Computer Network Software Operations (6651)

Teacher Resources

Instructional Scenarios

Designing a Secure and Functional Home Network

Duty Area: Using Desktop Systems Concepts

Scenario:
You have been retained to design a home network. (See the resource link below, Cyber.Org, for the complete lesson plan). You must map out a home network using the following:
- cable (ISP)
- modem
- router
- firewall
- repeater
- desktop computer
- all-in-one printer
- PlayStation (PS5)
- 3 cell phones
- a smart appliance
- one other device of your choice.

Big Question:
How can a home network function securely and seamlessly using wired and wireless devices?

Focused Questions:
- What is the difference between a wired and wireless device?
- What are the advantages and disadvantages of using wireless?
- What are the advantages and disadvantages of using wired?
- What is a repeater? Why is it important in a home network?
- What is a wireless access point (WAP)?

Project-Based Assessment:
Complete the design of your home network according to the resource guidelines provided and follow the scenario above.

Resources:
- https://cyber.org/
- https://cyber.instructure.com/courses/61

Capturing ARP and ICMP Packets

Duty Areas: Ensuring Network Security

Scenario:

This is a lab that allows students to work with Wireshark to capture address resolution protocol (ARP) and Internet control message protocol (ICMP) packets.

Time Required: 30 minutes

Instructions

1. If required, log on to your computer as **NetAdmin** and open a command prompt window.

2. Type **arp -d** and press **Enter** to clear your ARP cache.

3. Start Wireshark and click **Capture Options**.

4. In the Capture Filter text box, type **arp or icmp**, and then click **Start**.

5. At the command prompt, type **tracert books.tomsho.com** and press **Enter**.

6. When tracert is finished, click the **Stop the running live capture** toolbar icon in Wireshark to stop the capture.

7. Scroll to the first packet summary line, if necessary.

Find the ARP packets your computer has generated by looking in the Info column for "Who has *A.B.C.D*, Tell 192.168.100.*XX*" (replacing *A.B.C.D* with the address of your default gateway and *XX* with your student number). Click this packet summary line.

Notice that the Dst (for destination) address is ff:ff:ff:ff:ff:ff, indicating a broadcast. Next:

1. In the middle pane, click to expand the **Ethernet II** line. Notice that the Type field is ARP (0x806), which tells the Network access layer which Internetwork-layer protocol should receive the packet.

   a. Click again to collapse this line.

2. Click to expand the **Address Resolution Protocol (request)** line. Examine the information in the ARP header. The ARP message has fields to indicate what technology is used in the Network access layer (Ethernet) and the protocol type that needs the MAC address (IP, in this case).

   a. Click again to collapse this line.

3. In the top pane, click the ARP reply message immediately following the ARP request. The Info column should be similar to "*A.B.C.D* is at 0A:1B:2C:3D:4E:5F." The MAC address in the ARP reply is the MAC address of your default gateway.

   a. Explore the Network access and Internetwork headers for this frame.

b. (*Note*: You might also find an ARP request and ARP reply for your DNS server if it's in the same network as your computer.)

4 In the top pane, click the first **ICMP Echo (ping) request** message from your computer to the destination computer at *books.tomsho.com*. The IP address should be 67.210.126.125, but IP addresses can change, so it might be different.

5 In the middle pane, click to expand the **Internet Protocol** line.

a. Notice that the value in the "Time to live" line is 1.

6 In the top pane, click the **ICMP Time-to-live exceeded** message that follows the ping request. This message was generated by the first router en route to *books.tomsho.com*.

a. Notice that the source address is the address of your default gateway.

7 Find the next ICMP Echo (ping) request message and view the TTL value. Tracert sends three Echo (ping) request messages for each TTL value, so the first three messages have a TTL value of 1.

a. Find the fourth ICMP Echo (ping) request message and view the TTL value, which should be 2. The "Time-to-live exceeded" message following it is from the next router down the line. Tracert follows this pattern until reaching the destination device (*books.tomsho.com*).

8 Exit Wireshark but leave the command prompt window open if you're continuing to the next project.

Instructional scenario submitted by Jennifer Marden, Loudoun County High School, Loudoun County Public Schools, 2021.

Design Your Companies Authentication Backend

Duty/Concept Area(s): Using Desktop Systems Concepts

Scenario:

You are currently employed at WebWidgets Incorporated as a security consultant working on the redesign and development of their authentication systems. Your job is to design the backend authentication systems for a variety of outward-facing services that your company uses. You need to provide compelling arguments as to what type of authentication and authorization solutions can satisfy the security and usability needs.

WebWidgets Incorporated has the following services that their employees need to access when outside the company network:
- Webmail service
- Gitlab repositories
- Team management system
- Web admin panels

The team has already had an initial briefing where they discussed the possibility of hosting all services on their internal network or using software-as-a-service (SaaS) solutions. The CEO has expressed concerns over security, but also knows they cannot sacrifice major accessibility.

You need to explore popular methods for managing multiple services through a single-sign on (SSO) either provided by a service or housed locally. You will also have to consider the possible vulnerabilities that an SSO introduces and how those can be mitigated.

After weighing the possibilities and choosing a design, you will need to prepare a presentation for the CEO consisting of two options for your team.

Big Question:

How do modern-day systems manage network accounts for authentication and authorization through a variety of services?

Focused Questions:
- What is SSO?
- What is SaaS?
- What are common industry solutions for SSO (internal or provided) and SaaS?
- What types of threats should be considered when implementing SSO or SaaS?
- How can these threats be mitigated?

SOL Correlation:
C/T 9-12.2, C/T 9-12.3, C/T 9-12.4, C/T 9-12.5

Project-Based Assessment:

Student(s) will work to create a presentation to compare to possible designs for the company's new infrastructure.

Instructional scenario submitted by Karl Meister, Norview High School, Norfolk Public Schools, 2021.

Lockdown at International Hotel

Duty Area(s): Ensuring Network Security

Scenario:
Please refer to the resource link below for more information.
https://cyber.instructure.com/courses/6/pages/aics
Module 1: International Hotel Lockdown

Big Question:
How do agencies like the Department of Homeland Security investigate an incident using digital forensics and various media?

Focused Questions:
- Based on the evidence, how might you go about constructing a list of key names or groups that can be responsible for the incident?
- Based on the evidence gathered, what is the timeline of events?
- What type of information did you glean from the .txt file?
- Based on the evidence, were you able to identify connections between any of the key figures involved?

Project-Based Assessment:

Groups can be graded on the following:

- Opening Statements (clear, well organized, and relevant)
- Addressed Issues (coverage of topic)
- Supporting Facts (provided facts that support the topic)
- Persuasiveness (arguments are clear and convincing)
- Teamwork (all members contributed to briefing)
- Organization (addressed likely culprit and gave clear recommended response)
- Overall preparedness, effectiveness, and professionalism

Resources: Cyber.org/Cyber Society/AICS
https://cyber.instructure.com/courses/6/pages/aics

Instructional scenario submitted Jennifer Marden, Loudoun County High School, Loudoun County Public Schools, 2021; Kristi Rice, Spotsylvania High School, Spotsylvania County Public Schools, 2021, and Katrina Riggleman, Riverbend High School, Spotsylvania County Public Schools, 2012.

Cyber Security and Cyber Forensics Infusion Units

Cyber Security and Cyber Forensics Infusion Units (CYBR) were designed to be infused with designated CTE courses to help students in those programs achieve additional, focused, validated tasks/competencies in personal and professional cyber security skills. These units are not mandatory, and, as such, the tasks/competencies are marked as "optional," to be taught at the instructor's discretion.

Entrepreneurship Infusion Units

Entrepreneurship Infusion Units may be used to help students achieve additional, focused competencies and enhance the validated tasks/competencies related to identifying and starting a new business venture. Because the unit is a complement to certain designated courses and is not mandatory, all tasks/competencies are marked "optional."

Microsoft Imagine Academy Resources

Microsoft Imagine Academy (MSIA) offers classroom resources and materials and instructional techniques that will help enhance instruction and learning for this course. Using the school's membership ID and product key for the Microsoft Imagine Academy, all resources are available through the [MSIA Member Dashboard on the Microsoft site.](#)

- To access the curriculum resources, select the Classroom Tile from the member site.
- To access downloadable curriculum resources including the MOAC e-Book, Lesson Plans, and Study Guides select Curriculum Overview - Curriculum Downloads.
- To access Online Learning videos and tutorials select Online Learning Directory tile.
- For more information visit: [How to Get Started with Microsoft Imagine Academy Program.](#)