1.) Describe each CVE in your own words. State its base score.

Answer: CVE 2014-0160/ Base score: 7.5. is a sort of buffer overflow attack. Dealing with Heartbeat Extension Packets and allows remote attackers to obtain sensitive information. CVE-2020-1350 / Base Score 10 is a remote code execution vulnerability that exists in the

WDNS servers and when they fail to properly handle requests.

2) .Copy the CVSS Vector of the CVE in your submission, and explain each category of the vector (e.g. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has an Attack Vector of "Network", Attack complexity of "Low", etc.).

Answer:

CVE-2020-1350

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): Changed

Confidentiality (C): High

Integrity (I): High

Availability (A): High

CVE-2014-0160

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Attack Vector (AV): Network

Attack Complexity (AC): Low

Privileges Required (PR): None

User Interaction (UI): None

Scope (S): UnChanged

Confidentiality (C): High

Integrity (I): None

Availability (A): None

Source: NVD. (n.d.). https://nvd.nist.gov/vuln/detail/cve-2014-0160