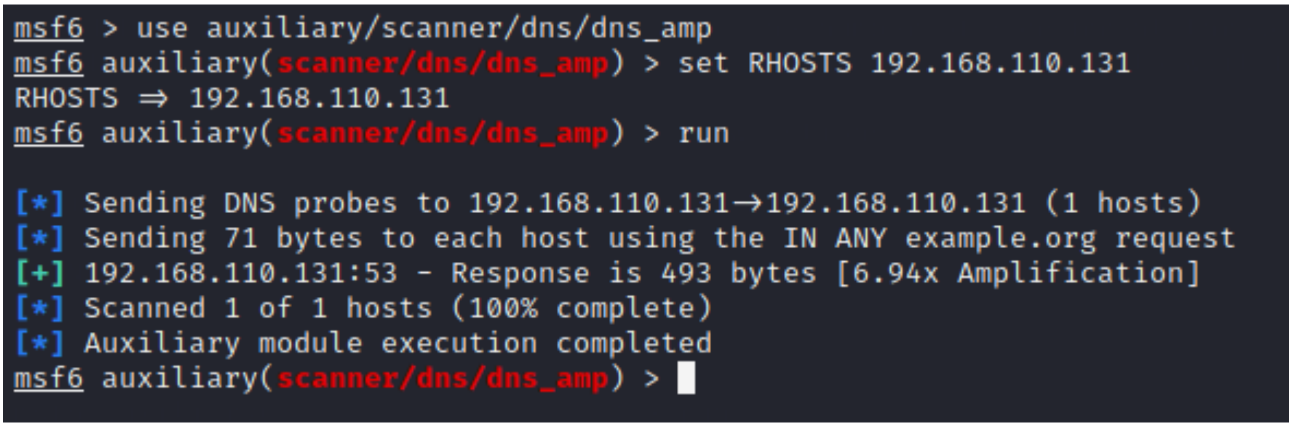
F21AN Group Report - DNS Amplification Attack

Note on Contributions: Both Matthew and Cal ran the DNS Amplification Exploit together before splitting up the work. Cal focused on preparing the script and recording the video. Matthew focused on writing the report. All work was collated and peer reviewed in the final week before submission. The demo used a Metasploit module to discover a virtual DNS server and expose recursive name lookups, which could be used in the amplification attack. Virtual Machines, running Kali Linux, acted as the DNS server; attacker; and victim.

Denial of Service (DoS)[1] is an attack that renders a network's resources unavailable by flooding the system with requests, and thus preventing it from serving legitimate users. Distributed DoS (DDoS)[1] increases the effectiveness of this attack as malicious requests are sent from multiple distributed sources. With these attacks becoming ever larger and more prevalent[2], it is important to understand what they are, the forms they take and how they can be mitigated. A popular form of DDoS attack is Domain Name System (DNS) amplification, which will be the focus of this report.

A DNS amplification attack achieves the same results as a standard DDoS attack, with the only difference being the larger-sized packets that are used to fill the victim's bandwidth[3]. An attacker exploits DNS protocols to use it as an intermediary system, with the ultimate goal being to flood the victim with lookup requests which will consume their network bandwidth to the point of failure[4].

When a user makes a standard HTTP request, the DNS accepts that request, finds the IP address linked to the given domain name, and sends the IP back to the user so that they can connect to the website. When performing an IP lookup, the user's device first checks its local cache for the address, and if not found, then queries their Internet Service Provider's (ISP's) DNS resolver[3]. If no address is found, then the request proceeds through a hierarchy of DNS resolvers until the IP address is found. There are numerous open and publicly accessible DNS resolvers in this hierarchy that can used by anyone to resolve requests[5]. Using these open resolvers, attackers can create a flood of fake requests without encountering any mitigation.



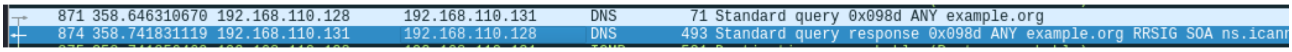
```
msf6 > use auxiliary/scanner/dns/dns_amp
msf6 auxiliary(scanner/dns/dns_amp) > set RHOSTS 192.168.110.131
RHOSTS ⇒ 192.168.110.131
msf6 auxiliary(scanner/dns/dns_amp) > run

[*] Sending DNS probes to 192.168.110.131→192.168.110.131 (1 hosts)
[*] Sending 71 bytes to each host using the IN ANY example.org request
[+] 192.168.110.131:53 - Response is 493 bytes [6.94x Amplification]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/dns/dns_amp) > █
```

Demo Figure 1: Metasploit probing the DNS server running on 110.131, and getting a response at an amplification factor of 6.94.

A standard DNS request is normally only around 24 bytes[6] in size and returns a response that is not much bigger than this. An attacker creates their malicious DNS request in such a way as to increase the size of the response as much as possible, for example, by requesting not just an IP address but all information on the domain and its subdomains. A 10-byte DNS request could then generate a response at an amplification factor of 10, 20, 50, or 100 times[7]. A single computer making malicious DNS requests (DoS rather than DDoS) and using just 100 Kb/second of bandwidth can send 2000 DNS requests/second. A typical distributed series of computers can send hundreds of thousands of DNS requests/second. A series of 10,000 endpoints controlled by an attacker, again using 100 Kb/second of bandwidth, each attacking the same IP address at an amplification factor of 60 would send 60 Gb/second of DNS responses to a victim[8].

DNS responses are typically sent over the User Datagram Protocol (UDP) for the benefit of speed and to reduce the overall load on the DNS. This protocol does not guarantee delivery or validate request data - it simply sends messages between sources and destinations before forgetting about them. It is also a connectionless protocol so it has no way of knowing if the source IP address in a request is valid[9]. When an attacker makes a malicious DNS requests, they replace the source IP address with that of the victim's. This strategy both hides the attacker's identity and ensures that all responses from the DNS resolver will be sent to the victim's system instead of the attacker's. In this way, the DNS resolvers are acting as reflectors, "returning" responses to a victim that didn't originally make the request[10].

While the attacker can successfully amplify DNS responses, if any packet reaches a certain upper size threshold, UDP will fragment that packet into smaller ones[9]. The result is still the same—the victim's system will still be overloaded because it must handle all of those fragmented packets and reassemble them, however it may take longer for the victim's bandwidth to reach maximum capacity.



```
871 358.646310670 192.168.110.128      192.168.110.131      DNS       71 Standard query 0x098d ANY example.org
874 358.741831119 192.168.110.131      192.168.110.128      DNS      493 Standard query response 0x098d ANY example.org RRSIG SOA ns.icann
```

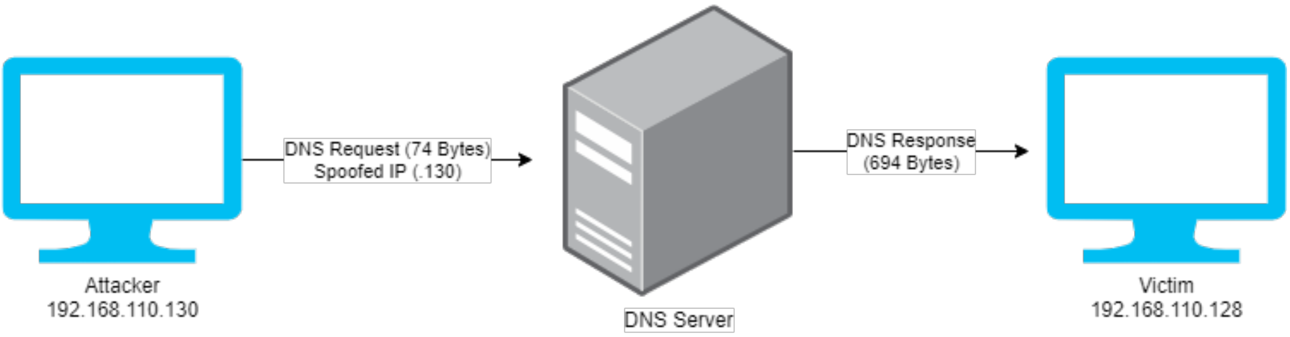
Demo Figure 2: Amplification packets, including the src; destination addresses; and size of the packets. Metasploit is running on 110.130 and the source IP has been spoofed with IP tables to be 110.128, hence why the packets have src IP as 110.128 and are returned to 110.128.

The DNS resolvers that are most vulnerable tend to have some misconfigurations in their access controls that leave them open to exploit. This includes limited or no access controls, or a local resolver that may have been unintentionally exposed to the internet. "Memcached" servers are notable for being particularly vulnerable due to their typical amplification factor - a possible 51000 times the spoofed request[4][17].

As with any DDoS attack, it is easy to detect a DNS amplification attack due to the volume of requests that will be sent to the victim. This attack is much harder to mitigate than detect because the victim receives responses from a legitimate resolver, and blocking this resolver could directly affect other user functions. The challenge is to distinguish legitimate user workloads from reflected traffic. In many cases, a victim's service will see an increase in legitimate user traffic because of repeat requests in response to its sluggish response. These retries can be mistakenly seen as part of the DoS behaviour[11].

There are a variety of strategies potential victims of DNS amplification attacks can run to protect their services. These include increasing server security, blocking some or all open and publicly accessible DNS resolvers, and limiting connection rates. These strategies do not, however effective, eliminate the source of an attack or reduce potential load on a network. Additionally, blocking all traffic from publicly accessible DNS resolvers can interfere with legitimate communication requests[10]. For example, some organisations create a publicly accessible DNS resolver to allow remote workers access to their Local Network. Remote workers can then resolve traffic from a "trusted" name server but blocking traffic from these servers can hinder that access[12][8].

Rate limiting can be applied to a request destination or to its source as a general method of DDoS mitigation. There is potential for collateral damage when implemented at a destination as this strategy cannot discern between legitimate and malicious messages; thus it should only be applied if no other mitigation strategy is effective and the system is at the point of failure. Rate limiting at a requests source is more effective as an access policy can help the system discern malicious requests from legitimate ones. For example, rate limiting, or UDP packet dropping, on a DNS resolver can block noisy request sources, such as an attacker, and reduce the impact of a DNS amplification attack[10][13].



Demo Figure 3: Demo Architecture

Another mitigation option against DNS amplification attacks is applying traffic signature filters, which are a common defence against any reflection attack. Reflection attacks can have identifiable repetitive structures in timing and packet construction, from which regular expressions can be derived and used as filters. These defence filters do, however, have to have the capacity to absorb data that passes through a network and the performance of regex expressions can be limiting - in software or hardware. Thus this mitigation may not be sufficient to stop a large DNS amplification attack with the potential to overwhelm the capacity of the filter[10][13].

Blocking unused network ports is another good security practice, however defending ports that are open to all internet traffic is more of a challenge. A DNS resolver tends to send responses to port 53 which must thus remain open to legitimate and malicious users, making it a common point of attack. Blocking this port would have the same effect as a DoS attack on all clients in the network that rely on this port[15].

Attackers are continuously scanning the internet, looking for DNS resolvers in the public hierarchy that they can use in their DNS amplification attacks. The servers that are vulnerable to being used in attacks can easily be found because intelligence companies keep a public list of them. These records are kept because blocking known vulnerable IP addresses is a highly effective, proactive mitigation strategy. The list is updated using reputation as a determining factor for blocking traffic however the challenge comes in blocking the millions of IP address records on all vulnerable machines[16]. For example, after the Spamhaus DNS amplification attack in 2013 which reached a size of 300 Gb/second, efforts were made to block any and all DNS resolvers that sent responses to unauthenticated DNS requests with the type “ANY”. Many of the DNS IP addresses of the servers that were vulnerable to abuse then continue to be available for access. A10’s DDoS threat intelligence map identifies about 4 million servers that are still vulnerable and being used in DNS reflected amplification attacks today[3].

The DNS is one of the key technologies that all network devices are reliant upon in order to connect to the internet. However, through this report, we have demonstrated that DNS is a tempting target for attackers to launch a relative amplification attack. The report raises a number of potential vulnerabilities in publicly accessible DNS resolvers, such as no access control policy or unintentional exposure to all internet traffic, that are still prevalent today. With the right mitigation strategy however, the impact of any potential threat can be substantially reduced. Therefore it is reliant upon all organisations that are dependant upon such servers to assess the defence strategies in place and be aware of the potential impact that any DNS amplification attack could have upon their service.

References

[1] Mirkovic, J. and Reiher, P., 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), pp.39-53.

[2] Vlajic, N. and Zhou, D., 2018. IoT as a land of opportunity for DDoS hackers. *Computer*, *51*(7), pp.26-34.

[3] Kim, S., Lee, S., Cho, G., Ahmed, M.E., Jeong, J.P. and Kim, H., 2017, September. Preventing DNS amplification attacks using the history of DNS queries with SDN. In *European Symposium on Research in Computer Security* (pp. 135-152). Springer, Cham.

[4] Gupta, V. and Sharma, E., 2018, September. Mitigating DNS Amplification Attacks Using a Set of Geographically Distributed SDN Routers. In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 392-400). IEEE.

[5] Park, J., Khormali, A., Mohaisen, M. and Mohaisen, A., 2019, June. Where are you taking me? behavioral analysis of open dns resolvers. In *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 493-504). IEEE.

[6] Liu, C., Dai, L., Cui, W. and Lin, T., 2019, October. A Byte-level CNN Method to Detect DNS Tunnels. In *2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)* (pp. 1-8). IEEE.

[7] Sehgal, A. and Dixit, A., 2019. Securing web access—dns threats and remedies. In *Emerging Trends in Expert Applications and Security* (pp. 337-345). Springer, Singapore.

[8] Tripwire, I., 2021. *DNS Amplification - Protecting Unrestricted (Open) DNS Resolvers*. [online] The State of Security. Available at: <https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/dns-amplification-protecting-unrestricted-open-dns-resolvers/> [Accessed 15 February 2021].

[9] Hercog, D., 2020. UDP Protocol. In *Communication Protocols* (pp. 337-339). Springer, Cham.

[10] Rajendran, B., 2020, February. DNS amplification & DNS tunneling attacks simulation, detection and mitigation approaches. In *2020 International Conference on Inventive Computation Technologies (ICICT)* (pp. 230-236). IEEE.

[11] Ahmed, M.E., Kim, H. and Park, M., 2017, October. Mitigating DNS query-based DDoS attacks with machine learning on software-defined networking. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)* (pp. 11-16). IEEE.

[12] Weimer, F., 2005, April. Passive DNS replication. In *FIRST conference on computer security incident* (Vol. 98).

[13] Wong, C., Bielski, S., Studer, A. and Wang, C., 2005, September. Empirical analysis of rate limiting mechanisms. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 22-42). Springer, Berlin, Heidelberg.

[14] Thomas, M. and Mohaisen, A., 2014, April. Kindred domains: detecting and clustering botnet domains using DNS traffic. In *Proceedings of the 23rd International Conference on World Wide Web* (pp. 707-712).

[15] Fachkha, C., Bou-Harb, E. and Debbabi, M., 2014, March. Fingerprinting internet DNS amplification DDoS activities. In *2014 6th International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-5). IEEE.

[16] Osterweil, E.M., McPherson, D.R., Thomas, M.A. and Chen, Q.A., Verisign Inc, 2020. Detecting and remediating highly vulnerable domain names using passive DNS measurements. U.S. Patent 10,652,271.

[17] Singh, K. and Singh, A., 2018, October. Memcached DDoS exploits: operations, vulnerabilities, preventions and mitigations. In *2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)* (pp. 171-179). IEEE.