

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

NAME

nemesis-tcp - TCP Protocol (The Nemesis Project)

SYNOPSIS

tcp [-v] [optlist]

DESCRIPTION

The Nemesis Project is designed to be a commandline-based, portable human IP stack for UNIX/Linux. The suite is broken down by protocol, and should allow for useful scripting of injected packet streams from simple shell scripts.

TCP Options

[-x Source Port]

Source Port of injected packet.

[-y Destination Port]

Target Port of injected packet.

-f TCP Flag Options (-fS/-fA/-fR/-fP/-fF/-fU) SYN, ACK, RST, PSH, FIN, URG

-w Window Size

TCP Window Size.

-s Sequence Number

TCP Sequence Number.

-a Acknowledgement Number

TCP Acknowledgement Number.

-u TCP Urgent Pointer

TCP Urgent Pointer.

-P Payload File

Filename to read for packet payload.

-v Verbose Mode

Display human readable output of currently injected packet.

IP Options

-S Source IP Address

Source Address of injected packet.

-D Destination IP Address

Target Address of injected packet.

-I IP ID

IP ID header tag.

-T IP TTL

IP Time To Live field.

-t IP tos

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

IP Type Of Service field.

-F IP frag

IP Fragmentation field.

-O IP Options

IP Options field.

Data Link Options

-d Ethernet Device

Name of ethernet device (eg. ne0, ed0, eth0).

-H Source MAC Address

Source MAC Address (XX:XX:XX:XX:XX:XX)

-M Destination MAC Address

Target MAC Address (XX:XX:XX:XX:XX:XX)

NAME

nemesis-udp - UDP Protocol (The Nemesis Project)

SYNOPSIS

nemesis-udp [-v] [optlist]

DESCRIPTION

The Nemesis Project is designed to be a commandline-based, portable human IP stack for UNIX/Linux. The suite is broken down by protocol, and should allow for useful scripting of injected packet streams from simple shell scripts.

UDP Options

[-x Source Port]

Source Port of injected packet.

[-y Destination Port]

Target Port of injected packet.

-P Payload File

Filename to read for packet payload.

-v Verbose Mode

Display human readable output of currently injected packet.

IP Options

-S Source IP Address

Source Address of injected packet.

-D Destination IP Address

Target Address of injected packet.

-I IP ID

IP ID header tag.

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

-T IP TTL
IP Time To Live field.

-t IP tos
IP Type Of Service field.

-F IP frag
IP Fragmentation field.

-O IP Options
IP Options field.

Data Link Options

-d Ethernet Device
Name of ethernet device (eg. ne0, ed0, eth0).

-H Source MAC Address
Source MAC Address (XX:XX:XX:XX:XX:XX)

-M Destination MAC Address
Target MAC Address (XX:XX:XX:XX:XX:XX)

NAME

nemesis-icmp - ICMP Protocol (The Nemesis Project)

SYNOPSIS

nemesis-icmp [-v] [optlist]

DESCRIPTION

The Nemesis Project is designed to be a commandline-based, portable human IP stack for UNIX/Linux. The suite is broken down by protocol, and should allow for useful scripting of injected packet streams from simple shell scripts.

ICMP Options

-i ICMP Type
Echo Reply (0), Destination Unreachable (3), Source Quench (4), Redirect (5), Echo Request (8), Router Solicitation (10), Time Exceeded (11), Parameter Problem (12), Timestamp Request (13), Timestamp Reply (14), Information Request (15), Information Reply (16), Address Mask Request (17), Address Mask Reply (18).

-c ICMP Code
DESTINATION UNREACHABLE: Network Unreachable (0), Host Unreachable (1), Protocol Unreachable (2), Port Unreachable (3), Fragmentation Needed (4), Source Route Failed (5), Destination Network Unknown (6), Destination Host Unknown (7), Source Host Isolated (8), Destination Network Administratively Prohibited (9), Destination Host Administratively Prohibited (10), Network Unreachable For TOS (11), Host Unreachable for TOS (12), Communication Administratively Prohibited By Filter (13), Host Precedence Violation (14), Precedence Cutoff In Effect (15).

REDIRECT: Redirect For Network (0), Redirect For Host (1), Redirect for TOS And Network (2), Redirect for TOS And Host (3).

TIME EXCEEDED: TTL=0 During Transmit (0), TTL=0 During Reassembly (1).

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

PARAMETER PROBLEM: IP Header Bad (0), Required Option Missing (1).

-s Sequence Number
ICMP Sequence Number.

-m ICMP Subnet Mask
ICMP Subnet Mask.

-G ICMP Preferred Gateway
ICMP Preferred Gateway.

-Co Time of Originating request
Time of Originating request.

-Cr Time request was Received
Time request was Received.

-Ct Time reply was Transmitted
Time reply was Transmitted.

-P Payload File
Filename to read for packet payload.

-v Verbose Mode
Display human readable output of currently injected packet.

IP Options

-S Source IP Address
Source Address of injected packet.

-D Destination IP Address
Target Address of injected packet.

-I IP ID
IP ID header tag.

-T IP TTL
IP Time To Live field.

-t IP tos
IP Type Of Service field.

-F IP frag
IP Fragmentation field.

-O IP Options
IP Options field.

Data Link Options

-d Ethernet Device
Name of ethernet device (eg. ne0, ed0, eth0).

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

-H Source MAC Address
Source MAC Address (XX:XX:XX:XX:XX:XX)

-M Destination MAC Address
Target MAC Address (XX:XX:XX:XX:XX:XX)

NAME

nemesis-arp - ARP/RARP Protocol (The Nemesis Project)

SYNOPSIS

nemesis-arp [-v] [optlist]

DESCRIPTION

The Nemesis Project is designed to be a commandline-based, portable human IP stack for UNIX/Linux. The suite is broken down by protocol, and should allow for useful scripting of injected packet streams from simple shell scripts.

ARP/RARP Options

-S Source IP Address
Source Address of injected packet.

-D Destination IP Address
Target Address of injected packet.

-h Sender hardware Address
Sender Hardware Address within ARP frame only.

-m Sender hardware Address
Target Hardware Address within ARP frame only.

-s Solaris Mode Enabler
Shortcut to set Target Hardware Address within ARP frame to ff:ff:ff:ff:ff:ff rather than the standard 00:00:00:00:00:00.

-T ARP/RARP Reply Enabler

-R RARP Enabler

-P Payload File
Filename to read for packet payload.

-v Verbose Mode
Display human readable output of currently injected packet.

Data Link Options

-d Ethernet Device
Name of ethernet device (eg. ne0, ed0, eth0).

-H Source MAC Address
Source MAC Address (XX:XX:XX:XX:XX:XX)

-M Destination MAC Address

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

Target MAC Address (XX:XX:XX:XX:XX:XX)

NAME

nemesis-igmp - IGMP Protocol (The Nemesis Project)

SYNOPSIS

nemesis-igmp [-v] [optlist]

DESCRIPTION

The Nemesis Project is designed to be a commandline-based, portable human IP stack for UNIX/Linux. The suite is broken down by protocol, and should allow for useful scripting of injected packet streams from simple shell scripts.

IGMP Options

-p IGMP Type
IGMP type.

-c IGMP Code
IGMP code.

-i IGMP Group Address
IGMP Group Address.

-P Payload File
Filename to read for packet payload.

-v Verbose Mode
Display human readable output of currently injected packet.

IP Options

-S Source IP Address
Source Address of injected packet.

-D Destination IP Address
Target Address of injected packet.

-I IP ID
IP ID header tag.

-T IP TTL
IP Time To Live field.

-t IP tos
IP Type Of Service field.

-F IP frag
IP Fragmentation field.

-O IP Options
IP Options field.

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

Data Link Options

-d Ethernet Device

Name of ethernet device (eg. ne0, ed0, eth0).

-H Source MAC Address

Source MAC Address (XX:XX:XX:XX:XX:XX)

-M Destination MAC Address

Target MAC Address (XX:XX:XX:XX:XX:XX)

NAME

nemesis-dns - DNS Protocol (The Nemesis Project)

SYNOPSIS

nemesis-dns [-v] [optlist]

DESCRIPTION

The Nemesis Project is designed to be a commandline-based, portable human IP stack for UNIX/Linux. The suite is broken down by protocol, and should allow for useful scripting of injected packet streams from simple shell scripts.

DNS Options

-q Number of Questions

Number of Questions.

-W Number of Answer RRs

Number of Answer RRs.

-A Number of Authority RRs

Number of Authority RRs.

-i Number of Additional RRs

Number of Additional RRs.

-P Payload File

Filename to read for packet payload.

-k TCP Transport Enable

Use TCP as the transport protocol.

-v Verbose Mode

Display human readable output of currently injected packet.

TCP Options (-k)

[-x Source Port]

Source Port of injected packet.

[-y Destination Port]

Target Port of injected packet.

-f TCP Flag Options (-fS/-fA/-fR/-fP/-fF/-fU)

SYN, ACK, RST, PSH, FIN, URG

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

-w Window Size
TCP Window Size.

-s Sequence Number
TCP Sequence Number.

-a Acknowledgement Number
TCP Acknowledgement Number.

-u TCP Urgent Pointer
TCP Urgent Pointer.

UDP Options (no -k)

[-x Source Port]
Source Port of injected packet.

[-y Destination Port]
Target Port of injected packet.

IP Options

-S Source IP Address
Source Address of injected packet.

-D Destination IP Address
Target Address of injected packet.

-I IP ID
IP ID header tag.

-T IP TTL
IP Time To Live field.

-t IP tos
IP Type Of Service field.

-F IP frag
IP Fragmentation field.

-O IP Options
IP Options field.

Data Link Options

-d Ethernet Device
Name of ethernet device (eg. ne0, ed0, eth0).

-H Source MAC Address
Source MAC Address (XX:XX:XX:XX:XX:XX)

-M Destination MAC Address
Target MAC Address (XX:XX:XX:XX:XX:XX)

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

NAME

nemesis-rip - RIP Protocol (The Nemesis Project)

SYNOPSIS

nemesis-rip [-v] [optlist]

DESCRIPTION

The Nemesis Project is designed to be a commandline-based, portable human IP stack for UNIX/Linux. The suite is broken down by protocol, and should allow for useful scripting of injected packet streams from simple shell scripts.

RIP Options

-c RIP Command
RIP Command.

-V RIP Version
RIP Version.

-r RIP Route Domain
RIP Route Domain.

-a RIP Address Family
RIP Address Family.

-R RIP Route Tag
RIP Route Tag.

-k RIP Network Address Mask
RIP Network Address Mask.

-h RIP Next Hop
RIP Next Hop.

-m RIP Metric
RIP Metric.

-P Payload File
Filename to read for packet payload.

-v Verbose Mode
Display human readable output of currently injected packet.

UDP Options (no -k)

[-x Source Port]
Source Port of injected packet.

[-y Destination Port]
Target Port of injected packet.

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

IP Options

-S Source IP Address

Source Address of injected packet.

-D Destination IP Address

Target Address of injected packet.

-I IP ID

IP ID header tag.

-T IP TTL

IP Time To Live field.

-t IP tos

IP Type Of Service field.

-F IP frag

IP Fragmentation field.

-O IP Options

IP Options field.

Data Link Options

-d Ethernet Device

Name of ethernet device (eg. ne0, ed0, eth0).

-H Source MAC Address

Source MAC Address (XX:XX:XX:XX:XX:XX)

-M Destination MAC Address

Target MAC Address (XX:XX:XX:XX:XX:XX)

NAME

nemesis-ospf - OSPF Protocol (The Nemesis Project)

SYNOPSIS

nemesis-ospf [-v] [optlist]

DESCRIPTION

The Nemesis Project is designed to be a commandline-based, portable human IP stack for UNIX/Linux. The suite is broken down by protocol, and should allow for useful scripting of injected packet streams from simple shell scripts.

OSPF Packet Types

-p OSPF Protocol (-pH, -pL, -pR), Hello (-pH), Database Description (-pD), Link State Request (-pL), Link State Update (-pU), Router Links Advertisement (-pR), Network Links Advertisement (-pN), IP Summary Links Advertisement (-pM), AS External Link Advertisement (-pA),

OSPF HELLO options

-N Neighbor Router Address

Neighbor Router Address.

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

-i Dead Router Interval
Dead Router Interval.

-I OSPF Interval
OSPF Interval.

OSPF Database Description (DBD) options

-z MAX DGRAM Length
OSPF Maximum Datagram Length

-x Exchange Type
OSPF DBD Exchange Type

OSPF Link State Update (LSU) options

-x Num LSAs to bcast
Number of Link State Advertisements to broadcast

OSPF Link State Advertisement (LSA) related options

-L Router ID
Router ID for Link State Advertisement packets.

-G LSA Age
Link State Advertisement Age.

OSPF Router Links Advertisement (LSA_RTR) options

-u LSA_RTR Number
Router Links Advertisement Number

-y LSA_RTR Router Type
Router Links Advertisement Router Type

-k LSA_RTR Router Data
Router Links Advertisement Router Data

OSPF Autonomous System External Link Advertisement (LSA_AS_EXT) options

-f LSA_AS_EXT Forward Address
Autonomous System Forward Address

-g LSA_AS_EXT Tag
Autonomous System Tag

OSPF options

-m OSPF Metric
OSPF Metric

-s OSPF Sequence Number
OSPF Sequence Number

-r OSPF Advertising Router Address
OSPF Advertising Router Address

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

-n OSPF Netmask
OSPF Netmask Address

-O OSPF Options
OSPF Options

-R OSPF Router ID
OSPF Router Identifier

-A OSPF Area ID
OSPF Area Identifier

-P Payload File
Filename to read for packet payload.

-v Verbose Mode
Display human readable output of currently injected packet.

IP Options

-S Source IP Address
Source Address of injected packet.

-D Destination IP Address
Target Address of injected packet.

-I IP ID
IP ID header tag.

-T IP TTL
IP Time To Live field.

-t IP tos
IP Type Of Service field.

-F IP frag
IP Fragmentation field.

-o IP Options
IP Options field.

Data Link Options

-d Ethernet Device
Name of ethernet device (eg. ne0, ed0, eth0).

-H Source MAC Address
Source MAC Address (XX:XX:XX:XX:XX:XX)

-M Destination MAC Address
Target MAC Address (XX:XX:XX:XX:XX:XX)

Command Line Windows Port

Command line additions for Windows port:

The Nemesis Project Documentation

Mark Grimes and Jeff Nathan

-d <Ethernet Device>

* list : to list available interfaces

* 0 : to select interface from the list

* 1+ (1, 2, 3...) : to select interface from its number

A few examples:

- nemesis-tcp -v -S 192.168.1.1 -D 192.168.2.2 -fS -fA -y 22 -P foo Send TCP packet (SYN/ACK) with payload from ascii file 'foo' to target's ssh port from 192.168.1.1 to 192.168.2.2. (-v allows a stdout visual of current injected packet)
- nemesis-udp -v -S 10.11.12.13 -D 10.1.1.2 -x 11111 -y 53 -P bindpkt send UDP packet from 10.11.12.13:11111 to 10.1.1.2's name-service port with a payload read from a file 'bindpkt'. (again -v is used in order to see confirmation of our injected packet)
- nemesis-icmp -S 10.10.10.3 -D 10.10.10.1 -G 10.10.10.3 -i 5 send ICMP REDIRECT (network) packet from 10.10.10.3 to 10.10.10.1 with preferred gateway as source address. Here we want no output to go to stdout - which would be ideal as a component in a batch job via a shell script.
- nemesis-arp -v -d 1 -H 0:1:2:3:4:5 -S 10.11.30.5 -D 10.10.15.1 send ARP packet through device n°1 from hardware source address 00:01:02:03:04:05 with IP source address 10.11.30.5 to destination IP address 10.10.15.1 with broadcast destination hardware address. In other words, who-has the mac address of 10.10.15.1, tell 10.11.30.5 - assuming 00:01:02:03:04:05 is the source mac address of our first device.