CS808: Computer Security Fundamentals

6.7 Article: Tarpits, Honeytraps and Sources of Current Security Vulnerabilities

Tarpits

In attempting to minimise the impact of successful attacks we have the option of deploying tarpits. Tarpits are a security mechanism which purposefully delays network connections to a server. This can be helpful in situations related to malware such as worms and DoS attacks. With worms, it can help slow the spread of infection as it will get longer and longer wait times to send the packets to the new potential host. With DoS if it is a http request flood, then each request will take longer and longer to respond to. This would have no impact for the genuine user, but could slow down the DoS.

Honeypots

In attempting to gather information on an attacker, we can make use of honeypots. These are apparently legitimate computers which are set up to be enticing to attackers, but have no valuable information on them. The attackers then attempt to attack the honeypot and in the process information about the attacker can be gathered. For example the honeypot could be server which appears to hold a database of customer details.

Keeping up to date with known vulnerabilities and attacks

There are a range of databases which contain known vulnerabilities and attacks. Below are some of the most popular databases. Take some time to explore these if you have not already make use of them in your work.

The Common Vulnerabilities Exposures database contains numbered known cyber security vulnerabilities. The website can be located here https://cve.mitre.org/

In particular, the Twitter feed can be useful for seeing regular updates on cyber vulnerabilities, from both the CVE and elsewhere. The CVE twitter account can be found here: https://twitter.com/CVEnew

The National Vulnerability Database (NVD) is a US government source of vulnerability data. https://nvd.nist.gov/

Malware Attribute Enumeration and Characterization is a structured language to share data on malware https://maecproject.github.io/

The Common Weakness Enumeration is community driven database of common software and hardware vulnerabilities.

https://cwe.mitre.org/

Open Web Application Security Project (OWASP) is an excellent resource for a range of security topics, and most notably provides the OWASP top 10 web application vulnerabilities. You can access OWASP here https://owasp.org/