Kush, Steven, Hugo, Imraan, Sandeep

|  |  |  |
| --- | --- | --- |
|  | **Activity - Internet Research: DNS in the Real World** |  |

**Directions:**

Carefully read and analyze your resource with your group at the bottom of the page. After you have finished you will share your analysis with other members of the class as directed by your teacher.

**Resource:** https://www.scmagazine.com/home/security-news/ddos-attacks-against-nato-likely-dns-amplification-or-ntp-reflection-expert-suggests/

|  |
| --- |
| **Summary:**  A massive DDoS attack nearly took out all NATO websites. Only informational websites of NATO were hit because just like other organizations, (like NATO) they have networks for high priority operations, that are not traditionally connected to the rest of the internet. The simple attack according to Prince were basically filling a pipe with requests that makes the routers unstable. Considering this attack was a volume DdoS attack, it shouldn’t create any risk of sensitive dada being revealed. The group that is responsible for this attack goes by the name “Cyber Berkut”. |
| **Key Points:**   * NATO fell under a DdoS attack by a group called “Cyber Berkut” * The attack was a “Volume DdoS” attack meaning that no crucial information was at risk of being revealed * The way the hack worked is a “pipe” was filled with requests that rendered the routers useless/unstable      * Prince says that although the attack is harmless, just to be safe, make sure your computers are not running any vulnerable systems that can be used to attack other systems |
| **Other Facts:** The attack peaked shy of 400 gb/s. |

**Jigsaw**

Join a new group as directed by your teacher and share what you each learned. Record the name of the topic and the key points of interest shared with you in the space below.

|  |  |  |
| --- | --- | --- |
| **Name: Joshua** | **Name: Carlos** | **Name: Faris** |
| **Key Points:**  **-Google and Lenovo was attacked**  **-the attackers name was “Lizard Squad”**  **-Every time google or Lenovo was searched up, it would redirect to an image of a boy in a room and the audio playing Walt Disney music**  **-The hack was a type of “Domain hijacking” that switches domain name and adress to another page**  **-This type of hack is dangerous as it could lead people to fake websites where malicious software would be downloaded** | **Key Points:**  **-DNS was overlooking attacks on their systems instead of protecting it**  **-they didn’t take responsibility for their DNS security**  **- The hackers sent a lot of self-duplicating files and in enough time, they were able to take over that network**  **-To stop these attacks, they cut off the bandwidth to other networks in places like China, Japan etc.** | **Key Points:**  **-2 ways to make a DdoS attack**  **-1) make multiple computers attack all in one area**  **-2) send a lot of requests in order to create a lot of traffic in the network paths**  **-Companies have multiple data centers so that incase of an attack, there are multiple servers to distribute the traffic.** |

|  |  |  |
| --- | --- | --- |
| **Name: Chen** | **Name: Hacqueem** | **Name:** |
| **Key Points:**  **-A video game company was under attack from mostly China and India**  **-This happened from millions and millions of requests being sent per second**  **-this caused the servers to slow down** | **Key Points:**  **-DdoS attacks aim to slow down the CPU performances**  **-These attacks can come from one source or multiple sources but aim to do the same thing**  **-If the website you are on is slowing down significantly and you know it is not of your doing, that means you are probably under attack**  **-for small scale attacks, you can find the IP address and block them**  **-Larger scale attacks will need the help of a third party IT specialist** | **Key Points:** |

|  |  |  |
| --- | --- | --- |
|  | **Articles List** | Name(s) |
| 1 | Growing Threat of DDoS on DNS  <http://www.information-age.com/technology/security/123459033/growing-threat-ddos-attacks-dns> | Nathaly,Tony, Carlos, Ulisses, Thomas |
| 2 | The Details Behind a Denial of Service Attack: What it is, Why it Matters, and What You can do to Stop it  <http://www.business2community.com/tech-gadgets/the-details-behind-a-denial-of-service-attack-what-it-is-why-it-matters-and-what-you-can-do-to-stop-it-01241089> | Nirujan, Hacqueem,Karanjeet, Aqueel, Warren |
| 3 | How to Launch a 65Gbps DDoS, and How to Stop One  <https://blog.cloudflare.com/65gbps-ddos-no-problem/> | Ji Yun, Earl, Xuelin(Faris), Pouyan,, Brian, Tyler |
| 4 | How DNS Works  <http://www.pcworld.com/article/2889392/like-google-in-vietnam-lenovo-tripped-up-by-a-dns-attack.html> | Noah, Joshua Salema, Joshua Salituro, Jainam, Derriffe, Paolo |
| 5 | DDoS Attacks Against NATO Likely DNS Amplification or NTP Reflection, Expert Suggests  https://www.scmagazine.com/home/security-news/ddos-attacks-against-nato-likely-dns-amplification-or-ntp-reflection-expert-suggests/ | Imraan, Hugo, Kush, Steven, Sandeep |
| 6 | DNS Flood DDoS Attack Hit Video Gaming Industry with 90 Million Requests per Second  <http://thehackernews.com/2014/06/dns-flood-ddos-attack-hit-video-gaming.html> | Gurbhinder, Hiral, Semra, Chen, Vaasu |

**Note: Submit worksheet ‘IP Address’ from previous class homework along with this lab2.**

**Rubric for DNS Research**

|  |  |  |  |
| --- | --- | --- | --- |
| **Categories** | **Level 1** | **Level 2** | **Level 3** |
| **Knowledge and Understanding of DNS issues:** |  |  |  |
| Clearly explains main idea of given DNS Article and by focusing on main aspects student records key points of the issue.  Adequately presents measures to control the attack | **Some part** | **Almost** | **Does a good job** |
| **Collaboration** | Students was highly collaborative and worked efficiently |  |  |
| **Completion of Worksheet – IP Address** | Completed with high degree of understanding |  |  |