



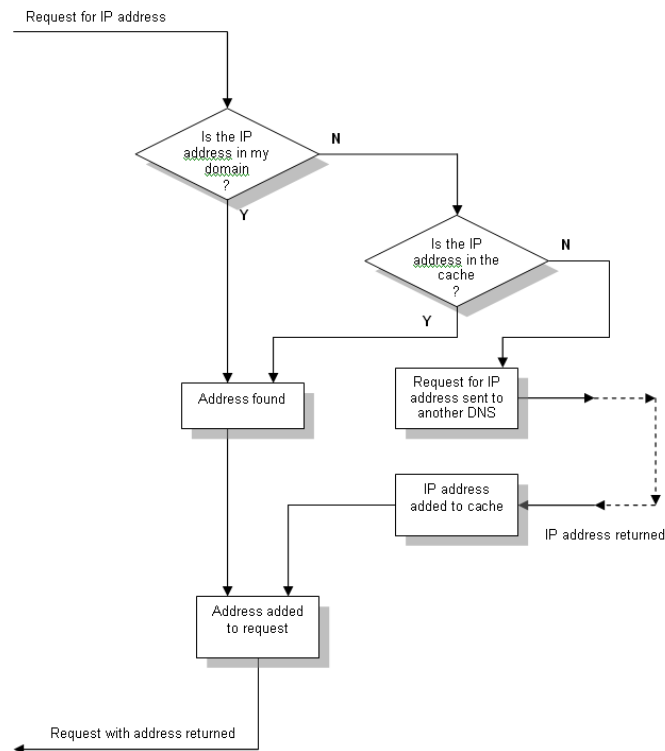
Chapter 7

DNS Attacks

The Domain Name Service (DNS) is a mechanism for recognizing and translating domain name addresses. These operations are carried out by devices called Domain Name Servers. Thus, DNS attacks are attacks against the Domain Name Servers.

As human beings, we prefer to operate with addresses such as *www.auckland.ac.nz* rather than *130.216.96.3*. The numeric representation is harder for us to remember than a meaningful representation. However, the underlying protocols of the Internet prefer 1s and 0s. To help us, a DNS is used to map the domain name to the numeric equivalent address (i.e., www, ftp, e-mail, etc.) where a given server awaits our request. When a request is made to a given domain, the request is translated by the DNS, and the equivalent IP address of the host server is returned. Internet DNS servers are arranged in a distributed manner so that if one server does not have the mapping, it may request the mapping from other DNS servers. If the mapping is requested from another server, then the requesting server stores a cached copy of the mapping for a limited period of time to be used for providing subsequent queries. Figure 7.1 shows the logic of the DNS operation.

Figure 7.1: Logic of DNS operations



Launching an Attack

How can a DNS attack be launched? The DNS protocol has virtually no authentication method that provides a means to ensure the identity of both sides of a given transaction (i.e., the requesting client and the DNS server). In the headers of the DNS query and response, there is a 16-bit field that is used for the identification of a query. However, there is no way of determining if the returned message contains a real IP address or if the entire message was sent by a real DNS server. So the whole game is about convincing the DNS client that the received message is genuine. The query IP is generated (in this 16-bit field) sequentially, and predicting future values is trivial through monitoring the communications. When the next query is sent, an attacker can send an

2 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/dns-attacks/25671

Related Content

Victimology of Terrorism

Nika Chitadze (2023). *Global Perspectives on the Psychology of Terrorism* (pp. 122-135).

www.irma-international.org/chapter/victimology-of-terrorism/314671

Cyberwar: Its Psychological Impact on Employees and Consequences for Organizations

Sumbul Rafiand Nasheed Imtiaz (2023). *Handbook of Research on War Policies, Strategies, and Cyber Wars* (pp. 108-127).

www.irma-international.org/chapter/cyberwar/318499

Influence Strategy: Consistency and Legitimacy as Key Factors

Bryan Pickettand Mike Lingenfelter (2011). *International Journal of Cyber Warfare and Terrorism* (pp. 12-36).

www.irma-international.org/article/influence-strategy-consistency-legitimacy-key/69770

Malevolent Information Crawling Mechanism for Forming Structured Illegal Organisations in Hidden Networks

Romil Rawat, Sonali Gupta, S. Sivaranjani, Om Kumar C.U., Megha Kulihaand K. Sakthidasan Sankaran (2022). *International Journal of Cyber Warfare and Terrorism* (pp. 1-14).

www.irma-international.org/article/malevolent-information-crawling-mechanism-for-forming-structured-illegal-organisations-in-hidden-networks/311422

Cyber Terrorism Taxonomies: Definition, Targets, Patterns, Risk Factors, and Mitigation Strategies

Ali Al Mazari, Ahmed H. Anjariny, Shakeel A. Habiband Emmanuel Nyakwende (2016). *International Journal of Cyber Warfare and Terrorism* (pp. 1-12).

www.irma-international.org/article/cyber-terrorism-taxonomies/152231