ndiff

Ndiff is a tool to aid in the comparison of Nmap scans. It takes two Nmap XML output files and prints the differences between them them: hosts coming up and down, ports becoming open or closed, and things like that. It can produce output in human-readable text or machine-readable XML formats.

Installed size: 433 KB

How to install: sudo apt install ndiff

Dependencies:

- python3
- python3-lxml

```
root@kali:~# ndiff -h
Usage: /usr/bin/ndiff [option] FILE1 FILE2
Compare two Nmap XML files and display a list of their differences.
Differences include host state changes, port state changes, and changes to
service and OS detection.

  -h, --help     display this help
  -v, --verbose  also show hosts and ports that haven't changed.
  --text         display output in text format (default)
  --xml          display output in XML format
```

nmap

Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more. Most Unix and Windows platforms are supported in both GUI and commandline modes. Several popular handheld devices are also supported, including the Sharp Zaurus and the iPAQ.

Installed size: 4.48 MB

How to install: sudo apt install nmap

Dependencies:

- libc6
- libgcc-s1
- liblinear4
- liblua5.4-0
- libpcap0.8t64
- libpcre2-8-0
- libssh2-1t64
- libssl3t64
- libstdc++6
- nmap-common
- zlib1g

```
root@kali:~# nmap -h
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma-separated list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --proxies <url1,[url2],...>: Relay connections through HTTP/SOCKS4 proxies
  --data <hex string>: Append a custom payload to sent packets
  --data-string <string>: Append a custom ASCII string to sent packets
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state

  --open: Only show open (or possibly open) ports

  --packet-trace: Show all packets sent and received

  --iflist: Print host interfaces and routes (for debugging)

  --append-output: Append to rather than clobber specified output files

  --resume <filename>: Resume an aborted scan

  --noninteractive: Disable runtime interactions via keyboard

  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML

  --webxml: Reference stylesheet from Nmap.Org for more portable XML

  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output

MISC:

  -6: Enable IPv6 scanning

  -A: Enable OS detection, version detection, script scanning, and traceroute

  --datadir <dirname>: Specify custom Nmap data file location

  --send-eth/--send-ip: Send using raw ethernet frames or IP packets

  --privileged: Assume that the user is fully privileged

  --unprivileged: Assume the user lacks raw socket privileges

  -V: Print version number

  -h: Print this help summary page.

EXAMPLES:

  nmap -v -A scanme.nmap.org

  nmap -v -sn 192.168.0.0/16 10.0.0.0/8

  nmap -v -iR 10000 -Pn -p 80

SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Nping

```
root@kali:~# nping -h

Nping 0.7.95 ( https://nmap.org/nping )

Usage: nping [Probe mode] [Options] {target specification}


TARGET SPECIFICATION:
  Targets may be specified as hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.*.1-24
PROBE MODES:
  --tcp-connect              : Unprivileged TCP connect probe mode.
  --tcp                      : TCP probe mode.
  --udp                      : UDP probe mode.
  --icmp                     : ICMP probe mode.
  --arp                      : ARP/RARP probe mode.
  --tr, --traceroute         : Traceroute mode (can only be used with
                               TCP/UDP/ICMP modes).
TCP CONNECT MODE:
   -p, --dest-port <port spec>    : Set destination port(s).
   -g, --source-port <portnumber>  : Try to use a custom source port.
TCP PROBE MODE:
   -g, --source-port <portnumber>  : Set source port.
   -p, --dest-port <port spec>    : Set destination port(s).
   --seq <seqnumber>          : Set sequence number.
   --flags <flag list>        : Set TCP flags (ACK,PSH,RST,SYN,FIN...)
   --ack <acknumber>          : Set ACK number.
   --win <size>               : Set window size.
   --badsum                   : Use a random invalid checksum.
UDP PROBE MODE:
   -g, --source-port <portnumber>  : Set source port.
   -p, --dest-port <port spec>    : Set destination port(s).
   --badsum                   : Use a random invalid checksum.
ICMP PROBE MODE:
  --icmp-type <type>          : ICMP type.
  --icmp-code <code>          : ICMP code.
  --icmp-id <id>              : Set identifier.
  --icmp-seq <n>              : Set sequence number.
  --icmp-redirect-addr <addr>     : Set redirect address.
  --icmp-param-pointer <pnt>      : Set parameter problem pointer.
  --icmp-advert-lifetime <time>   : Set router advertisement lifetime.
  --icmp-advert-entry <IP,pref>   : Add router advertisement entry.
  --icmp-orig-time  <timestamp>    : Set originate timestamp.
  --icmp-recv-time  <timestamp>    : Set receive timestamp.
  --icmp-trans-time <timestamp>    : Set transmit timestamp.
ARP/RARP PROBE MODE:
  --arp-type <type>              : Type: ARP, ARP-reply, RARP, RARP-reply.
  --arp-sender-mac <mac>         : Set sender MAC address.
  --arp-sender-ip  <addr>        : Set sender IP address.
  --arp-target-mac <mac>         : Set target MAC address.
  --arp-target-ip  <addr>        : Set target IP address.
IPv4 OPTIONS:
  -S, --source-ip                : Set source IP address.
  --dest-ip <addr>               : Set destination IP address (used as an
                                 alternative to {target specification} ).
  --tos <tos>                    : Set type of service field (8bits).
  --id  <id>                     : Set identification field (16 bits).
  --df                           : Set Don't Fragment flag.
  --mf                           : Set More Fragments flag.
  --evil                         : Set Reserved / Evil flag.
  --ttl <hops>                   : Set time to live [0-255].
  --badsum-ip                    : Use a random invalid checksum.
  --ip-options <R|S [route]|L [route]|T|U ...> : Set IP options
  --ip-options <hex string>                    : Set IP options
  --mtu <size>                   : Set MTU. Packets get fragmented if MTU is
                                 small enough.
IPv6 OPTIONS:
  -6, --IPv6                     : Use IP version 6.
  --dest-ip                      : Set destination IP address (used as an
                                 alternative to {target specification}).
  --hop-limit                    : Set hop limit (same as IPv4 TTL).
  --traffic-class <class> :      : Set traffic class.
  --flow <label>                 : Set flow label.
ETHERNET OPTIONS:
  --dest-mac <mac>               : Set destination mac address. (Disables
                                 ARP resolution)
```

```
 --source-mac <mac>            : Set source MAC address.
 --ether-type <type>           : Set EtherType value.
PAYLOAD OPTIONS:
 --data <hex string>           : Include a custom payload.
 --data-string <text>          : Include a custom ASCII text.
 --data-length <len>           : Include len random bytes as payload.
ECHO CLIENT/SERVER:
 --echo-client <passphrase>      : Run Nping in client mode.
 --echo-server <passphrase>      : Run Nping in server mode.
 --echo-port <port>            : Use custom <port> to listen or connect.
 --no-crypto                   : Disable encryption and authentication.
 --once                        : Stop the server after one connection.
 --safe-payloads               : Erase application data in echoed packets.
TIMING AND PERFORMANCE:
 Options which take <time> are in seconds, or append 'ms' (milliseconds),
 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m, 0.25h).
 --delay <time>                : Adjust delay between probes.
 --rate  <rate>                : Send num packets per second.
MISC:
 -h, --help                    : Display help information.
 -V, --version                 : Display current version number.
 -c, --count <n>               : Stop after <n> rounds.
 -e, --interface <name>         : Use supplied network interface.
 -H, --hide-sent               : Do not display sent packets.
 -N, --no-capture              : Do not try to capture replies.
 --privileged                  : Assume user is fully privileged.
 --unprivileged                : Assume user lacks raw socket privileges.
 --send-eth                    : Send packets at the raw Ethernet layer.
 --send-ip                     : Send packets using raw IP sockets.
 --bpf-filter <filter spec>      : Specify custom BPF filter.
OUTPUT:
 -v                            : Increment verbosity level by one.
 -v[level]                     : Set verbosity level. E.g: -v4
 -d                            : Increment debugging level by one.
```

```
  -d[level]              : Set debugging level. E.g: -d3

  -q                     : Decrease verbosity level by one.

  -q[N]                  : Decrease verbosity level N times

  --quiet                : Set verbosity and debug level to minimum.

  --debug                : Set verbosity and debug to the max level.

EXAMPLES:

  nping scanme.nmap.org

  nping --tcp -p 80 --flags rst --ttl 2 192.168.1.1

  nping --icmp --icmp-type time --delay 500ms 192.168.254.254

  nping --echo-server "public" -e wlan0 -vvv

  nping --echo-client "public" echo.nmap.org --tcp -p1-1024 --flags ack


SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

nmap-common

Nmap is a utility for network exploration or security auditing. It supports ping scanning (determine which hosts are up), many port scanning techniques, version detection (determine service protocols and application versions listening behind ports), and TCP/IP fingerprinting (remote host OS or device identification). Nmap also offers flexible target and port specification, decoy/stealth scanning, sunRPC scanning, and more. Most Unix and Windows platforms are supported in both GUI and commandline modes. Several popular handheld devices are also supported, including the Sharp Zaurus and the iPAQ.

This package contains the nmap files shared by all architectures.

Installed size: 21.76 MB

How to install: sudo apt install nmap-common

zenmap

Zenmap is an Nmap frontend. It is meant to be useful for advanced users and to make Nmap easy to use by beginners. It was originally derived from Umit, an Nmap GUI created as part of the Google Summer of Code.

Installed size: 1.75 MB

How to install: sudo apt install zenmap

Dependencies:

- gir1.2-gdkpixbuf-2.0
- gir1.2-glib-2.0
- gir1.2-gtk-3.0
- gir1.2-pango-1.0
- ndiff
- nmap
- python3
- python3-gi
- python3-gi-cairo

zenmap

```
root@kali:~# zenmap -h

Usage: zenmap [options] [result files]


Options:

 --version           show program's version number and exit

 -h, --help          show this help message and exit

 --confdir=DIR       Use DIR as the user configuration directory. Default:

                     /root/.zenmap

 -f RESULT_FILES, --file=RESULT_FILES

                     Specify a scan result file in Nmap XML output format.

                     Can be used more than once to specify several scan

                     result files.

 -n, --nmap          Run Nmap with the specified args.

 -p PROFILE, --profile=PROFILE

                     Begin with the specified profile selected. If combined

                     with the -t (--target) option, automatically run the

                     profile against the specified target.

 -t TARGET, --target=TARGET

                     Specify a target to be used along with other options.

                     If specified alone, open with the target field filled

                     with the specified target

 -v, --verbose       Increase verbosity of the output. May be used more
```

than once to get even more verbosity