Packet Crafting

Prepared by:

William Zereneh
zereneh@scs.ryerson.ca
January 2010

Packet Crafting

What is Packet Crafting?

- The art of manually generating packets to test network devices
- Packets are crafted to test Firewall, IDS, TCP/IP Stack,....
- Auditing network protocols looking for vulnerabilities to exploit
- Find inconsistencies and poor network protocol implementations

Packet Crafting Composition

Packet Crafting consist of the following basic concepts:

- Packet Assembly; the creation of a packet
- Packet Editing; altering packet content
- Packet Re/Play; send packets onto network
- Packet Decoding; Analyse and interpret packet content

Packet Crafting Tools

Packet Crafting tools that will be covered:

- Packet Assembly: hping3
- Packet Editing: netdude
- Packet Re-Play: tcpreplay
- Packet Decoding: wireshark

Tools: hping3

hping is a network tool that is capable of creating and sending custom TCP/IP packets.

Useful for:

- A TCP/IP stack editing/auditing tool
- Advanced port scanning and OS fingerprinting
- Test network performance
- Path MTU discovery
- Traceroute using different protocols; TCP, UDP
- IP spoofing
- And lots more....

Tools: hping3 example 1

hping3 for spoofing IP addresses:

#>hping3 –a 222.222.222.222 –S –c 1 172.16.20.131

12:59:10.463614 IP 222.222.222.222.2897 > 172.16.20.131.0: S 1346470266:1346470266(0) win 512
0x0000: 4500 0028 c3be 0000 4006 38c1 dede dede
0x0010: ac10 1483 0b51 0000 5041 817a 4b4b 57ec
0x0020: 5002 0200 af4d 0000 0000 0000 0000

12:59:10.463679 IP 172.16.20.131.0 > 222.222.222.222.2897: R 0:0(0) ack 1346470267 win 0
0x0000: 4500 0028 0000 4000 4006 bc7f ac10 1483
0x0010: dede dede 0000 0b51 0000 0000 5041 817b
0x0020: 5014 0000 5472 0000

Tools: hping3 example 2

hping3 for setting bogus TCP flags: results

#>hping3 –SFPU –c 1 172.16.20.131 –p 0

13:05:31.827803 IP 172.16.20.134.1995 > 172.16.20.131.0: SFP 905984445:905984445(0) ack 428561220 win 512 urg 0
0x0000: 4500 0028 7b12 0000 4006 7e94 ac10 1486
0x0010: ac10 1483 07cb 0000 3600 39bd 198b 5344
0x0020: 503b 0200 4828 0000 0000 0000 0000

13:05:31.828067 IP 172.16.20.131.0 > 172.16.20.134.1995: R 428561220:428561220(0) win 0
0x0000: 4500 0028 0000 4000 4006 b9a6 ac10 1483
0x0010: ac10 1486 0000 07cb 198b 5344 0000 0000
0x0020: 5004 0000 ba1c 0000

Tools: hping3 example 3

hping3 for sending data and setting multiple TCP/IP options

#>hping3 –b –M 1234567890 –t 127 –X 172.16.20.131 –p 80 –d 54 –E evil.txt –c 1

-b: Bad checksum
-M: TCP sequence number
-t: TTL (Time-To-Live)
-X: Set Xmas TCP flag (All flags)
-p: Destination port
-d: Data size
-E: Filename contents to fill packet's data
-c: Number of packets to send

Tools: hping3 example 3 results

13:43:14.798430 IP (tos 0x0, ttl 127, id 10255, offset 0, flags [none], proto TCP (6), length 94) 172.16.20.134.2631 > 172.16.20.131.80: E 1234567890:1234567944(54) win 512

```
0x0000:  4500 005e 280f 0000 7f06 9261 ac10 1486      E..^(......a....
0x0010:  ac10 1483 0a47 0050 4996 02d2 1abc e0d8      .....G.PI.......
0x0020:  5040 0200 0b7d 0000 4556 494c 2054 7261      P@...}..EVIL.Tra
0x0030:  6666 6963 2e2e 2e2e 2e0a 0000 0000 0000      ffic............
0x0040:  0000 0000 0000 0000 0000 0000 0000 0000      ................
0x0050:  0000                                         ..
```

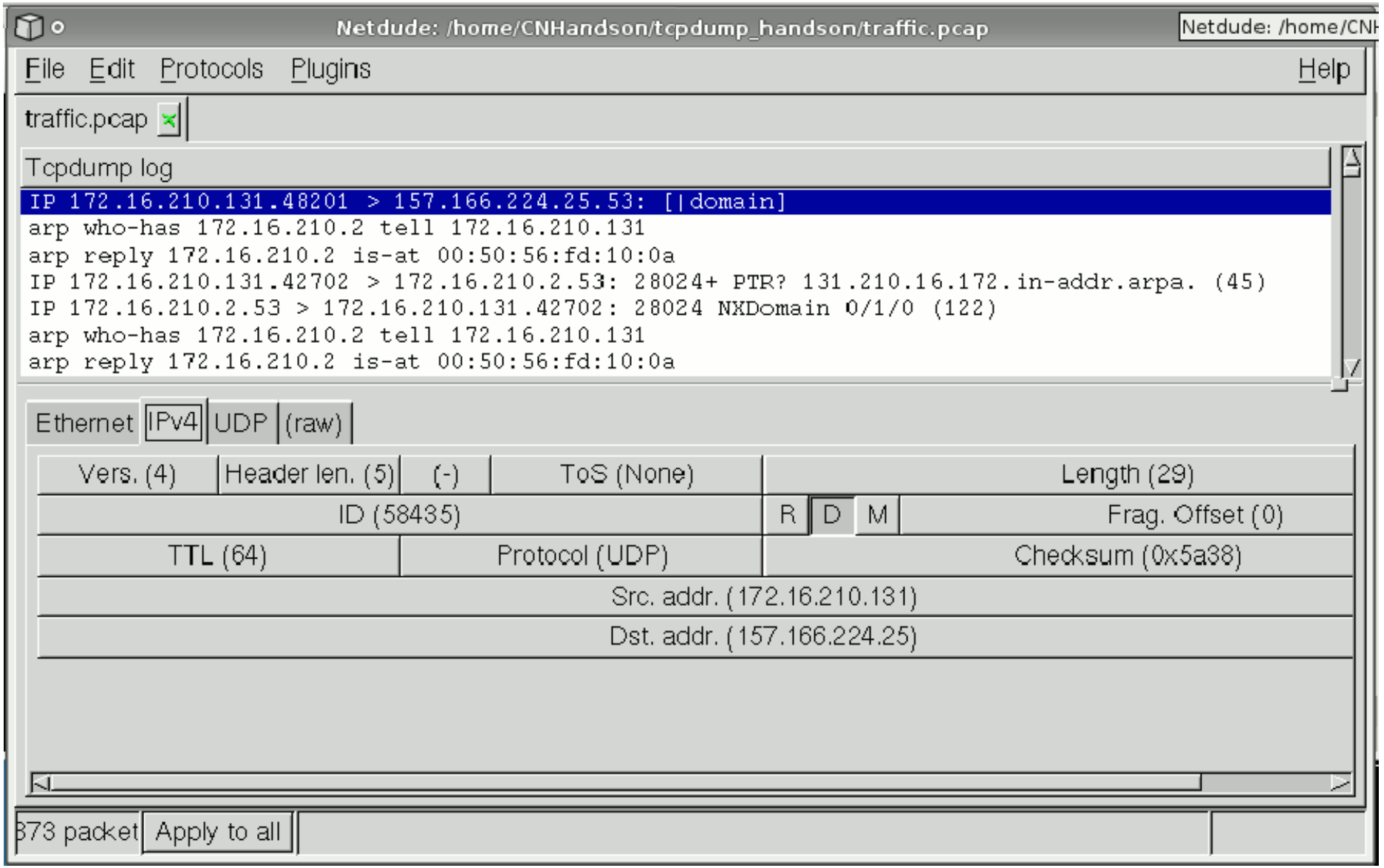
Tools: netdude

NETwork Dump data Displayer and Editor for tcpdump tracefiles

Useful for:

- Display and edit pcap binary files
- Change IP, TCP, MAC or any field in a packet
- Alter packet payload
- Fix checksums as needed.

Tools: netdude (DEMO)



Tools: tcpreplay

A tool to “replay packets back out onto the network from a pcap file”

- tcpreplay will replay back packets from a file at the same rate to which those packets were captured
- tcpreplay can re-send packets at different rates if specified
- Useful for testing Firewalls and IDS’s
- Replay packet at different rates to further test sniffer/IDS/Firewall stability and performance

Tools: tcpreplay example

#>tcpreplay -t --intf1=eth1 snort.pcap

sending out eth1
processing file: snort.pcap
Actual: 152 packets (11384 bytes) sent in 0.18 seconds
Rated: 613957.5 bps, 4.68 Mbps/sec, 8197.61 pps

Statistics for network device: eth1
Attempted packets: 152
Successful packets: 152
Failed packets: 0
Retried packets (ENOBUFS): 0
Retried packets (EAGAIN): 0

Tools: wireshark

A tool to “Interactively dump and analyze network traffic”

- wireshark can read/import many file formats.
  - Libpcap
  - snoop and atmsnoop
  - Shomiti/Finisar
  - Novell LANanlyzer
  - Microsfot Network Monitor captures
  - AIX’s iptrace captures
  - IPLog form Cisco Secure IDS
  - Many many more
- It can follow/reassemble all packets in a TCP conversation
- Display filters are extremely powerful

Packet Crafting References

- hping3 - http://www.hping.org
- Netdude - http://netdude.sourceforge.net
- tcpreplay - http://tcpreplay.synfin.net/trac
- wireshark - http://www.wireshark.org