Comp 5370  
HW-Z  
John Carroll  
jcc0044/902521946

**1.If you are given all the resources to setup a home network. Explain the steps you would take to secure the home network. Intrusion detection? How about bot detection (is a computer in my home network a bot?)?**

Answer:

Two things are vital to keeping your network safe: proper settings and prudence. The first step is easy; you just need to adjust the settings on your router once. The second step, however, takes more effort. Whenever you're online, you'll need to be prudent about your activities.

Mitigating vulnerabilities using host and network based firewalls, virus

scanners, host based intrusion detection (IDS), as well as a sound

patching policy.

There is behavioural detection and Centralized Detection which uses a network sniffer or firewall logging.

**2.Recapitulate the principles of classical and modern crypto; differences between symmetric and asymmetric. Why people do people use both?**

Answer:

Classical: Processes, methods, algorithms and keys are secret; security through obscurity assumptions.

Modern: Methods and algorithms are known (specified, published, studied: cryptanalysis studies and reports); keys kept secret (used as “secret” parameters of algorithms)

Public key algorithms (asymmetric), unlike symmetric key algorithms, do not require a secure channel for the initial exchange of one (or more) secret keys between the parties.

Because of the computational complexity of asymmetric encryption, it is typically only used for short messages, typically the transfer of a symmetric encryption key. This symmetric key is then used to encrypt the rest of the potentially long & heavy conversation. The symmetric encryption/decryption is based on simpler algorithms and is much faster.

**3.What is XSS? Why does it matter? How to prevent?**

Answer:

A cross-site scripting attack occurs when a web application executes a script that the attacker supplied to end users. This flaw can be found anywhere in an application where user input has been taken but not properly encoded. If the input is not properly encoded and sanitized, this injected malicious script will be sent to users. And a browser has no way to know that it should not trust a script. When the browser executes the script, a malicious action is performed on the client side. Most of the times, XSS is used to steal cookies and steal session tokens of a valid user to perform session hijacking.

To prevent cross-site scripting, browsers also have their own filters, but security researchers always find ways to bypass those filters. This vulnerability is generally used to perform cookie stealing, malware spreading, session hijacking, and malicious redirection. In this attack, the attacker injects malicious JavaScript code into the website so that the browser executes the script and performs action as commanded by the attacker in the script. The vulnerability is easy to find but hard to patch. This is why it can be found in any website if you try.

There are also several open source libraries for preventing a XSS attack.

“Cross-site scripting, the nightmare of Javascript. Because Javascript can run pages locally on the client system as opposed to running everything on the server side, this can cause headaches for a programmer if variables can be changed directly on the client’s webpage. There are a number of ways to protect against this, the easiest of which is input validation.”

**4.What are usual ways to authenticate a person into a system.**

Answer:

Something they know (password), something they have (token), and something they are (biometrics). Two-factor authentication often times uses a password and token setup, although in some cases this can be a PIN and thumbprint.

**5.What are the measures you would take for securing on the fly data and resting data?**

Answer:

When data is protected while it is just sitting there in its database or on its hard drive- it can be considered at rest. On the other hand, while it is going from server to client it is in-transit. Many servers do one or the other- protected SQL databases, VPN connections, etc, however there are not many that do both primarily because of the extra drain on resources. It is still a good practice to do both however, even if it does take a bit longer.

**6.Explain how a network intrusion detection system works.**

Answer: the first is a Host Intrusion Detection System whereas the second is a Network Intrusion Detection System. An HIDS runs as a background utility in the same as an anti-virus program for instance, while a Network Intrusion Detection System sniffs packets as they go across the network looking for things that aren’t quite ordinary. Both systems have two basic variants: signature based and anomaly based. Signature based is very much like an anti-virus system, looking for known values of known ‘bad things’, while anomaly looks more for network traffic that doesn’t fit the usual pattern of the network. This requires a bit more time to get a good baseline, but in the long term can be better on the uptake for custom attacks.

**7.Explain the differences between authorization and authentication. Given a brief explanation each of LDAP, DNS, Kerberos and Active Directory.**

Answer:

Authentication is the process of ascertaining that somebody really is who he claims to be.

Authorization refers to rules that determine who is allowed to do what. E.g. Adam may be authorized to create and delete databases, while Ben is only authorized to read.

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network.

Kerberos /ˈkərbərəs/ is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services.

**8. Read up and study “TOR,” the “deep web,” and document its major features, threats, its evolution, and key implications for security (150-200 words, references, definitions, etc). How is the deep web different from an IntraNet in a company. What if a series of companies shared a private web site... how would it be like and unlike the deep web (besides the criminality issue).**

Answer:

Tor is free software for enabling anonymous communication. The name is an acronym derived from the original software project name The Onion Router. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than six thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms". Tor's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

The Deep Web, Deep Net, Invisible Web, or Hidden Web are search terms referring to the content on the World Wide Web that is not indexed by standard search engines. Computer scientist Mike Bergman is credited with coining the term in 2000. The Deep Web, Deep Net, Invisible Web, or Hidden Web are search terms referring to the content on the World Wide Web that is not indexed by standard search engines. Computer scientist Mike Bergman is credited with coining the term in 2000.

If it can be accessed remotely providing we login with the correct username and password, then a company’s Intranet forms part of the Deep Web.

If a series of companies shared a private web site it be like the deep web in the same regards to my last answer because it can be accessed remotely from the other companies’ network access. However, it would be unlike the deep web because it is private and not truly accessible from outside the series of companies.