中央警察大學 106 學年度碩士班入學考試試題

所　別：資訊管理研究所
科　目：電腦犯罪與資訊安全

作答注意事項：

1.本試題共 4 題，每題 25 分；共 3 頁。
2.不用抄題，可不按題目次序作答，但應書寫題號。
3.禁用鉛筆作答，違者不予計分。

一、試申論電腦犯罪現場處理的內涵與注意事項。

二、解釋下列名詞：

1、溢波抗辯

2、Zero Day Attack

3、Setuid （Set user id）

4、數位憑證 （digital certificate）

5、Alternate Data Streams （ADS）

三、A Denial of Service (DoS) attack is an attempt to make a system unavailable to the intended user(s), such as preventing access to a website. This is accomplished when an attacker successfully consumes all available network or system resources, usually resulting in a slowdown or server crash. In Figure 1, a Reflection DDoS attack occurs when attackers spoof their IP address to pose as the intended victim and then send legitimate requests to legitimate public-facing servers. The responses to these requests are sent to the intended victim and originate from legitimate servers.

（一）Please translate the above paragraph into Chinese. （15 分）

（二）Whenever multiple sources are coordinating in the DoS attack, it becomes known as a DDoS. How can an administrator do to stop DDoS attacks? （10 分）

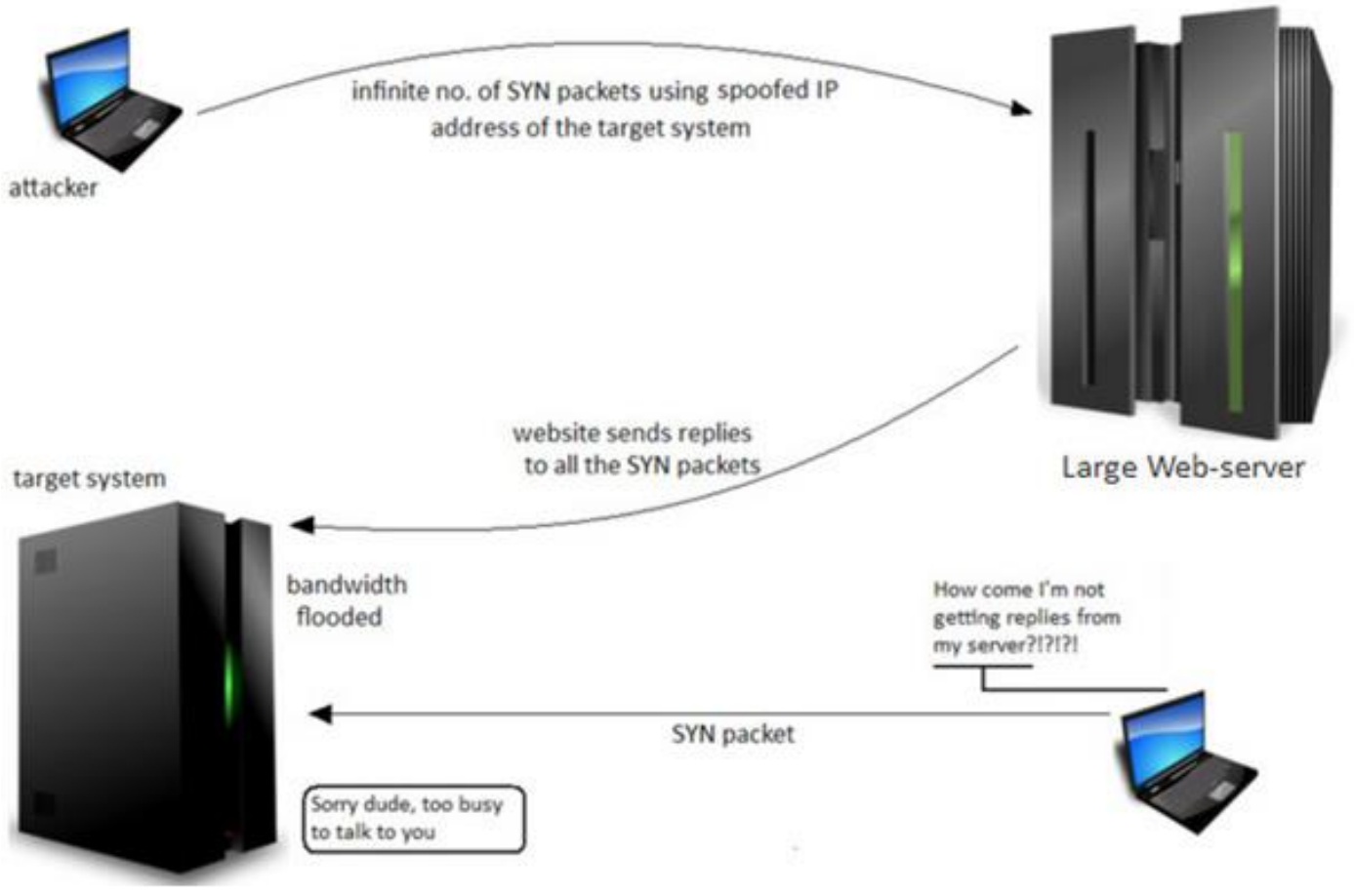

Figure 1: Reflection DDoS

四、The dark web is part of the Internet that is not accessible through traditional means. It requires that you use a technology like Tor (The Onion Router) or I2P (Invisible Internet Project) in order to access websites, email or other services. The deep web is slightly different. It is simply all of the web pages, or websites that have not been crawled by a search engine, is hidden behind paywalls or requires a username and password to access.

（一）Please translate the above paragraph into Chinese. （15 分）

（二）What kinds of principles or strategies are suitable for law enforcement agents to investigate dark web crime? Please draw a Table or Figure to explain it. （10 分）