How to DDOS

like a script kiddie

Vocabulary

Script kiddie: a person who uses existing computer applications or code to hack, lacking the expertise to write their own.

DOS: Denial of service, meaning one computer is sending an excessive amount packets to take down a network.

DDOS: Distributed Denial of Service, multiple computers sending an excessive amount of packets to collectively together take down a network or work towards another goal.

ISP: Internet service provider.

Why is DDOS so popular?

From now on I will refer to both DOS and DDOS as DDOS just for simplicity's sake. DDOS is a very popular method of attacking due to its effectiveness and its' extreme simplicity. The simplicity to DDOS someone also contributes to the fact why it is so popular among the gaming community.

Meat and potatoes.

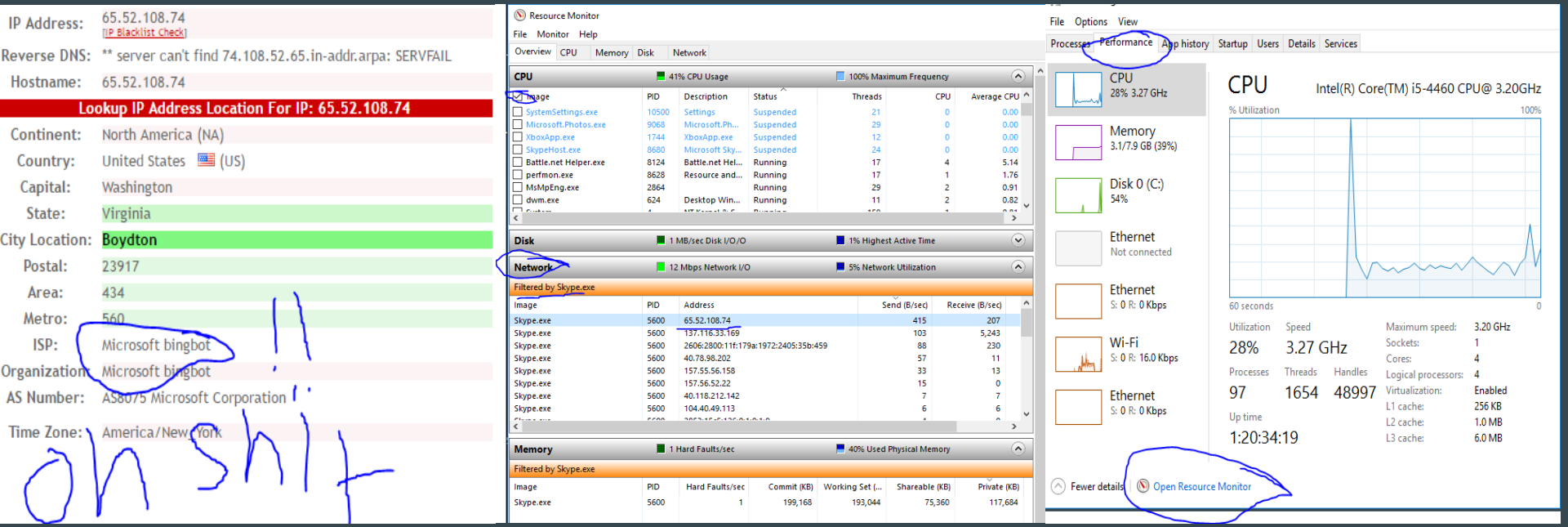
How to grab an IP address, getting the IP address of a network you want to attack is the first and most important step of attempting a DDOS attack.

Clickbait method: Visit this website(http://whatstheirip.com/) type in your email address it will give you a choice of a few links that you need to clickbait people into... clicking. This method requires a wee bit of social engineering. For example you tell the person “Hey I found this forum post about you, hahaha it’s pretty funny!! Do you know these people or something?” This type of sentence really peaks the interest of someone, increasing the chance of them clicking on it.

Meat and potatoes p2

The second method is to use a network monitor. An easy and free network monitor to grab IPs is built right into windows administrative tools!! First open task manager, go to performance, then go to resource monitor, go to network, then click on the application you want to filter on. Next click on sent bytes, try spamming messages to the target, if you see an increase in sent bytes next to an ip address, write down the IP address, then double check the target's IP address by location and more importantly ISP. Go to http://www.ip-tracker.org/ type in the IP address, look at the ISP, if you haven't heard of the ISP google it, make sure the ISP isn't known for hosting VPNs or other security measures.

Screenshot


IP Address: 65.52.108.74
[IP Blacklist Check]
Reverse DNS: ** server can't find 74.108.52.65.in-addr.arpa: SERVFAIL
Hostname: 65.52.108.74
Lookup IP Address Location For IP: 65.52.108.74
Continent: North America (NA)
Country: United States (US)
Capital: Washington
State: Virginia
City Location: Boydton
Postal: 23917
Area: 434
Metro: 560
ISP: Microsoft bingbot
Organization: Microsoft bingbot
AS Number: AS8075 Microsoft Corporation
Time Zone: America/New_York
Resource Monitor
File Monitor Help
Overview CPU Memory Disk Network
CPU 41% CPU Usage 100% Maximum Frequency
Disk 1 MB/sec Disk I/O/O 1% Highest Active Time
Network 12 Mbps Network I/O 5% Network Utilization
Filtered by Skype.exe
Memory 1 Hard Faults/sec 40% Used Physical Memory
Filtered by Skype.exe
File Options View
Processes Performance App history Startup Users Details Services
CPU 28% 3.27 GHz
Memory 3.1/7.9 GB (39%)
Disk 0 (C:) 54%
Ethernet Not connected
Ethernet S: 0 R: 0 Kbps
Wi-Fi S: 0 R: 16.0 Kbps
Ethernet S: 0 R: 0 Kbps
CPU Intel(R) Core(TM) i5-4460 CPU@ 3.20GHz
% Utilization 100%
60 seconds 0
Utilization 28%
Speed 3.27 GHz
Processes 97
Threads 1654
Handles 48997
Up time 1:20:34:19
Maximum speed: 3.20 GHz
Sockets: 1
Cores: 4
Logical processors: 4
Virtualization: Enabled
L1 cache: 256 KB
L2 cache: 1.0 MB
L3 cache: 6.0 MB
Fewer details
Open Resource Monitor

Analyzing the IP address

Based on the information provided by http://www.ip-tracker.org/locator/ip-lookup.php?ip=65.52.108.74
It tells us that the IP originates from microsoft bingbot! WE DO NOT WANT TO ATTACK THIS ADDRESS! This address is covered by microsoft, hitting it will be a waste of time, but do not worry if you do, no legal action will be pressed on you. (I know from experience).

Now it's time for the attack

Once you have the IP address, go to Ipstresser.com which is a decent online booter. You can choose which ports and attack methods to use against the IP. The typical port for HTTP connections is port 80. You can use multiple attacks and different methods V.S. the same target to maximize your range and effectiveness of attacks. After the attack has been going for two minutes go to http://ping.eu/ping. If the pings have no reply that means the skid is offline!

Additional information

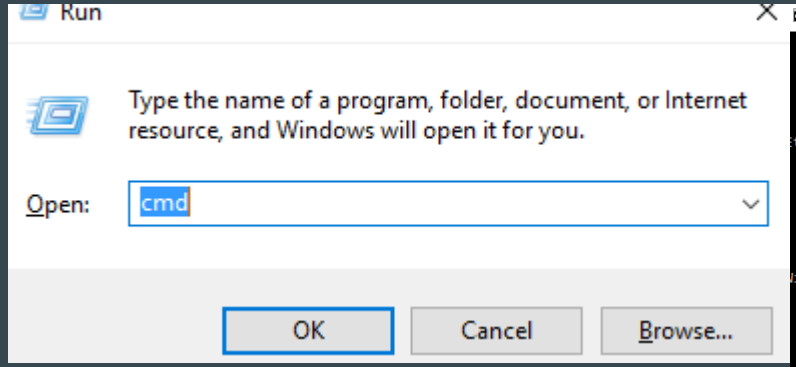
Combining other booters and DDOS methods will maximize the attack try using other free booters to hit off the target, although one should be way more than enough for any home network.

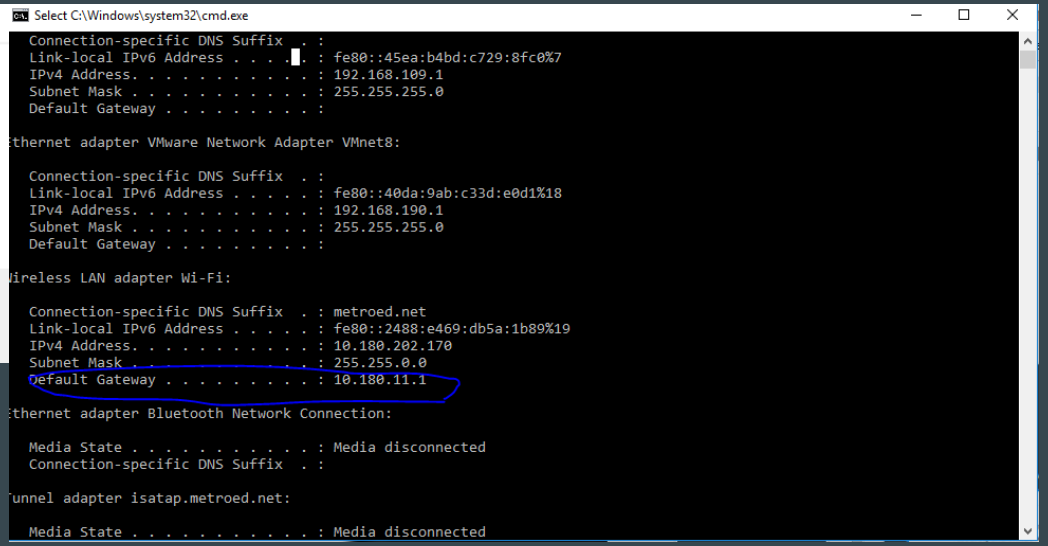
Stopping a DDOS attack on a home network?!

Stopping a DDOS attack on a home network is nearly impossible, the only way to stop it is to unplug your router.... Which fulfills the want of the attacker.
You may be able to lessen the income of packets, by going to CMD, type in Ipconfig, look for the default gateway, next type in the IP address of the default gateway into your browser, search the web for the default username and password, afterwards you need to look around in the advanced firewall setting for something related to packet filter. This is different for each ISP and I'm not getting enough extra credit to provide steps for all the most popular ISPs.

How to get to router configuration

Press the windows key+R, type in CMD press enter, then search for default gateway.





Prevention is key

If you can prevent a script kiddie from gaining your IP, then they can't DDOS you. The best way to do this is to enable a VPN whenever clicking on suspicious links, also whenever using applications that connect users together directly, they can grab your IP. All in all investing a little bit of money in a dependable VPN is worth it. Example of free VPNs are Cyberghost, Tunnelbear, VPN Gate, and Hide Me. Please note that before using any of these VPNs do some research about what data they gather about the users.

Questions, comments, critiques, memes?