Introduction to CyberSecurity

Workshop 1 - 03/10/2022

Threats to cybersecurity

When it comes to cyber security there are many different vectors that an attacker could use, ranging from social engineering to many types of malware. This means that you have to consider each of these attack vectors in turn in order to protect your data or application. Some common examples of these are SQL injection, DDOS attacks and MITM attacks. There are also many defences that can be used to stop these attacks.

SQL Injections

SQL injections work by filling in text entry with malicious code, this code is then used in the original query and can allow the attacker to release more data than the creator intended. An attacker can use this to gain entry to a system by revealing usernames and passwords from a table; they could also just bypass the password altogether by using a statement that will return true.

These sorts of attacks can be prevented by preparing sql statements before execution so that they will not run malicious code.

SQL Injection demo

SQL injection demo

Explanation on Youtube

Password Cracking video

Malware

Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. It’s used for ransomware, spyware, as a trojan or it can even be polymorphic. This is part of what makes it so dangerous, that it can work in lots of ways to achieve different results.

When stopping malware it is best to keep software up to date so that it can best prevent unauthorised access. Making sure that antivirus software is installed and updated is also a good practise to use along with ensuring proper authentication is in order.

Ransomware

These pieces of code typically like to encrypt or hijack data, and demand money or other information in exchange for a decryption key.

One of the most notable pieces of ransomware was the WANNACRY virus, which infected thousands of devices within the NHS and demanded large sums of money after encrypting confidential patient files.

Spyware

Unlike ransomware, the main goal of spyware is to stay under the radar and observe, typically infecting devices by piggybacking off other safe programs to bypass anti-malware programs.

A common form of spyware is a keylogger, which once deployed, monitors every keystroke a user enters on their pc, allowing hackers to obtain passwords and information with relative ease.

Trojan

Much like the Trojan horse used to enter the city of Troy, trojan malware disguises itself as a harmless program that the user can use in order to trick the user into installing it or giving it permissions it shouldn’t have.

Some trojans may even work as actual programs that the user can utilize , but behind the scenes, it is opening doorways for a hacker to gain access to your pc.

Polymorphic

Perhaps the most renowned form of malware is a polymorphic virus. This piece of code self replicates at impeccable speed, constantly changing its code to remain undetectable by antivirus software, it can infect hundreds of files with relative ease, and once it infects a system, it is very hard to completely wipe out.

Cryptography

The earliest form of cryptography was created using the Caesar cypher, this allowed Julius Caesar to send messages to his generals without them being read by messengers or spies along the way. The basic concept is taking each letter in a message and encrypting it by shifting it by an amount that only the receiver knows so that they can decrypt the message

Cryptography

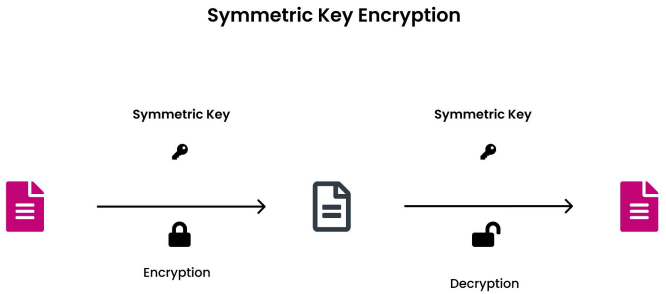
Enigma is a very famous example of a cipher that was used by the Germans during WWII. One person would enter text into keys on the cipher device and then write down the letters that would light up upon pressing each key. This encoded message could then be safely sent along the airwaves to a receiver who could decrypt it with the same device. Each day the settings for the device would be changed and this would mean changing the rotor positions that the device relied upon as well as the plug board positions being changed.

Cryptography

Modern cryptography relies upon the use of keys, in two methods. These are called symmetric and asymmetric encryption, with the former involving the use of secret keys and the latter using private and public keys.

Secret keys rely upon both parties involved having the same or mathematical related but slightly different key which will allow them to send and receive messages from each other. These can be implemented using block ciphers, which work by encrypting a whole block of text at a time using the secret key. They can also be implemented using stream ciphers which work by encrypting the text with a stream of key material, generated using the secret key to create the internal state.

Asymmetric encryption relies on the creation of a public key and a private key that are mathematically related to each other. The public key is then used for the encryption of messages, and the private for the decryption of them.



Social Engineering

Social Engineering covers any kind of cyber attack involving the social element, as the name implies. What does this mean though? It encompasses things like phishing, where an attacker is trying to convince a target that they need to hand over their data or money. This is one of the most dangerous kinds of attacks because they are so easy to set up and run while having a potentially very high reward.

Relevant Laws

The main laws that surround cybersecurity are the Computer Misuse Act (1990) and the Data Protection Act (2018), however other laws can come into play depending on the offence. For most cases of hacking this is illegal under the computer misuse act as it is an offence to perform any function with the intent to secure unauthorised access to any program or data held in a computer or enable such access.

- Network and Information Systems Regulations 2018 (NIS Regulations)
- Investigatory Powers Act 2016
- Copyright Designs and Patents Act 1988
- Fraud Act 2006(Phishing)

Kali Linux

To save time in future workshops, and to provide you with a suitable toolkit, we recommend installing a kali linux VM. Kali linux is a debian distribution designed for penetration testing. If you don't have a VM framework, we recommend either VMware or Virtualbox, this will be the program you use to launch the Virtual Machine. After you have your VM software installed

1. Head to https://www.kali.org/get-kali/ and select Virtual Machines
2. Select your VM software and press the download button
3. Once this download is complete, extract the file
4. Launch your VM software and press Add, then select the Machine image we just extracted
5. Adjust the settings to suit your system
6. Once installed, boot up the VM
7. Login to Kali using the Username & Password: kali / kali

Unlike Most VMs Kali is a very specialised tool, for this reason we recommend that you don't use tools that you are not familiar with, as many of them can be unsafe if used incorrectly. If you want to learn more about kali and it's tools feel free to message the society discord and we'll try to get back to you!

Suggestions for Future Workshops

Workshop Suggestions