Collaborative Development: Security Tools used in mainstream business.

When Security is involved, there are a tremendous amount of effort put into not only making sure something is secure but also to maintain the security over whatever it is you have been you’ve been employed to protect therefor you have to constantly be evolving and adapting your methods in order to keep up with the people also adapting there methods in order to access data through illegal methods.

There are many different tools with a large variety of uses some on the features they have are as follows Anti-virus software, web vulnerability, penetration testing, packet sniffers, network intrusion detection and these are just a few however all these tools can do just one or sometimes multiple things from this list and a more wide range tool that can have multiple different below is going to be a short explanation of each category of Security tool.

**Anti-virus software** this tool is one of the most commonly found pieces of security software however can be one of the most effective the whole job of this software is to find viruses and remove them it will work in real time and detect and delete viruses however they can also prevent the virus from ever being installed in the first place as well and can do many other things like black or white listing specific programs and also blocking specific websites and IP’s.

**Positives for anti-virus software**

* Easy to use and simple (ease of access)
* Fast can be used whenever needed also is automated so scans will be fast with instant results.
* Free/cheap as with the simplicity and automation there is no need for a trained staff member therefor this process is cheap and most of the time the software is free.

**Negatives for anti-virus software**

* Performance issues can be a common problem as this application scans the computer it can often use hog a lot of the disc usage which will slow down the computer’s performance.
* Lack of guidance and true understanding as its an automated application it will look for common naming variable and other things like that which will not work against bespoke viruses intentionally designed to get passed these types of anti-virus software’s.

**Web-vulnerability software** this is also one of the more basic tools that are pretty much automated as far finding vulnerabilities as they run common search parameters that usually make a website unsafe this can be great because it allows instant results as well as it being able to be used without too much knowledge on web security some example of these common issues are cross-site scripting, SQL Injection and cross-site request forgery.

**Positives for Web-vulnerability software**

* Automated scans save time and money.
* Needed to meet the date protection requirements for a company to ensure the safety of the date that you are storing so to receive date you must prove that you can keep it safe.
* Most hackers aren’t cyber geniuses and are usually just executing attacks from the same type of software like this they are using tools like this yourself on your own company can identify weakness before an attack was ever launched.

**Negatives for Web-vulnerability software**

* You will not be safe from bespoke attacks that use new or non-conventional hacking methods.
* With automatic tools false flags are quite common so you will have to investigate each flagged attack or vulnerability by a trained security technician to confirm the vulnerability and fix it.

**Penetration Testing** is used when attempting to test a website for any vulnerability in which someone could exploit to gain access to their data this tool will be used to target a website or a system and then proceed to scan it to attempt to find weaknesses including open services, application security issues also it can find open-source vulnerabilities.

**Positives for pen testing**

* Putting yourself in the hacker’s shoes can give you a different perspective on your system or website and can allow you to see things that maybe you missed before.
* More personal tests provide better results as they apply directly to the problems that you could have which can also be better at finding fixes for vulnerabilities that would not be found by an automated system.
* Finding and exploiting issues in a controlled environment that will not then be used against the company is great as it allows the tester to attack a problem without having to confine them selves to the rules however there will be no draw back to this as the information gathered will not be used maliciously.

**Positives for pen testing**

* Expensive when doing this type of testing proper preparation and resources need to be taken to get the best results this can only be done by trained professionals and therefor will cost a decent amount if you want it done correctly.
* Using the techniques that these cybercriminals use to locate the issues that they would find before they find them raises ethical questions amongst the board on whether it’s acceptable or not.

**Packet-sniffer software** also which is also referred to as a packet analyser which can be both hardware and software and is used for monitoring network traffic a packet sniffer will examine streams of data packets that go from the computer to the network to gather information.

**Positives for packet sniffing software.**

* This can be used by security and software administrators to maintain a watchful eye over the network to keep it secure.
* Relatively simple software to use.

**Negatives for packet sniffing software.**

* However simple the software is to use it needs to be constantly monitored by personal and logs need to be created of anything suspicious which most likely would require a trained security analyst so it could be a costly endeavour.

**Network intrusion detection software** is used to monitor a network and waits to flag potentially malicious behaviour that will then create a flag which will be investigated further by whoever set up or maintains this software this information is normally stored using an event management system.

**Positives for network intrusion detection software.**

* This can be used to not only detect an attack, but it can also quantify it there for an appropriate response can be calculated to correctly address and fix the threat without having gone over the top which allows for efficient and cost-effective fixes to be deployed.
* Another positive would be they can be tuned to specific content which allows the user customisability which can help when looking out for specific attacks.

**Negatives for network intrusion detection software.**

* This software only detects attacks and can not prevent them from happening.
* This method also cannot process encrypted packets, so it has its own set of limitations.
* False positives are common when using this type of software and will need trained security technicians to evaluate and customise the software to reduces this issue however that can cost more time and money.