COMP 6801 Project

Question 1

Java Deserialization Bug

Backgroud

The vulnerability exists in the manner in which many Java apps handle a process known as object deserialization. A serialization is a technique that many programming languages use to transfer complex data structures over the network and between computers.

It's a process in which a Java object is essentially broken down into a series of bytes to make it easier to transport and then reassembled back into an object at the other end. The disassembling process from an object into a sequence of bits is called serialization, while the reassembly from the bits back to an object is called deserialization.

The problem lies in the fact that many apps that accept serialized objects do not validate or check untrusted input before deserializing it. This gives attackers an opening to insert a malicious object into a data stream and have it execute on the app server.

The WLS Security component in Oracle WebLogic Server 10.3.6.0, 12.1.2.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to execute arbitrary commands via a crafted serialized Java object in T3 protocol traffic to TCP port 7001, related to oracle_common/modules/com.bea.core.apache.commons.collections.jar.

Task

Write a paper on this vulnerability. Write a script that given a list of IPs determines whether or not the servers on the list of sites vulnerable to this bug.

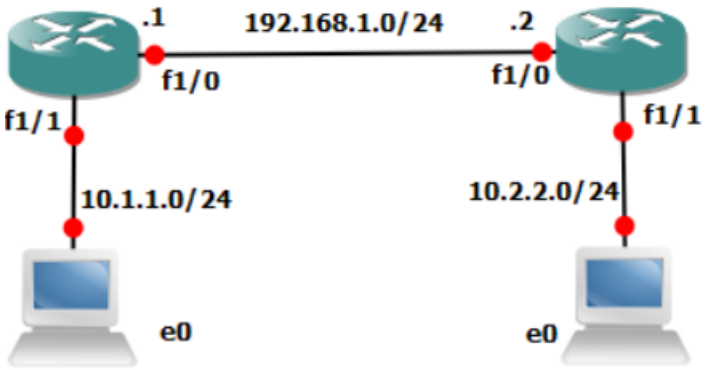
Question 2

The concept of ARP spoofing is explained in section 8.2.1. Construct an experiment involving two computers and a wired or wireless switch/router to illustrate how a man in the middle attack can be created.

SSL Stripping is briefly described in Section 7.2.2. Download the SSL Stripping Tool and investigate how it works. Your task is to construct an experiment to demonstrate how a SSL Stripping attack can be done.

Question 3

Using Tunnel mode IPSec your task is to configure the routers shown in the network diagram below. This involves reading Chapter 7 to get the theoretical understanding of IPSec and then researching how to configure Cisco routers for IPSec. You are required to use the routers in CS LAB 1 to test your configuration.



Question 4

You are required to design the necessary functions required to generate Elgamal private and public keys, to encrypt and decrypt messages using the Elgamal approach and to encrypt and decrypt messages using the DES block cipher (***From the Crypto.Cipher import the DES module***). After building the Elgamal module do the following tasks:

1. Generate a private key
2. Generate the corresponding public key.
3. Encrypt the private key using the DES algorithm. Use a secret password. Why is this necessary?
4. Save the encrypted private key to a file called privatekey.dat
5. Save the public key to a file called publickey.dat
6. Use the public key from step 2 to encrypt using the Elgamal approach, a 144 twister message to President Trump.
7. Email the encrypted letter to a COMP 6801 classmate.
8. In a separate email attached the encrypted private key file generated from step 4 to the same classmate as step 7.
9. In a separate email attached the DES key used to encrypt the private in step 3.
10. Your classmate (you – since you are in the class) should write a python program to use the encrypted letter and decrypted private (used the DES key from step 9) to decrypt the letter and print its contents to the screen.

Question 5 (can be done in place of question 1)

Academic researchers have found an exploitable hole in WPA, a popular form of wireless networking encryption. Write a paper on the recently exploited vulnerability in the WPA which uses a e 4-way handshake to generate a fresh session key. Download a hacking tool to demonstrate how the attack works.

Note: TurnItIn will be used for all papers