Rodrigo K. A. M.

IT19001180

ICS Lab 3 - Learning the Details of Attacks

2016 Dyn Cyberattack

Mirai botnet took place in October of 2016. It is still ranking as the largest DDOS attack ever launched. The target was a DNS provider Dyn. The attakcers attacked this using a botnet of IoT devices (a botnet is a number of internet connected devices each of which is running one or more bots. A bot is a software that runs automated tasks/ scripts over the internet). It managed to cripple Dyn servers and brought huge sections of the internet down. Twitter, Netflix, Reddit and CNN were affected. Attackers used Mirai malware to infect connected devices. Once it successfully infected a vulnerable IoT gadget automatically searched the internet for other vulnerable devices. Whenever it found one the malware used the default name and password to login into device, install itself and repeat the process.

a) According to researches outdated firmware or weak default passwords which made them vulnerable and easy to hack.
b) New world hackers and anonymous are the suspects for this attack. According to Dyn, DDoS attack began at 7.00 a.m. and was resolved by 9.220 a.m. The second attack was reported at 11.52 a.m. and internet users began reporting difficulties accessing websites. A third attack began in the afternoon, after 4.00 p.m. At 6.11 p.m. Dyn reported that they had resolved the issue.
c) Vulnerabilities are unintended flaws found in software programs or operating systems. Vulnerabilities can be the result of improper computer or security configurations and programming errors. If left unaddressed vulnerabilities create holes that cybercriminals can exploit. Because of outdated software/firmware, weak passwords and etc, vulnerabilities are made.
d) Update firmware, software

   Creating strong passwords

   Employ a Security Services Lifecycle Approach

   Authenticate

   Encrypt the important stuff

   Proper patch management

   Content filtering should be policy driven