# Common exploits found in the exploitation phase and countermeasures

1.) Buffer Overflows

A buffer overflows when there are more characters being placed into the buffer then what the buffer what written for.

Countermeasures

* Error checking programs and making sure the buffers Reid e the type and amount of information required.
* Stop accepting data when buffer is filled by adding boundary protection.
* Write secure code because most buffer overflows occur because of code that has been poorly written.
* Keeping systems and applications patched.

2.) Phishing with pretexting

Phishing with protecting is a type of social engineering attack that is commonly used today. is the art of presenting oneself as someone else to obtain private information. This can be done by creating a faker persona or impersonation a staff member.

Countermeasures

* Enforce polices that deal with service calls software updates and gifts from outside companies
* Manually test to see if company is prepared
* Empower employees to recognize potential threats and independently make correct security decisions.
* Limit employees' information access to only that information that they have a need to have access to.
* Use dual factor authentication along with strong passwords that are regularly changed
* Provider user training awareness for employees and management
* Limit use of BYOD

3.) Man-in-the-middle Attacks

A man-in-the-middle attack is an attack where the attacker intercepts communications between two parties to eavesdrop or impersonate.

Countermeasures

* check the security certificate of a website. Make sure the beginning of the URL says HTTPs instead of HTTP. This lets a user know that the site is secure. Most man in the middle attacks use fake websites to gain access to users’ data.
* Don’t connect to public WIFI router directly. Use a Virtual Private network instead.
* Install an Anti-Virus program.
* Set up an Intrusion detection system.
* Spend time educating oneself on phishing and the different types that are commonly used in man in the middle attacks.
* Encrypting Passwords and usernames

.

4.) SQL Injection

SQL injection is a database exploit that injects poison into SQL statements. A SQL injection can also give someone control over the database.

Countermeasures

* Use of Prepared Statements to ensure that an attacker is not able to Chang the SQL query.
* Use of Stored Procedures
* Whitelist Input Validation: Validate input against whitelist. A whitelist is a list of possible correct inputs.
* Enforcing Least Privilege by minimizing the privileges to every database account in network.

5.) VLANs hopping

VLAN hopping works by sending packets to a port which should not be accessible.

There are two types of VLN hopping:

* Switch Spoofing: A hacker tries to spoof itself as switch to configure a system.
* Double Tagging: a hacker gains access to a VLAN by tagging transmitter frames.

Countermeasures:

* Disable Dynamic trunk protocol on truck ports
* Configure all the ports that should connect to end stations as access, assign them to an unused VLAN and shut them down
* Secure the switch physically (who can gain physical access to the switches, room temperature, UPS, etc.)
* Disable all the unused services on the switch (the TCP and UDP small servers, service config, HTTP server, etc.).
* Use of a Private VLAN when appropriate
* Use MD5 authentication if a VTP is used.