devices up to date with the latest firmware and security patches.

(c). What is the default login and password for pfSense Router?

The default login credentials for a pfSense router are:

* **Username**: admin
* **Password**: pfSense

**Important Notes:**

* It's highly recommended to change these default credentials immediately after the initial setup to enhance security.
* If you have changed the password and cannot remember it, you may need to reset the device to factory settings to regain access.

(d). Recall the Project #0: download the encrypted\_image\_jpg.enc file and decrypt it with a key (0xABC) to see what it is.

Blue screen of death

(e). From Problem 6.(d), show the first 256 bytes of each file (encrypted file/decrypted file) as a hexadecimal.

**A screenshot of a computer program

Description automatically generated**

(24 Points)

A computer screen shot of a computer code

Description automatically generated