第 9 回 IT ソフトウェア翻訳士認定試験

＜1 次試験＞　3 月 15（日）10：00〜15：00

問題 1・2 の両方について解答のこと。選択ではありません。

＜問題 1＞　全文を訳して提出してください。

Protecting Browsers from DNS Rebinding Attacks

4.1 Firewall Circumvention

A firewall restricts traffic between computer networks in different zones of trust. Some examples include blocking connections from the public Internet to internal machines and mediating connections from internal machines to Internet servers with application-level proxies. Firewall circumvention attacks bypass the prohibition on inbound connections, allowing the attacker to connect to internal servers while the user is visiting the attacker's Internet web page.

Spidering the Intranet. The attacker need not specify the target machine by IP address. Instead, the attacker can guess the internal host name of the target, for example **hr.corp.company.com**, and rebind **attacker.com** to a **CNAME** record pointing to that host name. The client's own recursive DNS resolver will complete the resolution and return the IP address of the target. Intranet host names are often guessable and occasionally disclosed publicly. This technique obviates the need for the attacker to scan IP addresses to find an interesting target but does not work with the multiple **A** record technique described in Section 3.1.

Having found a machine on the intranet, the attacker can connect to the machine over HTTP and request the root document. If the server responds with an HTML page, the attacker can follow links and search forms on that page, eventually spidering the entire intranet. Web servers inside corporate firewalls often host confidential documents, relying on the firewall to prevent untrusted users from accessing the documents. Using a DNS rebinding attack, the attacker can leverage the client's browser to read these documents and exfiltrate them to the attacker, for example by submitting an HTML form to the attacker's web server.

出展：Collin Jackson et al. Stanford University

＜問題 2＞　全文を訳して提出してください。

The recent spate of DDoS attacks made victims not only of their Web site targets but also of the computers that hackers mind-controlled into making the attacks

In early February, hackers used a form of denial-of-service (DoS) attacks --- distributed denial-of-service (DDoS) attacks --- to bring Yahoo, Amazon, CNN.com, ZDNet, and other prominent Internet sites to their knees. The media's widespread coverage of these attacks has made this common hacking technique a household phrase.

A DoS attack's objective is to deny a user access to some type of service. In most cases, a DoS attack uses one computer to inundate another computer with network traffic, specifically traffic that contains confusing messages that cause the victim computer to waste time and resources trying to understand what it has received. Ultimately, this data influx can jam the victim computer, which ties up its communication lines and blocks legitimate visitors.

A distributed DoS attack amplifies the basic DoS attack. In a DDoS attack, one computer instructs multiple computers to attack multiple networks, using them to mount a more powerful, coordinated attack. Like an ant colony in which the queen controls an army of zombie ants, one computer instructs an army of computers to attack the victim simultaneously. This type of attack can even bring down sites such as Yahoo, that are designed to handle high volume. An individual ant can't bring down a robust Web site, but an army of ants can. This recent development has established DoS and DDoS attacks as a critical security issue.

The media has focused on the victims, sites like Yahoo and Amazon. Yet it may be more illuminating to examine how hackers assemble an army of zombie ants.

One solution is to step back and recognize that the brute force approach to security won't scale. If you administer one or two machines, you can assign individuals to manually perform security steps, but as systems become larger, this strategy ceases to be viable.

出展：http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=839372&isnumber=18131