2024 年【科學探究競賽-這樣教我就懂】

大專/社會組　科學文章表單

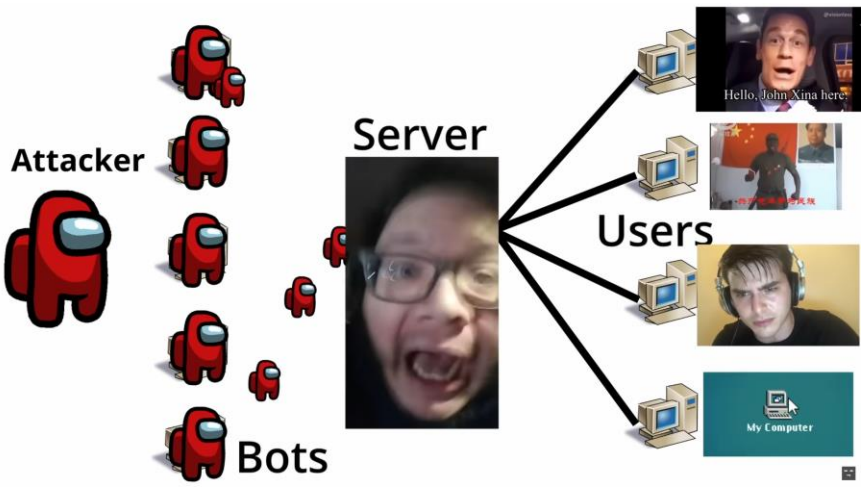
文章題目： DDOS 技術簡介

摘要：介紹 DDOS 網路攻擊原理與其演變

文章內容：（限 500 字~1,500 字）

任何一個安全的網路系統都存在一個不安全的隱患那就是 DDOS。為何 DDOS 存在已久卻無法徹底解決？DDOS 的運作原理到底是什麼，駭客們與資安專家們圍繞著 DDOS 的攻防戰是如何進行的呢？

再了解 DDOS 攻擊之前我們要先了解它的原始型態 DOS(Denial of Service)”拒絕服務”，DOS 攻擊是藉由對單一伺服器的大量訪問霸佔網路資源，使伺服器無法回覆其他正常使用者的訪問。然而若只在同一個設備上發動攻擊伺服器則能夠直接封鎖攻擊者的網路 IP，因此駭客們改良了原先的 DOS 攻擊，創造出來的就是我們的主角 DDOS(Distributed denial of Service) “分布式拒絕服務”，他的不同點在於攻擊者一次使用大量的設備進行 DOS 攻擊，我們可以簡單的理解為”群毆”。



(圖一) DDOS 攻擊式意圖

DDOS 的攻擊需仰賴大量設備，這些設備可以式電腦、伺服器、甚至是你的手機，這些設備之間相互會組成一個網路，我們一般稱它為殭屍網路(BotNet)，並且稱每個設備為一個殭屍。

假設現在你是一個攻擊者，那麼問題來了，你該怎麼組建你的殭屍網路呢？這個問題有很多種答案，每種答案也有他們適合的受眾。

1. 利用走後門的惡意軟體如：釣魚、木馬、蠕蟲等程序感染大量設備。這種方法適合技術高超的駭客或是你所擁有的資金不多時。
2. 直接花錢購買殭屍網路，理論上花費的多寡與殭屍網路的規模呈正相關，也就是說你花的錢越多你所得到的殭屍網路就越大攻擊力也越強。

現在我們有了殭屍網路但是在攻擊前我們還需要先了解一下網路是怎麼傳遞的，現在的網路傳輸大多是藉由 TCP/IP 協議進行傳輸的，這種協議在正式傳遞資料之前會使用固定的方法進行三次的身分確認，也就是確認你有找對訪問的對象，網路傳輸我們可以用生活中常見的東西來理解，網路的傳輸可以看成是郵局將信件送至目的地，而網路中也有收件地址與送件地址，也就是 IP 地址，攻擊者只需要偽裝好自己的 IP 地址就能夠避免被追蹤，就算這些殭屍網路中的設備的 IP 地址被禁止也無所謂，因為大部分殭屍網路中設備的使用者其實督不知道自己是中的一員。

DDOS 是一種歷史悠久的網路攻擊方法，它的原理極為簡單粗暴，也正因為如此它難以根治，它並不是一種複雜的算法，也沒有利用什麼漏洞，因此難以利用修復漏洞去避免它發生，我們每個人都應該注意不要成為殭屍網路的一員，不要輕易點擊可疑網站，說不訂你就變成殭屍網路的一員。

參考資料

DDOS 技術鑑賞

https://youtu.be/7kB9-nQJR44?si=t6dZ0k9qW3iFrEh6

圖一 How DDoS Works

https://youtu.be/r3bEjsv9JFw?si=9cEIzvTmxdeft1vm

DDOS 攻擊定義，防護策略與三手法

https://www.cloudflare.com/zh-tw/learning/ddos/what-is-a-ddos-attack/