Stage 10

Article Name: ***Growing Threat of DDoS on DNS***

Student Name:John & Kevin

Summary:
DNS security has been getting attacked by DDos. Still other companies use DNS security on their IT infrastructure. Since DNS are easy to exploit, a lot of hacker knows the weakness around it. Hackers hijack the system to send queries to nameservers across the internet from a spoof IP address of their target.Other organization still don't know how much of a threat this is, and it's very much dangerous for you and your organizations.

Key Points:

- "In its **2014 Annual Security Report**, Cisco found that all the corporate networks examined showed evidence of having been compromised."
- "To see the extent to lity for DNS security and taking steps to understand typical query loads are both relatively simple which these amplified responses can be used as an effective DDoS attack, consider a query of just 44 bytes. This single query, if sent from a spoofed IP address to a domain containing DNSSEC records, could generate a response of over 4,000 bytes."
- "Formally assigning responsibility for DNS security and taking steps to understand typical query loads are both relatively simple tasks that will help reduce exposure to DNS attacks.
- "Formally assigning responsible tasks that will help reduce exposure to DNS attacks."

Other Facts:

How is the crashing of my website dangerous? If i had a profitable business, maybe I would lose customers, rapport, security from a hack like this.How can one avoid a DNS attach? (guest)
why do companies use DNS if its easy to exploit?(christian)
What are the weaknesses of the Domain Name System? (Vanessa F)
How does it crash the web site and how is it affected? (LAURA)

How is it dangerous to us and our organizations? Why hasn't extensive measures been taken to stop these destructive attacks?(Carissa Mangahas)
What does it mean by "all the corporate networks examined showed evidence of having been compromised."
Why don't organizations know how large the threat is? (stephanie)
What is an IT Infrastructure?(ana)
How is this dangerous and how do the hacker find the weak spot? (Belcy)

What is an IT infrastructure? (Citlaly Moncada)
What makes the DDos and DNS so effective? (Carmela M)

how does this affect everyday users?(Myra)
What threats does DDos pose on users? (Nancy Lopez)
Article Name:The Details Behind a Denial of Service Attack: What It Is, Why It Matters & What You Can Do To Stop It.
Student Name:Laura Ana

Summary:The denial-of-service is a attack that concentrated automated attempt to the overload a target network. This happens when a network is being overload.The central processing unit (CUP) is a unit that tries to help out the network by answering the answers. A DoS attack involves a single initiating source computers. A DDoS attack is more serious than a DoS attack. An attack is more likely to happen during a Black Friday/Cyber Monday sale or a new important product launching. There are three different types of fundamental forms of denial-of-service & distributed-denial-of-service attacks & they are ; volumed based, protocol based, & application based. A volume based attack's goal is to overwhelm your network capacity. A protocol based attack is servers which exploit the way systems communicate with each other. Application based attacks are hackers that know the vulnerability of the web & they try to crash it down.

Key Points:

- One common type of application based attacks is to send partial requests to a server to attempt to use up the entire database connection pool of the server which in turn blocks legitimate requests.
- Cloudwatch services tracks various network I/O metrics & can also signal performance degradation.

Other Facts:

The first step in preventing an attack is to setup a remote website monitoring service. This will send you a notification when your online store becomes slow or crashes down. DDoS attacks often involved vulnerabilities in low level operating systems.

What does it take to have a network overload in what would become disruptive to services we've been accustomed to be easily accessible?(Carissa Mangahas)
What happens when it messes up or a difficulty happens ? Would it be able to be fixed ? (Kevin A.)
How is a DDos attack more serious than a Dos attack?(Lissete)
Why would a volume based attack want to overwhelm a network's capacity? (Citlaly Moncada)
why is sending partial requests to a server a common type of an application based attcacks?(christian)
How do you know when you've been attacked? (Belcy)

How do people learn how to send these attacks? Is there a way to monitor and destroy that knowledge to prevent further attacks? (guest)
Is the process of setting up a remote website monitoring service complex and time-consumi
Is a remote website monitoring system service reliable, considering many websites still get gacked with few levels of security?
Is it guaranteed that attackers won't be able to attack if you use this?(Carmela M)
What are some ways of upgrading low level operating systems so that they won't be as vulnerable to Ddos attacks?(Myra)

Is there any more measures that we can take to prevent these kinds of attacks? (Nancy Lopez)

Article Name: How to Launch a 65Gbps DDoS, and How to Stop One
Student Name: Eric Marive

Summary: This article talks about how to launch a 65 Gbps DDoS, and how to stop one. It explains how a DDoS is initially created and what components go into one.

Key Points:

- A DDoS is a type of DoS attack. A DoS is a denial of service attack. The point of this attack is to make a machine or network unavailable to its intended users.
- These attacks use zombie computers that are infected with a virus, that send a great amount of data to the machine or network, to make it unavailable.
- For a DDoS to be successful, it needs to have thousands of computers that are infected, so the traffic sent to that certain network or machine in a great amount, to the point where it can no longer handle it.

Other Facts:

When someone wants to create an attack they usually rent a large botnet. Though these can be highly expensive, attackers usually look for other ways to amplify the size of their attacks. One technique that these attackers use is called DNS reflection.

What components go into a single DDoS?(Carissa Mangahas)
How is it that this attack make components go in?
Is the DDos a big threat in terms of hacking ? (john D.)
What is a zombie computer?(Lissete)
What is a DNS reflection? how do we set up such attacks? (Guest)
What is a botnet and how are you able to rent it?(Vanessa F)
What did the DNS reflection do? (Kevin A.)

Can these attacks use another source other than zombie computers? (Stephanie Diaz)
How can you get rid of this virus? (Citlaly Moncada)
Why do attackers look
What enables attackers to rent a large botnet?(Carmela M)
How can you prevent it from infecting your device?(Belcy)
why do they rent a large botnet when someones wants to create an attack?(christian)
How does a DNS reflection work?
How long is the virus active? (Nancy Lopez)

ARTICLE NAME: HOW DNS WORKS

Student Name: Enrique Francisco

Summary:
In February 2015, both Lenovo and Google became victims to domain hijacking. When users tried to access those websites, they were instead redirected to different websites.Both Lenovo and Google were victims of in other words “IP spoofing” which spoofs the website that one tries to access and instead redirects it to the owner of the fake website.In this case, once Lenovo was redirected to the website the culperates behind the spoofing were taking live stream of Lenovo and redirecting others as well forcing them to watch Lenovo.

Key Points:

- Domain hijacking is a type of attack against the Domain Name System(DNS) which translated domain names into IP addresses that can be called into a browser.
- Changes to domain name records can be dangerous for Web users since there’s little they can do to protect themselves.
- Domain name registrars have been slowly implementing a security technology called Domain Name System Security Extensions (DNSSEC) to better protect domain name records.
- DNSSEC is difficult to set up and has not been supported by many registrars and hosting providers.

Other Facts:
The hacker group Lizard Squad took credit for the attacks. They also had access to Lenovo’s email. DNSSEC could have helped protect Lenovo from the attacks or at least made the steps much more difficult for the attackers.

What percent of people have actually been fooled by what to us is quite obviously fake?(Carissa Mangahas)- We live in the 21st century where a percent of people don’t have the common sense to figure it out, and are swayed by the hackers.(MORGAN THE JUGG)
what kind of websites were they redirected to?(christian)
How do we educate the general public to be aware of such spoofing attacks? They are so common and many people lose money this way. (guest)-Make a note not to give out information so easily and question them, also make sure to be on guard for this kind of scenario.
Which registrars and hosting providers support the DNSSEC?(Lissete)
Do you know what kind of websites they were redirected to? (Citlaly Moncada) The Lenovo website was redirected to a picture of some teenager in his room while the article did not state where Google was redirected to.
What makes it so difficult to set up DNSSEC? (Belcy)
How were they able to hack?-The IP address of the website was changed and redirected to the fake website.

Why are hackers able to take over such famous and big companies?(Carmela M)- The hacker gained access to a company that is responsible for the domain names and was able to find a vulnerability through them and not directly with those big companies

What other attacks have been done by the Lizard Squad? (Vanessa F)-Lizard Squad has supposedly taken credit for attacks against many other.- Google it.
companies such as Microsoft.
How were they able to hijack google and lenovo? (Ana)- They gained access to their DNS and changed it in order for it to be redirected to different websites.how did lenovo and google get revenge? (John D.)
Was is it difficult to attack for Lizard Squad ? (Kevin A.)-I really isnt quite actually, you just need the correct type of equipment to pull off such a scheme, such as a protocol that changes the IP address of the hacker every minute.
how would you be able to tell when you are being hacked?(Myra)- You would be able to tell if you do not reach the website that you requested and were instead taken to another. In addition, those other websites might have malicious software that can disrupt your computer.

What effects does domain hacking have on servers? (Nancy Lopez)

Article Name: DDoS Attacks Against NATO Likely DNS Amplification or NTP Reflection,Expert Suggests
Student Name:Vanessa

Summary:The video explains how the Domain Name System,or the DNS,works.
Key Points: ● Computers and other devices communicate using IP Addresses to identify each other on the Internet. ● People don't remember IP Addresses so they use words. ● The Domain Name System brings the two together and gets you to your destination. ● The DNS goes through the server and finds the IP Addresses.
Other Facts: The DNS works by searching for the IP Address and goes through a process to find the IP Address for that website.The DNS first goes through by finding the root of the websites and checks for that IP Address.Next,it goes again that process but it looks for the websites.After it is done going through those process it becomes the websites.

Why does it go through that process ? Why remember words instead of the numbers? Isint it the same? you still have to remember it. (Laura)
So the DNS is like the old school phone operator? You dial zero and they answer and ask you who you are looking for. You give them a name. They ask for an address. They give you back a phone number so you can connect to that person. If that person has no number listed, you are told that persons phone does not exists. There was a fee for this service. I am wondering is there a fee for DNS? (guest)
Why is it that people don't remember their IP addresses? (Stephanie Diaz)
Isn't using words for remembering an IP address a bit unreliable?(Morgan 'n Nava)
So the DNS finds the IP address for the website you go on? (Citlaly Moncada)
What does DNS stand for?(Myra)
Does the DNS act much like anything else in the Internet?(Carissa Mangahas)
Is the IP address important ? (John & Kevin)
How does it help you get to your destination?(Belcy)
Are IP addresses basically just websites with numbers instead of letters?(Vanessa F)

What reasons would we need DNS if we have IP adresses?

How does the DNS find you websites?(Ana)
When was the DNS system created?(Lissete)
Why does DNS/s help internet users and how does it function the way it does? (Carmela M)
What advantages do we benefit from by using the DNS system? (Nancy Lopez)

Article Name: DDoS Attacks Hit Video Gaming Industry with 90 Million Requests per Second
Student Name: Belcy Lissete

Summary: The researchers at a US security firm noticed a DDoS attack against a famous Video Gaming website. The attack peaked at approximately 90 Mpps (Million Packets Per Second), which a majority of the IP addresses belong to China and India. The attack was symmetrical meaning thousands of rapid valid DNS requests are targeted to the server. This caused the site to have more traffic resulting in slower and slower response times for legitimate requests. This malicious attack has been exhausting the server considering it could only process up to 170 Gbps/100 Mpps worth of traffic at an incline rate, and up to now they have only seen 50-60 Gbps without amplification. Recently the hackers are reaching above 110 Gbps, so the researchers have to figure out how to face this comeback.

Key Points:

- DNS servers provide the roadmap to the Internet and help clients find the servers they are looking for.
- DNS floods attempt to exhaust server side assets with large number of UDP requests generated by the malicious scripts running on several compromised botnet machines.
- DNS amplification attack is an asymmetrical DDoS attack meaning that that the attackers set the source address to that of the targeted victim.
- Attacks are launched from multiple connected devices that are distributed across the internet.

Other Facts:

Researchers at the DDoS protection service are mitigating with this attack with just one of their servers they are able to process up to 170Gbps/100Mpps worth of traffic at an inline rate.
A US based security solution provider is Incapsula is protecting a famous Video Gaming website from this high bandwidth DDoS attack from the last 48 hours.
Majority number of attacking IP addresses belong to India and China,

China is seen in the big seen in regards to the gaming world, yet how is it so that it is in similar amounts of hacking as it were in India had it been that India is not one with such high demographic terms in gaming with China? Is it possible that the percent of hacking in India is as high as it is to China as a proportionate or overall? Is the forms of hacking in games so disruptive that it is taken into the median to the attention of the United States when it is well guarded based on the well popular game providers known as Valve?(Carissa Mangahas)
How were the attacks making the process slower and slower?(Laura)
Is the reason China and India have majority of the IP addresses because of the amount of hacking that takes place in those two countries?(Vanessa F)
Did they say what famous video gaming website was hit? What are the benefits of slowing down service from a video gaming website? (guest)
What do these people get from hacking a video game industry? (Citlaly Moncada)

Why were most of the requests coming from India and China?(Nva and Mrgn)

How do dns servers provide roadmaps?
why would china and india have the majority number of attacking IP addresses?(christian)
Did they take it as a Threat ? (Kevin & John)

How will China and India take care of this issue? Are they planning to take care of this issue? (Carmela M)

Can the server’s tolerance of traffic be increased in order to be faster? (Nancy Lopez)

Article Name: St. Louis Federal Reserve Suffers DNS Breach
Student Name: Christian and Fara

Summary: The U.S.'s central bank forced a password reset after a cyberattack redirected visitors to parts of its website to fake Web pages. The Federal Reserve Bank of St. Louis was made aware that on April 24, 2015, computer hackers manipulated routing settings at a domain name service (DNS) vendor used by the St. Louis Fed so that they could automatically redirect some of the Bank's web traffic that day to web pages they created to simulate the look of the St. Louis Fed's research website, including webpages for FRED, FRASER, GeoFRED and ALFRED. Users who were redirected to one of these phony websites may have been unknowingly exposed to vulnerabilities that the hackers may have put there, such as, malware and access to usernames and passwords.

Key Points:

- Hackers manipulated routing settings at a domain name service used by the St. Louis Federal so that they could automatically redirect some of the Bank's web traffic that day to fake web pages they created to simulate the look of the St. Louis Fed's research website.
- Attackers succeeded in hijacking the domain name servers for the institution.
- The Federal Reserve Bank of St. Louis was made aware that on April 24, 2015, computer hackers manipulated routing settings at a domain name service (DNS)
- As of today The St. Louis Federal is still not clear how it happened, it remains unclear of what impact.

Other Facts:
Once they found out there was a DNS attack many were informed to change their passwords to prevent these hackers from getting everyone's information.

What measures are being taken to alleviate the amount of hacking, and to what extent is something then entitled as a breach of federal law?(Carissa Mangahas)
How can they be unaware of how it happened? Was it an inside job? (guest)
Was there anything else the bank could've done rather than tell people to change their passwords and usernames?(Nava and Morgan)
How can the Federal Reserve Bank of St. Louis improve their computer systems to avoid this in the future? (Stephanie)
How were users directed to "phony" websites? (Ana)
How many times did they try to hack it ? (Kevin)
How were users alerts that their were being hacked? (LAURA)
What did they do to recover from this? (Belcy)
What is the effect of a DNS attack to it's users?
How did they get better security after? (John D.)
Were the members of the bank given any compensation for such failure of security?(Lissete)

How did the hackers manipulate the routing system? (Citlaly Moncada)

Does the rerouting of the Bank’s web traffic affect anyone’s money in any of the accounts? (Vanessa F)yes

How is the government dealing with this issue, and what makes it easy for hackers to hack in the first place? (Carmela M)

Did the government implement any additional security in order to prevent future hackers from doing this? (Nancy Lopez)

Stage 8
Article Name: Accidental DDoS? How China's Censorship Machine Can Cause Unintended Web Blackouts
Student Name: Vanessa and Citlaly

Summary: The data Hockenberry was looking at, showed a massive spike in traffic hitting the email server of his software and graphic design company, Iconfactory. After the initial shock, an investigation revealed the massive influx was caused by a significant number of requests that were supposed to go to other sites, from facebook to youtube but ended up being routed to Iconfactory. Instead of timing out users connections to banned sites. The DNS system took citizens to seemingly random websites. Those online services that weren't ready for what would amount to distributed denial of service (DDoS) attacks flatlined. If China's censorship machine either screws up or is hacked it could redirect hundreds of millions of connections to online services and subsequently wipe out bits of the web. China would start to clog up some of the internet pipes out to the wider world.

Key Points:

- A massive influx of data occurred in the Iconfactory because of many requests that were supposed to go to other sites, from Facebook and Youtube, but ended up being routed to the graphic design company.
- China's government tweaks the Domain Name System (DNS) to stop people from accessing non-approved websites. This is called DNS poisoning as hackers often use it to direct people to malicious sites.
- Something went wrong with China's hacking efforts and instead of timing out users' connections to banned sites, the DNS system took citizens to random websites.
- Distributed denial of service is called DDoS and it is the attack of hackers sending people to different websites. Users are sent to various sites that are unrelated to what they were really searching for.

Other Facts: Anyone with control over the DNS system could take advantage of their position and launch DDoS attacks.

The Domain Name System converts website names like Forbes.com to a numerical IP address so PCs and servers can talk with one another.

Censorship systems may or may not always be secure.

How do you prevent DDoS attacks?(Morgan and Nava)

Where are these hackers coming from and what are their intentions? Do they benefit from this in any way, in regards to China and its overall ideology of how to govern?
What are examples of sites these people are getting redirected to?(Carissa Mangahas)
Why were they send to the iconfactory instead of sending them to where they wanted?
how can we prevent more attacks? (myra)

Why is the censorship system not always secure? (Belcy)
Why use a censorship system if it may or may not work? (Stephanie Diaz)
What are examples of non-approved websites?(Lissete)
What laws are in place to protect a web designer from these hacking efforts? What supports exists to assist a company such as the graphic design company mentioned in the article?

How is China censorship machine will crash? (John D.)
Why do the they use the machine if it only causes trouble and confusion? (Carmela M)
Why will they hijack the DNS system ? (Kevin A.)
Why were email software and graphic design companies hit the most? (Debbie Argueta)
Why aren't always censorships good or bad? - Christian M

Why may censorship systems may or may not be secure?(Ana)

How can someone take control of the DNS system? (Nancy Lopez)

Article Name: Turkish ISPs Intercept Google DNS Services to Spy on Internet users
Student Name: Carissa& Myra

Summary:

The Internet is a place that serves to store an excessive amount of information based on the large base of users that have access to it. This makes it so that it is susceptible/subjected to hacking and a nice target for ill-wishing groups, much involved in politics. Though vulnerable, very few times has there been hijacking for DNS servers, Recent cases, however, have shown that Turkey was involved in hijacking Google's DNS servers, as it changes the IP addresses of some users- alternating the website to one that would benefit them in a sense that they can gather that information, not run regularly by merely imitating sites and not actually being the official. This misuse of the internet shows the corrupt governing of Turkey and its internet providers in regard to personal privacy, thus affecting Youtube, Twitter, and plenty of other popular domain names(social networking sites).

Key Points:

- DNS networks are being hijacked by Turkish Telecom
- Turk Telecom began to hijack the IP addresses of popular free and open DNS providers such as Google's 8.8.8.8, OpenDNS' 208.67.222.222 and Level3's 4.2.2.2.
- Turkey has been tracking down users or citizens attempting to avoid censorship efforts by the government. For example, on March 21, the government began to block access on twitter and claimed that the social networking site violated the privacy laws of Turkey.
- Google discovered that most Turkish Internet service providers have disguised themselves as Google DNS, perhaps to spy on its users.

Other Facts:

- **It all began when the president of Turkey ordered the censorship of Twitter.com**
- **There is similar activity of hijacking of DNS networks in China**

How can we manage to protect the Internet more secure for those that are able to access it?(Morgan and Nava)

Why not ban other social media forms? (Stephanie Diaz)

What does the government gain by acting as a spoof site to gather and steal information from its citizens?

Why Twitter? In what ways does the social networking site violate the privacy laws? (sounds like LAUSD) Guest

Other than to spy on the users, why may have Turkish Internet services have desguised themselves?(Lissete)

Has there been any DNS hijacks in the US?(Ana Cisneros)

Does this mean Turkey is basically “banned” from using social media because it violates their privacy? (Vanessa F)

Why did Turkey do that? (Debbie Argueta)

why does hacking DNS server
How does it violate Turkey’s law? (Belcy)

Why is it that they attack more the social networking ? And how is is that they are able to change the IP address? (laura)

How do they change the IP addresses of the users? (Citlaly Moncada)

Why does Turkey leaders believe it is fit to affect the social networks just for their own protection? (Carmela M)

what were their ip adresses changed to? - christian

Does Turkey continue to pose a threat to social networking sites? (Nancy Lopez)

Article Name: DDoS Attacks Double But Could Go Bigger Still With IPv6
Student Name: *Stephanie* & *Debbie*

Summary: Attacks are becoming larger and nearly doubling since the past year. Akamai found a rise in application layer attacks, up to 22.22 %. As well as the infrastructure layer (level 3&4) attacks, rising 36.74%. Gaming was hit by the most attacks with 35%. An increase in DDoS-for-hire activity and had seen eight 'major' attacks reaching more than 100Gbps, with attackers leveraging all techniques including SYN floods, DNS and ICMP. SSDP, a protocol enabled by default in millions of home and office devices including routers, smart TVs, webcams, printers and media server, accounted for 20% of activity, a rise considering it was not in the previous report. According to Akamai Technologies, more attacks may occur as we migrate to IPv6. The DDoS is being used more frequently as a masking agent or security perimeter degradation tool.

Key Points:

- Attacks have increased by 116.5% on a year-on-year basis.
- Attacks have been more severe than usual.
- Akamai found that there was a significant rise in application layer attacks over the past year.
- Security organizations should begin taking the security of low-level DDoS seriously.

Other Facts:

- Akamai Technologies expects to see more of these attacks as plans advance to migrate to IPv6
- Attacks have also become longer, up from 24.82 hours from 17.38 hours (an increase of 40 percent) on a yearly basis.
- Security organizations aren't taking proper action when dealing with these attacks.
- Smaller attacks are not reported as often as they should be.
- Gaming was hit the most by these attacks (35% of the attacks.)

By attacks, do you mean hacking and DDos attacks? (Vanessa F)

Why is it most popular to see hacking integrated to gaming, or in relations to the gaming community? Many games are entitled to what is known as a VAC ban, thus hacking in such high numbers seem to be unlikely, why do you believe Akai sees it as so?(Carissa Mangahas)

Why are smaller attacks not reported as often? (Belcy)

Why have attacks increased or become longer? (Citlaly Moncada)

Who is AKAMAI and how are they related to gaming and DNS? What are the results of getting a trojan when gaming? (guest)

what are DDos attacks? - (christian)
How can you limit or stop this from happening? (Myra Pham)

Could they turn to a different alternative rather than using IPv6?(IPv6 is a form of hierarchy protocol in which IP addresses are assigned to.) {Nava and Morgan}
What are the causes of the sudden increase in attacks?(Lissete)
What is IPv6? (guest)

Do you believe that attacks will increase as times goes by? (Ana Cisneros)

How many times will there be an attack ? (Kevin Arellano)

What kind of attacks are these? (Carmela M)

Why is it that the gaming attacks have increased? (laura)

Why do they attack it? (John D.)

How many times will they attack ? (Kevin A.)

What is the cause of the increase in attacks? (Nancy Lopez)

Article Name: “New Zealand Internet Providers Threatened with Legal Action for Providing Access to US Netflix”
Student Name: Carmela & Nancy

Summary:

New Zealand providers had allowed their subscribers to access the US-based version of Netflix. The problem with this, however, is that it goes against Netflix’s terms to access of being outside the US. There is nothing illegal about it, but the providers of Netflix in the US are still concerned with the legal threat.

Key Points:

- “If the group does take the providers to court it’ll be an interesting legal battle with potentially wide-reaching consequences.”
- “The service, called “global mode” uses a DNS trick to make users appear to be in the US. It’s a legal grey area that’s officially banned by Netflix’s terms and conditions, but the company hasn’t yet enforced yet.”
- “The problem is, those working around geo-restrictions aren’t exactly doing anything illegal. It *might* be against Netflix’s terms to access it outside the US, but it’s not the same thing as piracy. Some lawyers in New Zealand believe that using such tricks to gain access to Netflix is technically “parallel importing” and so is perfectly legal.”
- “If the group does take the providers to court it’ll be an interesting legal battle with potentially wide-reaching consequences.”

Other Facts:

“Exclusive TV rights within a country are even harder to control with an open internet, and if the court rules in favor of the rights holders it could set precedent to make accessing overseas content entirely illegal.”

“The internet providers are currently rebuffing the efforts from the TV networks to kill the global mode technology, however it remains to be seen if they’ll fight it if the case is escalated to the courts or simply back down.”

Questions:
When users use their financial information to log into the site, are they using real info? Is it traced back to New Zealand or US accounts? Netflix should have access to financial documents to verify New Zealanders are using the account against their privacy policy. (Mrs. Guest)
~The users are using real information. However, a DNS trick is used in order to manipulate information and make it seem as if the users are in the US.
Is Netflix doing anything to prevent their services from illegally reaching territories outside of the U.S.? (Vanessa F)

~Well, Netflix already states it in their terms of service that the US-based Netflix is for US users. New Zealand can possibly have their own version of Netflix, which would be New Zealand Netflix. And that's exactly the problem that the US has. Because the US Netflix is for US users, they find it unfitting that New Zealand would have the need to use their Netflix(US Netflix) instead of their own Netflix, which is the New Zealand Netflix.

How does Netflix know in the first place that it's a "fake" account? It can possibly just be a normal account that is being accused. {Eric Atayde}
~The accounts are not fake. They include real information. However, they recently traced several accounts to New Zealand by reversing the DNS trick and discovered that thousands of accounts were actually from New Zealand.

Why is it not misconduct of Netflix policy if a New Zealand user were to be entitled to be set in the same terms as that of Americans? Is it disruptive to have these people use American servers?(Carissa Mangahas)
~Well I'm not too sure why the US would find this as a threat, since the internet is, after all, spreading globally. I find it quite unfair that they made too much of a big deal about it, since it isn't even illegal in the first place.

Why is wrong with Netflix extending their access? (Stephanie Diaz)
~The thing is that Netflix is US-based. They only allow people in the US to view their programs. The reason why they don't extend their access in not only due to economic impact, but they must also take into account that they need consent from the owners of the content. This is a tedious process that requires a lot of time and money. Therefore, Netflix only allows US users to view the content.

Is "global mode" banned by any other companies? (Ana Cisneros)
~Yes, "global mode" is a major issue. Several companies are currently in court regarding this issue and they're attempting to stop this.

Did netflix suffer from this incident? (Debbie Argueta)
~Netflix have not suffered from this, as far as I'm concerned, but since they aren't taking action into it yet, we're not sure of the entire situation of why the US finds this threatening. Netflix in the US gave

Why is this happening specifically in New Zealand? (Myra Pham)
~This is happening specifically in New Zealand because it is the New Zealand programmers that had started the accessing of the US-based Netflix in New Zealand, for their subscribers.

Why doesn't netflix just allow their services to other countries besides the U.S.? (Citlaly Moncada)
~The thing is that Netflix is US-based. They only allow people in the US to view their programs. The reason why they don't extend their access in not only due to economic impact, but they must also take into account that they need consent from the owners of the content. This is a

tedious process that requires a lot of time and money. Therefore, Netflix only allows US users to view the content.

How did Netflix find out about this? (Belcy)
~They recently traced several accounts to New Zealand by reversing the DNS trick and discovered that thousands of accounts were actually from New Zealand.

Does New Zealand not have their own website similar to the US version of Netflix?(Lissete)
What actions has Netflix taken against this act?(Morgan and Nava)
~Netflix has given a date for the programmers in New Zealand to stop this service. After that date, if the service continues, then the US may take action in a court, concerning this issue.

What are the profits from this act? Seems like Netflix would change their policy if it is a financial gain.
~This actually hurts their wallet due to the fact that Netflix has exclusive rights, meaning that the people who own the movies and shows that Netflix provides only gave them permission to provide this material to US users. The owners of the rights could sue Netflix for allowing international users to view this content and Netflix would end up paying millions in lawsuits.

Why is it against the outside of the United States? (Laura)
~The thing is that Netflix is US-based. They only allow people in the US to view their programs. The reason why they don't extend their access in not only due to economic impact, but they must also take into account that they need consent from the owners of the content. This is a tedious process that requires a lot of time and money. Therefore, Netflix only allows US users to view the content.

Why does netflix consider it still a threat? (John D.)
~Netflix considers this a threat due to the fact that it could cause them to lose a lot of money. Netflix has exclusive rights, meaning that the people who own the movies and shows that Netflix provides only gave them permission to provide this material to US users. The owners of the rights could sue Netflix for allowing international users to view this content and Netflix would end up paying millions in lawsuits.