

OSEC



1828 W. Webster Chicago, IL 60614
phone: 773.394.8310 fax: 773.394.8314
osec.neohapsis.com www.neohapsis.com

Report # 00003 April 7, 2003

NIDS Verification Certificate

Netscreen IDP-100 sensor 2.0p2-2 / signatures v.2.0.0 update 49

Device Integrity	
Test	P/F/NA
Test A1	P
Test A2	P
Test A3	P
Test A4	P
Test A5	P
Test A6	P
Test A7	P
Test A8	P

Signature Baselines	
Test	P/F/NA
Test B1	P
Test B2	P

State Tests	
Test	P/F/NA
Test C1	P
Test C2	P
Test C3	P
Test C4	P
Test C5	P
Test C6	P
Test C7	P
Test C8	P
Test C9	NA
Test C10	NA

Discard Tests	
Test	P/F/NA
Test D1	P
Test D2	P
Test D3	P
Test D4	NA
Test D5	NA
Test D6	NA
Test D7	P
Test D8	P
Test D9	NA
Test D10	NA
Test D11	NA
Test D12	P

Engine Flex Tests	
Test	P/F/NA
Test E1	P
Test E2	P
Test E3	P
Test E4	P
Test E5	NA
Test E6	NA
Test E7	NA
Test E8	NA

Evasion Handling	
Test	P/F/NA
Test F1	P
Test F2	P
Test F3	P
Test F4	P
Test F5	P
Test F6	P
Test F7	P
Test F8	P
Test F9	P
Test F10	P
Test F11	P
Test F12	P
Test F13	P
Test F14	P
Test F15	P
Test F16	P
Test F17	P

Evasion Handling	
Test	P/F/NA
Test F18	NA
Test F19	NA
Test F20	P
Test F21	P
Test F22	P
Test F23	P
Test F24	P
Test F25	P
Test F26	P
Test F27	P
Test F28	P
Test F29	P
Test F30	P
Test F31	P
Test F32	P
Test F33	P

In-Line/Tap Tests	
Test	P/F/NA
Test G1	NA
Test G2	NA

Listening Service Inventory			
Protocol	SSH 2.0	HTTP	HTTPS
Port	TCP/22	TCP/80	TCP/443
Known Vuln	P	P	P



OSEC NIDS Evaluation Tests version 1.0

A – Device Integrity Checking

A1	Listening Service Inventory (added or required services)
A2	Known-vulnerabilities Check
A3	SNMP v1 Protos Tests
A4	Routable ISIC protocol mix TO
A5	Routable ISIC protocol mix THROUGH
A6	Unfiltered ISIC protocol mix TO
A7	Unfiltered ISIC protocol mix THROUGH
A8	TCP / ISN generation test

B – Signature Baseline

B1	Mainstream Attack Baseline (Trigger test of all attacks)
B2	Modified Attacks (ADMutated shellcode, content-altered attack)

C – State Test

C1	State Confirmation Test
C2	Tool Dry-run (varies by product; one run for highest load to be tested)
C3	Low session, small address block (25,000 sessions, 200 addresses)
C4	Low session, large address block (25,000 sessions, 10,000 addresses)
C5	Medium session, small address block (50,000 sessions, 200 addresses)
C6	Medium session, large address block (50,000 sessions, 10,000 addresses)
C7	Medium session, small address block (100,000 sessions, 200 addresses)
C8	Medium session, large address block (100,000 sessions, 10,000 addresses)
C9	High session, small address block (200,000 sessions, 200 addresses)
C10	High session, large address block (200,000 sessions, 10,000 addresses)

D – Discard Test

D1	Tool dry-run (varies by product; one run for highest load to be tested)
D2	Bogus port and injection (10 Mbps)
D3	Bogus port and injection (80 Mbps)
D4	Bogus port and injection (200 Mbps)
D5	Bogus port and injection (500 Mbps)
D6	Bogus port and injection (750 Mbps)
D7	Valid port and injection (10 Mbps)
D8	Valid port and injection (80 Mbps)
D9	Valid port and injection (200 Mbps)
D10	Valid port and injection (500 Mbps)
D11	Valid port and injection (750 Mbps)
D12	Invalid traffic (64byte frames)

E – Engine Flex

E1	Tool dry-run (varies by product; one run for highest load to be tested)
E2	HTTP (10 Mbps) + injection
E3	HTTP (80 Mbps) + injection
E4	HTTP (80 Mbps, 536 MSS) + injection
E5	HTTP (200 Mbps) + injection
E6	HTTP (500 Mbps) + injection
E7	HTTP (500 Mbps, 536 MSS) + injection
E8	HTTP (750 Mbps) + injection

F – Evasion List

F1	Basic IP Fragmentation (ordered 8-byte) [fragrouter F1]
F2	Basic IP Fragmentation (ordered 24-byte) [fragrouter F2]
F3	Complex IP Fragmentation (ordered 8-byte IP fragments, one out of order) [fragrouter F3]
F4	Complex IP Fragmentation (ordered 8-byte IP fragments, one duplicate) [fragrouter F4]
F5	Complex IP Fragmentation (out of order 8-byte fragments, one duplicate) [fragrouter F5]
F6	Complex IP Fragmentation (ordered 8-byte fragments, marked last frag first) [fragrouter F6]
F7	Basic TCP segmentation (3-whs, ordered 1-byte segments, one out of order) [fragrouter T8]
F8	Complex TCP Segmentation (3-whs, bad TCP checksum FIN/RST, ordered 1-byte segments) [fragrouter T1]
F9	Complex TCP Segmentation (3-whs, ordered 1-byte segments, one duplicate) [fragrouter T3]
F10	Complex TCP Segmentation (3-whs, ordered 1-byte segments, one overwriting) [fragrouter T4]
F11	Complex TCP Segmentation (3-whs, ordered 2-byte segments, fwd-overwriting) [fragrouter T5]
F12	Complex TCP Segmentation (3-whs, ordered 1-byte segments, interleaved null segments) [fragrouter T7]
F13	Complex TCP Segmentation (3-whs, out of order 1-byte segments) [fragrouter T9]
F14	Complex TCP Segmentation (3-whs, ordered 1-byte segments, interleaved SYN) [fragrouter C2]
F15	Complex TCP Segmentation (ordered 1-byte null segments, 3-whs, ordered 1-byte segments) [fragrouter C3]
F16	Complex TCP Segmentation (3-whs, RST, 3-whs, ordered 1-byte segments) [fragrouter R1]
F17	Delayed injection @ 100,000 sessions
F18	Delayed injection @ 250,000 sessions
F19	Delayed injection @ 500,000 sessions
F20	HTTP obfuscation (hex encoding)
F21	HTTP obfuscation (double hex encoding)
F22	HTTP obfuscation (Unicode / UTF-8 encoding)
F23	HTTP obfuscation (self-referential directories) [whisker -I 2]
F24	HTTP obfuscation (premature URL ending) [whisker -I 3]
F25	HTTP obfuscation (prepend long string) [whisker -I 4]
F26	HTTP obfuscation (fake URL parameter) [whisker -I 5]
F27	HTTP obfuscation (case sensitivity) [whisker -I 7]
F28	HTTP obfuscation (Windows directory syntax) [whisker -I 8]
F29	HTTP obfuscation (session splicing) [whisker -I 9]
F30	HTTP obfuscation (connection reuse)
F31	HTTP obfuscation (version 0.9)
F32	HTTP obfuscation (version 1.0)
F33	HTTP obfuscation (version 1.1)

G – In-line/Tap Test

G1	Tool dry-run (1500Mbps)
G2	HTTP (1500 Mbps) + injection

Key:	
P	Pass
F	Fail
NA	Not Available/Not tested

