Security

What port does ping work over?

It doesn't work over a port. A ping test uses ICMP, so there are no real ports being used. ICMP is a layer 3 protocol. ICMP basically roofs, or sits on top of, the IP address. Therefore it is not a layer four protocol either.

How would you implement two-factor authentication for a public-facing website?
Using the GoogleAuth library

How would you harden user authentication?

Generate Memorable Secure Passwords/Password Generators

Use password vaults

Use good antivirus softwares

What is the difference between threat, vulnerability, and a risk?

A threat is from an attacker that will use a vulnerability that was not mitigated because someone forgot to identify it as a risk. Vulnerability (weakness) is a gap in the protection efforts of a system, a threat is an attacker who exploits that weakness. Risk is the measure of potential loss when that the vulnerability is exploited by the threat.

What is the difference between a vulnerability and an exploit?

One is a potential problem while the other is an active problem. Think of it like this: You have a shed with a broken lock where it won't latch properly. In some areas such as major cities, that would be a major problem that needs to be resolved immediately, while in others like rural areas its more of a nuisance that can be fixed when you get around to it. In both scenarios it would be a vulnerability, while the major cities shed would be an example of an exploit – there are people in the area, actively exploiting a known problem.

SSH (TCP port 22) is a secure connection used on many different systems and dedicated appliances. Routers, Switches, SFTP servers and insecure programs being tunnelled through this port all can be used to help harden a connection against eavesdropping. Despite the fact that most times when you hear about somebody 'SSHing' into a box it involves Linux, the SSH protocol itself is actually implemented on a wide variety of systems – though not by default on most Windows systems. Programs like PuTTY, Filezilla and others have Windows ports available, which allow Windows users the same ease-of-use connectivity to these devices as do Linux users.

How do traceroutes work?

TTL stands for Time To Live. When a TCP packet is sent, its TTL is set, which is the number of routers (hops) it can pass through before the packet is discarded. As the packet passes through a router the TTL is decremented until, when the TTL reaches zero, the packet is destroyed and an ICMP "time exceeded" message is returned. The return message's TTL is set by the terminating router when it creates the packet and decremented normally.

Trace Route works by setting the TTL for a packet to 1, sending it towards the requested destination host, and listening for the reply. When the initiating machine receives a "time exceeded" response, it examines the packet to determine where the packet came from – this identifies the machine one hop away. Then the tracing machine generates a new

ICMP “time exceeded” message to that of the message being killed. So if the TTL is 0, the packet will be killed by the next machine to which it is passed. This can have two effects on a trace. If the computer is an intermediate machine in the trace, the entry will remain blank. No information is returned to the machine conducting the trace because the “time exceeded” message never makes it back. If the machine you are doing a trace to has this bug in its TCP stack, return packets won’t reach the originating machine unless the TTL is high enough to cover the round trip. So Trace Route will show a number of failed connections equal to n (the number of hops to the destination machine) minus 1.

How does SSL Handshake work?

Client: “Hello there. I want to establish secure communication between the two of us. Here are my cipher suits and compatible SSL/TLS version.”

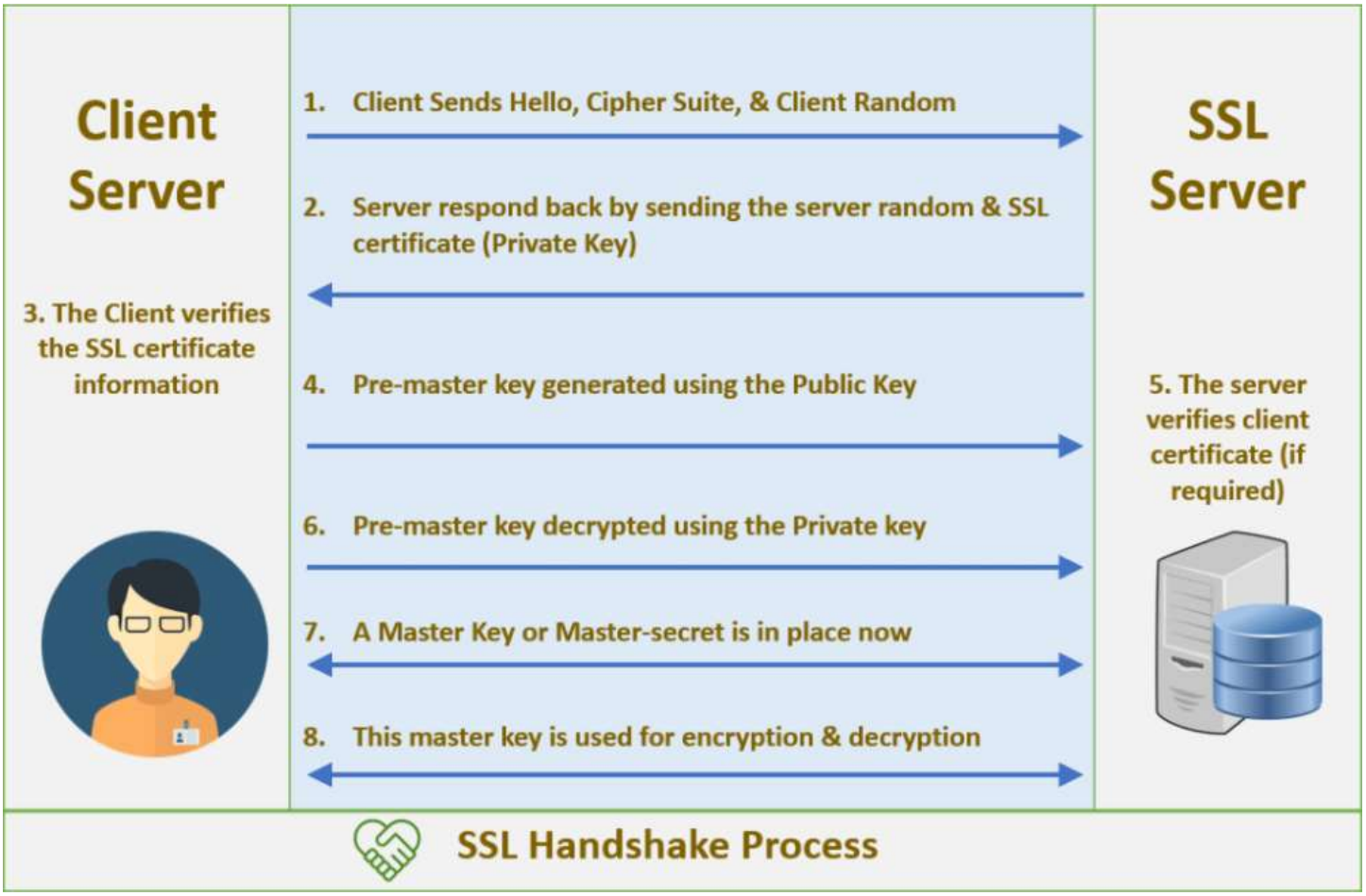
Server: “Hello Client. I have checked your cipher suits and SSL/TLS version. I think we’re good to go ahead. Here are my certificate file and my public key. Check ‘em out.”

Client: “Let me verify your certificate. (After a while) Okay, it seems fine, but I need to verify your private key. What I’ll do is, I will generate and encrypt a pre-master (shared secret key) key using your public key. Decrypt it using your private key and we’ll use thing master key to encrypt and decrypt the information”

Server: “Done.”

Client: "I'm sending you this sample message to verify that our master-key works. Send me the decrypted version of this message. If it works, our data is in safe hands."

Server: "Yeah, it works. I think we've accomplished what we were looking for."



What is OAuth?

parlance, this is known as secure, third-party, user-agent, delegated authorization.

– Created and strongly supported from the start by Twitter, Google and other companies, OAuth was released as an open standard in 2010 as RFC 5849, and quickly became widely adopted.

– The simplest example of OAuth is when you go to log onto a website and it offers one or more opportunities to log on using another website's/service's logon. You then click on the button linked to the other website, the other website authenticates you, and the website you were originally connecting to logs you on itself afterward using permission gained from the second website.

How OAuth works

– Let's assume a user has already signed into one website or service (OAuth only works using HTTPS). The user then initiates a feature/transaction that needs to access another unrelated site or service. The following happens (greatly simplified):

1] The first website connects to the second website on behalf of the user, using OAuth, providing the user's verified identity.
2] The second site generates a one-time token and a one-time secret unique to the transaction and parties involved.
3] The first site gives this token and secret to the initiating user's client software.
4] The client's software presents the request token and secret to their authorization provider (which may or may not be the second site).

6] The user approves (or their software silently approves) a particular transaction type at the first website.
7] The user is given an approved access token (notice it's no longer a request token).
8] The user gives the approved access token to the first website.
9] The first website gives the access token to the second website as proof of authentication on behalf of the user.
10] The second website lets the first website access their site on behalf of the user.
11] The user sees a successfully completed transaction occurring.

OAuth is not the first authentication/authorization system to work this way on behalf of the end-user. In fact, many authentication systems, notably Kerberos, work similarly. What is special about OAuth is its ability to work across the web and its wide adoption. It succeeded with adoption rates where previous attempts failed (for various reasons). Although not as simple as it could be, web coders seem to readily understand the involved transactions. Making a website OAuth-compatible can be done in a few hours to a day (much faster if you've done it before).

How would traceroute help you find out where a breakdown in communication is?

Tracert/traceroute, depending on the operating system, allows you to see exactly what routers you touch as you move along the chain of connections to your final destination. However, if you end up with a problem where you can't connect or can't ping your final

What protocol does traceroute use?

The type of packet that is sent differs depending on the implementation. By default Windows tracert uses ICMP and both Mac OS X and Linux traceroute use UDP. All versions of traceroute rely on ICMP type 11 (Time exceeded) responses from each hop along the route. If ICMP type 11 responses are being blocked by your firewall, traceroute will not work. These packets are inbound, not outbound.

How exactly does traceroute/tracert work at the protocol level?

In case you can't ping the final destination, tracert will help to identify where the connection stops or gets broken, whether it is firewall, ISP, router etc. The key point people usually miss is that each packet that's sent out doesn't go to a different place. Many people think that it first sends a packet to the first hop, gets a time. Then it sends a packet to the second hop, gets a time, and keeps going until it gets done. That's incorrect. It actually keeps sending packets to the final destination; the only change is the TTL that's used. The extra credit is the fact that Windows uses ICMP by default while Linux uses UDP.

exceeded" message is returned. The return message's TTL is set by the terminating router when it creates the packet, and decremented normally.

Describe a Unix traceroute hitting google.com at all seven layers of the OSI model.

The top 3-4 levels of the OSI model are not used (depending on the the operating system) traceroute makes a request to the networking library to send either an ICMP (layer 3) or UDP (layer 4) packet to the destination with a TTL of 1, the response that is returned includes information presented to the user and the TTL is increased to 2 for the next packet and sent. This proceeds until the destination is reached. The packets themselves are constructed at the bit level for level 1, and broken down to individual frames in level 2. This frame is packed in a 'packet' in layer 3. Then the remaining transformations depend on whether UDP is used or ICMP.

If I'm on my laptop, here inside my company, and I have just plugged in my network cable. How many packets must leave my NIC in order to complete a traceroute to twitter.com?

What is your opinion on hacktivist groups such as Anonymous?

Like any major group without a central leader, they seem to be mostly chaotic, at times seeming like a force for good, while at others causing havoc for innocents.

What's the difference between Symmetric and Asymmetric encryption?

To boil down an extremely complicated topic into a few short words, Symmetric encryption uses the same key to encrypt and decrypt, while Asymmetric uses different keys for encryption and decryption. Symmetric is usually much faster, but is difficult to implement most times due to the fact that you would have to transfer the key over an unencrypted channel. Hence, a hybrid approach should be preferred. Setting up a channel using asymmetric encryption and then sending the data using symmetric process.

What is an IPS and how does it differs from IDS?

Another difference is the positioning of the devices in the network. Although they work on the same basic concept but the placement is different.

How would you compromise an "Office Workstation" at a hotel?

Considering how infected these typically are, I wouldn't touch one with a 10ft pole. That being said, a USB keylogger is easy to fit into the back of these systems without much notice while an autorun program would be able to run quickly and quietly leaving behind software to do the dirty work. In essence, it's open season on exploits in this type of environment.

What is worse in Firewall Detection, a false negative or a false positive? And why?

When the device generated an alert for an intrusion which has actually not happened: this is false positive and if the device has not generated any alert and the intrusion has actually happened, this is the case of a false negative. A false positive is annoying, but easily dealt with – calling a legitimate piece of traffic bad. A false negative however is a piece of malicious traffic being let through without incident – definitely bad.

In penetration testing scenarios, a red team is trying to break in while a blue team is defending. Red Teams typically are considered the 'cooler' of the two, while the Blue Team is usually the more difficult. The usual rules apply like in any defense game: the Blue Team has to be good every time, while the Red Team only has to be good once. That's not entirely accurate given the complexities at work in most scenarios, but it's close enough to explain the idea. Being on the red team seems fun but being in the blue team is difficult as you need to understand the attacks and methodologies the red team may follow.

What's the difference between a White Box test and a Black Box test?

Information given by the person commissioning the test. A White Box test is one where the pen testing team is given as much information as possible regarding the environment, while a Black Box test is…well…a Black Box. They don't know what's inside.

What is the difference between Information Protection and Information Assurance?

configurations, backups, non-repudiation techniques, etc.

How would you lock down a mobile device?

The baseline for these though would be three key elements: An anti-malware application, a remote wipe utility, and full-disk encryption. Almost all modern mobile devices regardless of manufacturer have anti-malware and remote wipe available for them, and very few systems now do not come with full-disk encryption available as an option directly within the OS.

What's the difference between encoding, encryption, and hashing?

Encoding is designed to protect the integrity of data as it crosses networks and systems, i.e. to keep its original message upon arriving, and it isn't primarily a security function. It is easily reversible because the system for encoding is almost necessarily and by definition in wide use.

Encryption is designed purely for confidentiality and is reversible only if you have the appropriate key/keys.

ensures integrity.

What is SSL and why is it not enough when it comes to encryption?

SSL is identity verification, not hard data encryption. It is designed to be able to prove that the person you are talking to on the other end is who they say they are. SSL and its big brother TLS are both used almost everyone online, but the problem is because of this it is a huge target and is mainly attacked via its implementation (The Heartbleed bug for example) and its known methodology. As a result, SSL can be stripped in certain circumstances, so additional protections for data-in-transit and data-at-rest are very good ideas.

How would you find out what a POST code means?

POST is one of the best tools available when a system will not boot. Normally through the use of either display LEDs in more modern systems, or traditionally through audio tones, these specific codes can tell you what the system doesn't like about its current setup. Because of how rare these events can be, unless you are on a tech bench day in and day out, reference materials such as the Motherboard manual and your search engine of choice

How do you protect your home Wireless Access Point?

Using WPA2, stop broadcasting the SSID, and using MAC address filtering

What could you do to prevent a man-in-the-middle attack?

Secure/Multipurpose Internet Mail Extensions: Encrypts the email in transit

Use HTTPS

Use VPMS/Proxy

What is the difference between a Black Hat, Grey hat hacker and a White Hat?

Black hat hackers are those who hack without authority.

White hat hackers are authorized to perform a hacking attempt under signed NDA.

Grey hat hackers are white hat hackers which sometimes perform unauthorized activities.

You need to reset a password-protected BIOS configuration. What do you do?

While BIOS itself has been superseded by UEFI, most systems still follow the same configuration for how they keep the settings in storage. Since BIOS itself is a pre-boot system, it has its own storage mechanism for its settings and preferences. In the classic scenario, simply popping out the CMOS battery will be enough to have the memory storing these settings lose its power supply, and as a result it will lose its settings. Other times, you need to use a jumper or a physical switch on the motherboard. Still other times you need to actually remove the memory itself from the device and reprogram it in order to wipe it out. The simplest way by far however is this: if the BIOS has come from the factory with a default password enabled, try ‘password’.

What is XSS/Cross-site scripting, how will you mitigate it?

side, this can cause headaches for a programmer if variables can be changed directly on the client's webpage. Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts (also commonly referred to as a malicious payload) into a legitimate website or web application

The easiest way to explain this is a case when a user enters a script in the client side input fields and that input gets processed without getting validated. This leads to untrusted data getting saved and executed on the client side. Countermeasures of XSS are input validation, implementing a CSP (Content security policy) etc.

XSS vs SQL Injection?

– Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same origin policy.
– SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

How would you login to Active Directory from a Linux or Mac box?

accessed from a Linux or Mac system by using the Samba program. Depending on the version, this can allow for share access, printing, and even Active Directory membership.

What are SMB Protocol?

In computer networking, Server Message Block (SMB), one version of which was also known as Common Internet File System (CIFS) operates as an application-layer network protocol mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network. It also provides an authenticated inter-process communication mechanism. Most usage of SMB involves computers running Microsoft Windows, where it was known as “Microsoft Windows Network” before the introduction of Active Directory. Corresponding Windows services are LAN Manager Server (for the server component) and LAN Manager Workstation (for the client component)

I run an SMB. I have 4 people in my entire company and a web-based store. I don’t have the time, patience or manpower to have a computer guy. Why should I care about exploits and computer jibberish?

security consultant. An SMB will acknowledge what they need to do to keep their store secure and keep receiving payments since following the money will tend to help move things along.

What are Open Systems Interconnection Layers?

Layer 7: The application layer. ...
Layer 6: The presentation layer. ...
Layer 5: The session layer. ...
Layer 4: The transport layer. ...
Layer 3: The network layer. ...
Layer 2: The data-link layer. ...
Layer 1: The physical layer

What are salted hashes?

Salt at its most fundamental level is random data. When a properly protected password system receives a new password, it will create a hashed value for that password, create a new random salt value, and then store that combined value in its database. This helps

its hashes, the values will be different.

What do you think of social networking sites such as Facebook and LinkedIn?

Many think they are the worst thing that ever happened to the world, while others praise their existence. In the realm of security, they can be the source of extreme data leaks if handled in their default configurations. It is possible to lock down permissions on social networking sites, but in some cases this isn't enough due to the fact that the backend is not sufficiently secured. This also doesn't help if somebody else's profile that you have on your list gets compromised. Keeping important data away from these kinds of sites is a top priority, and only connecting with those you trust is also extremely helpful.

What are the three ways to authenticate a person?

Something they know (password),
Something they have (token),
Something they are (biometrics).

How would you judge if a remote server is running IIS or Apache?

Error messages oftentimes giveaway what the server is running, and many times if the website administrator has not set up custom error pages for every site, it can give it away as simply as just entering a known bad address. Other times, just using telnet can be enough to see how it responds. Never underestimate the amount of information that can be gained by not getting the right answer but by asking the right questions.

What is data protection in transit vs data protection at rest?

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.

A Linux admin account (root) has many powers that are not permitted for standard users. That being said, it is not always necessary to log all the way off and log back in as root in order to do these tasks. For example, if you have ever used the 'run as admin' command in Windows, then you will know the basic concept behind 'sudo' or 'superuser (root) do' for whatever it is you want it to do. It's a very simple and elegant method for reducing the amount of time you need to be logged in as a privileged user. The more time a user spends with enhanced permissions, the more likely it is that something is going to go wrong – whether accidentally or intentionally.

What is an easy way to configure a network to allow only a single computer to login on a particular jack?

Sticky ports are one of the network admin's best friends and worst headaches. They allow you to set up your network so that each port on a switch only permits one computer to connect on that port by locking it to a particular MAC address. If any other computer plugs into that port, the port shuts down and you receive a call that they can't connect anymore. If you were the one that originally ran all the network connections then this isn't a big issue, and likewise if it is a predictable pattern then it also isn't an issue. However if you're working in a hand-me-down network where chaos is the norm then you might end up spending a while toning out exactly what they are connecting to.

source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.

You can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts. Although sticky secure addresses can be manually configured, it is not recommended.

How would you build the ultimate botnet?

Cover the basics: encryption, DNS rotation, the use of common protocols, obscuring the heartbeat, the mechanism for providing updates, etc.

You are remoted in to a headless system in a remote area. You have no physical access to the hardware and you need to perform an OS installation. What do you do?

not have the capability of pushing out images via the network. This reduces the amount of hands-on time that is required on each system, and keeps the installs more consistent.

On a Windows network, why is it easier to break into a local account than an AD account?

Windows local accounts have a great deal of baggage tied to them, running back a long long way to keep compatibility for user accounts. If you are a user of passwords longer than 13 characters, you may have seen the message referring to this fact. However, Active Directory accounts have a great deal of security tied onto them, not the least of which is that the system actually doing the authenticating is not the one you are usually sitting at when you are a regular user. Breaking into a Windows system if you have physical access is actually not that difficult at all, as there are quite a few dedicated utilities for just such a purpose, however that is beyond the scope of what we'll be getting into here.

What is the CIA triangle?

Confidentiality, Integrity, Availability.

As close to a 'code' for Information Security as it is possible to get, it is the boiled down

Availability- keeping data accessible & available to the authorized parties at all times.

What is the difference between an HIDS and a NIDS?

Both acronyms are Intrusion Detection Systems, however 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. For an enterprise, NIDS is preferred as HIDS is difficult to manage, plus it consumes processing power of the host as well.

You find out that there is an active problem on your network. You can fix it, but it is out of your jurisdiction. What do you do?

particular way, and looking it out could mean big trouble. Bringing up your concerns to the responsible party is the best way to let them know that you saw a potential problem, are letting them know about it, and covering yourself at the same time by having a timestamp on it.

You are an employee for a tech department in a non-management position. A high-level executive demands that you break protocol and allow him to use his home laptop at work. What do you do?

You would be amazed how often this happens, even more so in the current BYOD environment. Still, the easiest way out of this one is to contact your manager again and have them give a yay or nay. This puts the authority and decision where it needs to be, and gives you assistance if the department needs to push back. Stress can be a real killer in position where you have to say 'no' to people that don't like hearing it, so passing the buck can be a friend.

What is the difference between closed-source and open-source? Which is better?

able to make changes yourself and recompile the code. Both have arguments for and against them, most have to do with audits and accountability. Closed-source advocates claim that open-source causes issues because everybody can see exactly how it works and exploit weaknesses in the program. Open-source counter saying that because closed-source programs don't provide ways to fully check them out, its difficult to find and troubleshoot issues in the programs beyond a certain level.

What is the Three-way handshake? How can it be used to create a DOS attack?

The three-way handshake is a cornerstone of the TCP suite: SYN, SYN/ACK, ACK. SYN is the outgoing connection request from client to server. ACK is the acknowledgement of the server back to the client, saying that yes I hear you, let's open a connection. SYN/ACK is the final connection, and allows the two to speak. The problem is that this can be used as a very basic type of Denial of Service Attack. The client opens up the SYN connection, the server responds with the SYN/ACK, but then the client sends another SYN. The server treats this as a new connection request and keeps the previous connection open. As this is repeated over and over many times very quickly, the server quickly becomes saturated with a huge number of connection requests, eventually overloading its ability to connect to legitimate users.

Much like getting a fresh set of eyes on a problem, sometimes you have people that don't want to see or don't want to admit to an issue. Bringing in extra help as an audit can really help eliminate problems that your team isn't able to resolve on their own. Granted they may cost a small fortune, but they are extremely good at what they do.

If you were going to break into a database-based website, how would you do it?

Learning to break into your own systems so that you can pen test them yourself. While the exact methods are different for each type of database server and programming language, the easiest attack vector to test for first is an SQL injection technique. For example, if the input fields are not sterilized, just entering a specific set of symbols into a form field may be enough to get back data. Alternatively, depending again on how the site is written, using a specially crafted URL may be enough to get back data as well. Footprinting the server ahead of time can help in this task if it isn't one you built yourself.

Why are internal threats oftentimes more successful than external threats?

and don't react as quickly to possible threats. On the other hand, say for example you have an annoyed employee that is soon to be fired and wants to show his soon to be former employer that he can bring them down, so he sells his still active credentials and card-key to a local group that specializes in white-collar crime. Still other infiltrators dress up as delivery people and wander around aimlessly in office buildings, getting information off of post-it notes and papers lying around. External threats do not have access to near this level of information about the company, and more often than not do not get in as far as somebody that spent 20 bucks on a knock-off UPS uniform.

What is residual risk?

A new car built by my company leaves somewhere traveling at 60 mph. The rear differential locks up. The car crashes and burns with everyone trapped inside. Now, should we initiate a recall? Take the number of vehicles in the field, A, multiply by the probable rate of failure, B, multiply by the average out-of-court settlement, C. A times B times C equals X. If X is less than the cost of a recall, we don't do one."

Residual Risk is what is left over after you perform everything that is cost-effective to increase security, but to go further than that is a waste of resources. Residual risk is what the company is willing to live with as a gamble in the hopes that it won't happen.

When you press delete on a file, it doesn't actually go anywhere. A bit on the file is flipped telling the operating system that that file is no longer needed and it can be overwritten as is required. Until that happens, the file can still be restored no matter if it's in a Recycling Bin or not. There are ways around this, such as using File Shredders and disk wipers, but both of these take quite a bit of time to finish their jobs to a reasonable degree.

What is the Chain of Custody?

When keeping track of data or equipment for use in legal proceedings, it needs to remain in a pristine state. Therefore, documenting exactly who has had access to what for how long is vital when dealing with this situation. Any compromise in the data can lead to legal issues for the parties involved and can lead to a mistrial or contempt depending on the scenario.

How would you permanently remove the threat of data falling into the wrong hands?

ensuring a disk's destruction by first using a specially made disc wiping program, taking apart the hard drive, removing the platters, scratching them up beyond recognition and then degaussing them with a high-powered magnet. This ensures that the data cannot be recovered through conventional means.

What is Exfiltration?

Infiltration is the method by which you enter or smuggle elements into a location. Exfiltration is just the opposite: getting sensitive information or objects out of a location without being discovered. In an environment with high security, this can be extremely difficult but not impossible. Again we turn to our friends in the fake delivery uniforms wandering around the building, and see that yes there are ways to get in and out without a lot of issues.

I'm the CEO of a Fortune 500 company. I make more in an afternoon than you make in a year. I don't care about this stupid security stuff, it just costs time and money and slows everything down. Why should I care about this junk?

having done your homework and having the support of the local IT team instead of alienating them is vital. Performing site assessments, creating executive summaries and line-by-line breakdowns of what goes where can help them to better understand what is going to be done and keep the project going.

I'm the legal council for a large corporation. We have requirements to document assets and code changes. We have a very limited budget for this task. How would you resolve this?

This is actually one of the easier ones – you have an informed party, asking for assistance to something that is important. They have money for the project (albeit not much), but it is better than nothing. At the very bottom of the spectrum, this could be accomplished in nothing more than Excel with a lot of time and data entry, moving all the way up the chain to automated Network Scanners documenting everything they find to a database and programs that check-in and out programs with versioning and delta files. It all depends on how big the project is, and how big the company is.

I'm the new guy – I used to be a coder at my old job and my manager wants me to create some custom programs. I need domain administrator rights

Unfortunately you will run into the hardball guy at least once in your career. In this case though, like others we have run into, it's time to move it up the chain to the manager. They will be able to give the yay or nay depending on exactly what the project is and be able to take the brunt of an attack if it comes.

Are you a coder/developer or know any coding languages?

Although this is not something an information security guy is expected to know but the knowledge of HTML, JavaScript and Python can be of great advantage. HTML and JavaScript can be used in web application attacks whereas python can be used to automate tasks, exploit development etc. A little knowledge of the three can be of great advantage – both in the interview and on the floor.

What is a WAF and what are its types?

WAF stands for web application firewall. It is used to protect the application by filtering legitimate traffic from malicious traffic. WAF can be either a box type or cloud based.

Cross Site Request Forgery is a web application vulnerability in which the server does not check whether the request came from a trusted client or not. The request is just processed directly. It can be further followed by the ways to detect this, examples and countermeasures.

When an attacker gets a victim's browser to make requests, ideally with their credentials included, without their knowing. A solid example of this is when an IMG tag points to a URL associated with an action, e.g. http://foo.com/logout/. A victim just loading that page could potentially get logged out from foo.com, and their browser would have made the action, not them (since browsers load all IMG tags automatically).

How does one defend against CSRF?

1. Synchronizer (i.e.,CSRF) Tokens (requires session state)

Unique per user session which uses a Large random value Generated by a cryptographically secure random number generator. The server rejects the requested action if the CSRF token fails validation

Approaches that do require no server-side state:

What is a Security Misconfiguration?

Security misconfiguration is a vulnerability when a device/application/network is configured in a way which can be exploited by an attacker to take advantage of it. This can be as simple as leaving the default username/password unchanged or too simple for device accounts etc.

What is a firewall?

A firewall is a device that allows/blocks traffic as per defined set of rules. These are placed on the boundary of trusted and untrusted networks.

How do you keep yourself updated with the information security news?

The world has recently been hit by Attack/virus etc. What have you done to protect your organization as a security professional?

Different organizations work in different ways, the ways to handle incident is different for all. Some take this seriously and some not. The answer to this should be the process to handle an incident.

What is port scanning?

Port scanning is process of sending messages in order to gather information about network, system etc. by analyzing the response received.

What is the difference between Vulnerability Assessment and Penetration testing?

What are the objects that should be included in a good penetration testing report?

A VAPT report should have an executive summary explaining the observations on a high level along with the scope, period of testing etc. This can be followed by no of observations, category wise split into high, medium and low. Also include detailed observation along with replication steps, screenshots of proof of concept along with the remediation.

What is compliance?

Abiding by a set of standards set by a government/Independent party/organisation. E.g. An industry which stores, processes or transmits Payment related information needs to be complied with PCI DSS (Payment card Industry Data Security Standard). Other compliance examples can be an organization complying with its own policies.

Tell us about your Personal achievements or certifications?

what are your next steps.

Various response codes from a web application?

1xx – Informational responses
2xx – Success
3xx – Redirection
4xx – Client side error
5xx – Server side error

DDoS and its mitigation?

DDoS stands for distributed denial of service. When a network/server/application is flooded with large number of requests which it is not designed to handle making the server unavailable to the legitimate requests. The requests can come from different not related sources hence it is a distributed denial of service attack. It can be mitigated by analysing and filtering the traffic in the scrubbing centres. The scrubbing centres are centralized data cleansing station wherein the traffic to a website is analysed and the malicious traffic is removed.

Explain the objects of Basic web architecture?

How often should Patch management be performed?

Patch should be managed as soon as it gets released. For windows – patches released every second Tuesday of the month by Microsoft. It should be applied to all machines not later than 1 month. Same is for network devices, patch as soon as it gets released. Follow a proper patch management process.

Can you describe rainbow tables?

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a password (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters.

What's more secure, SSL or HTTPS?

an updated, more secure, version of SSL. We still refer to our security certificates as SSL because it is a more commonly used term

If you had to both encrypt and compress data during transmission, which would you do first, and why?

Compress then encrypt. If you encrypt first you'll have nothing but random data to work with, which will destroy any potential benefit from compression.

In public-key cryptography you have a public and a private key, and you often perform both encryption and signing functions. Which key is used for which function?

You encrypt with the other person's public key, and you sign with your own private. If they confuse the two, don't put them in charge of your PKI project.

How do you govern various security objects?

the PCs will have the latest or last month's patch. On similar lines various security objects can be managed.

How does a Process Audit go?

The first thing to do is to identify the scope of the audit followed by a document of the process. Study the document carefully and then identify the areas which you consider are weak. The company might have compensatory controls in place. Verify they are enough.

What is the difference between policies, processes and guidelines?

As security policy defines the security objectives and the security framework of an organisation.
A process is a detailed step by step how to document that specifies the exact action which will be necessary to implement important security mechanism.
Guidelines are recommendations which can be customized and used in the creation of procedures.

Check the policy for the AV and then the alert. If the alert is for a legitimate file then it can be whitelisted and if this is malicious file then it can be quarantined/deleted. The hash of the file can be checked for reputation on various websites like virustotal, malwares.com etc. AV needs to be fine-tuned so that the alerts can be reduced.

Software testing vs. penetration testing?

Software testing just focuses on the functionality of the software and not the security aspect.
A penetration testing will help identify and address the security vulnerabilities.

What is you preferred – Bug bounty or security testing?

Both are fine, just support your answer like Bug Bounty is decentralised, can identify rare bugs, large pool of testers etc.

Web server hardening is filtering of unnecessary services running on various ports and removal of default test scripts from the servers. Although web server hardening is a lot more than this and usually organizations have a customized checklist for hardening the servers. Any server getting created has to be hardened and hardening has to be re-confirmed on a yearly basis. Even the hardening checklist has to be reviewed on a yearly basis for new add-ons.

What is data leakage? How will you detect and prevent it?

Data leak is when data gets out of the organization in an unauthorized way. Data can get leaked through various ways – emails, prints, laptops getting lost, unauthorized upload of data to public portals, removable drives, photographs etc. There are various controls which can be placed to ensure that the data does not get leaked, a few controls can be restricting upload on internet websites, following an internal encryption solution, restricting the mails to internal network, restriction on printing confidential data etc.

What are the different levels of data classification and why are they required?

organization, in broader terms data can be classified into:

Top secret – Its leakage can cause drastic effect to the organization, e.g. trade secrets etc.
Confidential – Internal to the company e.g. policy and processes.
Public – Publicly available, like newsletters etc.

In a situation where a user needs admin rights on his system to do daily tasks, what should be done – should admin access be granted or restricted?

Users are usually not provided with admin access to reduce the risk, but in certain cases the users can be granted admin access. Just ensure that the users understand their responsibility. In case any incident happens, the access should be provided for only limited time post senior management approval and a valid business justification.

What are your views on usage of social media in office?

Social media is acceptable, just ensure content filtering is enabled and uploading features are restricted. Read only mode is acceptable till the time it does not interfere with work.

There can be various ways in which this can be done:

Employees should undergo mandatory information security training post joining the organization. This should also be done on yearly basis, and this can be either a classroom session followed by a quiz or an online training. Sending out notifications on regular basis in the form of slides, one pagers etc. to ensure that the employees are kept aware.

In a situation where both Open source software and licensed software are available to get the job done. What should be preferred and why?

For an enterprise, it is better to go for the licensed version of the software as most of the software have an agreement clause that the software should be used for individual usage and not for commercial purpose. Plus, the licensed version is updated and easy to track in an organization. It also helps the clients develop a confidence on the organizations' software and practices.

When should a security policy be revised?

document and versioning. In case there are any major changes the changes need to be notified to the users as well.

What all should be included in a CEO level report from a security standpoint?

A CEO level report should have not more than 2 pages:

A summarized picture of the state of security structure of the organization.
Quantified risk and ALE (Annual Loss Expectancy) results along with countermeasures.

How do you report risks?

Risk can be reported but it needs to be assessed first. Risk assessment can be done in 2 ways: Quantitative analysis and qualitative analysis. This approach will cater to both technical and business guys. The business guy can see a probable loss in numbers whereas the technical guys will see the impact and frequency. Depending on the audience, the risk can be assessed and reported.

Any event which leads to a compromise of the security of an organization is an incident.
The incident process goes like this:

Identification of the Incident
Logging it (Details)
Investigation and root cause analysis (RCA)
Escalation or keeping the senior management/parties informed
Remediation steps
Closure report.

Is social media secure?

Not sure if the data is secure or not but users can take steps from their end to ensure safety.
Connect with trusted people
Do not post/upload confidential information
Never use the same username password for all accounts

Chain of custody?

issues for the parties involved.

How should data archives be maintained?

Gone are the times when there used to be files and cabinets which held data over the years. This phase was long followed by archiving data over magnetic tapes and storing the tapes. There is another overhead for the maintenance and safety of the tapes. These are few conventional approaches, but the world is slightly moving to the cloud storage architecture. The only hurdle is the data privacy. Companies are not very sure about handing the critical data. This will actually take time but securely configured and managed cloud can be one of the best options.

Does TLS use symmetric or asymmetric encryption?

Both. Have them talk through how each are used. The key (sorry) is that they understand the initial exchange is done using asymmetric and that bulk data encryption requires speed and therefore symmetric algorithms.

Look for the standard responses, with the client sending helo with ciphers, server responding with a public key and picking a cipher, agreement on a shared key, etc. But then dive deeper into the questions below.

If someone steals the server's private key can they decrypt all previous content sent to that server?

Traffic Eavesdropping, Man-In-The-Middle.

What are some common ways that TLS is attack, and/or what are some ways it's been attacked in the past?

Look for a conversation about weak ciphers, vulnerabilities like Heartbleed,

Forward Secrecy is a system that uses ephemeral session keys to do the actual encryption of TLS data so that even if the server's private key were to be compromised, an attacker could not use it to decrypt captured data that had been sent to that server in the past.

What are your first three steps when securing a Linux server?

Document the host information. User management. Generate an SSH key pair. Linux SSH daemon configuration. Firewalls. Account-level security. Simple intrusion prevention. Intrusion detection. Keep your OS up to date. Secure BIOS protection. Hard disk encryption. Lock the boot directory.
Check for open : Use 'netstat' command to view open ports and and corresponding services .
Enable SELinux : Security-Enhanced Linux (SELinux) is an access control security mechanism provided in the kernel.

Permissions and verifications

What are your first three steps when securing a Windows server?

Set up appropriate access control to the physical machine and logical components
Institute a strong audit and logging policy | Create a baseline backup | Keep an eye on accounts.
Keep patches up-to-date.

Why is DNS monitoring important?

DNS has an important role in how end users in your enterprise connect to the internet. Each connection made to a domain by the client devices is recorded in the DNS logs. Inspecting DNS traffic between client devices and your local recursive resolver could reveal a wealth of information for forensic analysis.

DNS queries can reveal:

Botnets/Malware connecting to C&C servers
What websites visited by an employee
Which malicious and DGA domains were accessed
Which dynamic domains (DynDNS) accessed
DDOS attack detection like NXDomain, phantom domain. random subdomain

Do you prefer filtered ports or closed ports on your firewall?

rat has eaten through the data cable, you have a bad optical transceiver etc. On the other hand, rejection packets from a closed port could be used in a DDOS attack against a third party. You won't get any amplification to speak of (as you might from a too-open NTP server) but you could obfuscate the source of at attack.

Filtered: sends back a response that traffic is blocked, gives away firewall presence

Closed: causes timeout, not response.

Obscurity increases the attackers work by a bit. They suspect but do not know for sure that a firewall is present. Attacker can attempt again or attempt other types of traffic. This may increase chances of detecting 'scanning'.

What are Linux's strengths and weaknesses vs. Windows?

Cost: Free | Security: + | System Requirements: Low | Options: Gnome, KDE, Xfce | Learning Curve

Cryptographically speaking, what is the main method of building a shared secret over a public medium?

So lets take an example of Alice and Bob.

1] Alice has private key A. Bob has private key B. (Never shared with anyone)
2] In between these two there is a public domain. There is a big prime number N and a generator G.
3] Lets assume there is one big copy of G.
4] We combine the private keys with the generator in the public domain. Alice gets AG. Bob gets BG. They are public and are exchanged.
5] As an attacker, you know AG & BG which are Alice and bob's public component.
6] Alice will now take the public component that bob sent her and add her private key, while Bob will take the public component that Alice sent her and add his private key.

Which results in Alice getting ABG & Bob getting BAG. (Which are done in privately and they both get same keys) And also the order doesn't matter.

What's the difference between Diffie-Hellman and RSA?

Diffie-Hellman is a key-exchange protocol, and RSA is an encryption/signing protocol.
One requires you to have key material beforehand (RSA), while the other does not (DH).

Where can automation be improved in security?

Automatic vulnerability scan remediation

Automated code vulnerability remediation

Automated forensic analysis

How malware evades signature-based antivirus?

The basic explanation is that it mutates itself, rewriting its own code automatically until no antivirus programs detect it.

What is Info Sec VS App Sec VS Network Sec Vs IT Sec

These are all relatively loose terms, and practitioners often have to be able to function in the roles of regular admins or programmers to be functional. That does not mean they have to be as efficient — AppSec folks probably aren't as used to writing sorting algorithms, for example.

– Information Security:

Covering everything to do with information security. InfoSec specialists cover a wide range of topics and are skilled generalists. In a big company setup, they are your CISOs and managers. In a smaller company, they are your practitioners.

– Network Security:
Firewalls, IDS, VPNs; practitioners understand lots of application-specific protocols. Anything that flows through a router is in their world.
– IT Security:
Host-based security, domain controllers / auth servers, mandatory access controls systems. ITSec is focused inside of the system.

Where is Cyber Sec + Data Science used?

Threat intelligence, malware reversing, and detection all use data science. Their goal is to generalize from a small set of observed samples of malware into something that can be reliably detected. There are also a lot of unique roles based on individuals' research.
A person with skill in both data science and security is one of the hottest commodities in the labor market right now.

How to mitigate DDos attacks?

The simple idea is to use highly optimized servers or hardware to rapidly identify packets from the attack based on patterns in the traffic.

and if the attacker controls 10 Mbps of bandwidth, the victim received a 1 Gbps DDoS attack. For example, a single packet sent to an NTP server can cause it to send dozens of packets of unwanted time data to the victim.

However, using these amplification techniques causes patterns in the packets received by the victim, since the attacker doesn't have total control over what's sent. For example, they might all start with a certain header that's not normally seen by that server.

The DDoS protection servers look for this type of unusual traffic and drop it before it reaches the application servers. The patterns are usually identified automatically but can also be programmed manually.
Because the DDoS protection servers are doing such basic computations, their throughput can be very high. But it's not infinite: in theory a large enough DDoS attack could overwhelm them, although the required scale might saturate other aspects of network infrastructure first.

How would you detect insider threats?

Users from one department or job role accessing or attempting to access data from another in a suspicious way
Large file transfers by employees around the time they're leaving a company
Accesses to services like Dropbox that the company doesn't usually use
Employees with privileged access using that access much more often than their peers
Unusual login activity that might indicate someone using someone else's password or

Why do we fail to detect hackers?

We try to detect malicious activity using pattern matching against signatures of known exploits and malware. This works horribly. Attackers can simply purchase every commercial product on the market and automatically mutate their exploits until the commercial products don't detect them, and they can innovate new attack techniques that the defenders don't know about.

What sort of anomalies would you look for to identify a compromised system?

Draw out a basic network architecture including security technologies like IPS/IDS, Firewalls, AV, etc, and described the type of traffic and logs you could use to identify a compromised system.

What kind of attack is a standard Diffie-Hellman exchange vulnerable to?

How would you implement a secure login field on a high traffic website where performance is a consideration?

TLS is a must for the entire site at this point, and that there are very few situations where you shouldn't insist on encryption.

What are the various ways to handle account brute forcing?

Account lockouts, IP restrictions, log, etc.

How does HTTP handle state?

It doesn't, of course. Not natively . "cookies", but the best answer is that cookies are a hack to make up for the fact that HTTP doesn't do it itself.

Stored is on a static page or pulled from a database and displayed to the user directly. Reflected comes from the user in the form of a request (usually constructed by an attacker), and then gets run in the victim's browser when the results are returned from the site.

What are the common defenses against XSS?

Input Validation/Output Sanitization.

What is the primary reason most companies haven't fixed their vulnerabilities?

This is a bit of a pet question for me, and I look for people to realize that companies don't actually care as much about security as they claim to–otherwise we'd have a very good remediation percentage. Instead, we have a ton of unfixed things and more tests being performed.

This is a big one. What I look for is one of two approaches; the first is the über-lockdown approach, i.e. “To control access to information as much as possible, sir!” While admirable, this again shows a bit of immaturity. Not really in a bad way, just not quite what I’m looking for. A much better answer in my view is something along the lines of, “To help the organization succeed.”

If you were to start a job as head engineer or CSO at a Fortune 500 company due to the previous guy being fired for incompetence, what would your priorities be?

Where is the important data? Who interacts with it? Network diagrams. Visibility touch points. Ingress and egress filtering. Previous vulnerability assessments. What’s being logged an audited? Etc. The key is to see that they could quickly prioritize, in just a few seconds, what would be the most important things to learn in an unknown situation.

As a corporate Information Security professional, what’s more important to focus on: threats or vulnerabilities?

Codenza

Designed by **Divyendra Patil and Pratik Paranjape**