

Network Security Incident Handling Toolkit

Listed below are tools that can be used by the incident handlers to handle and respond to various network security incidents.

Network Security Incident Handling Tools	
Category	Tools
Windows-based Network Analysis Tools	<ul style="list-style-type: none">▪ Nmap (https://nmap.org)▪ Wireshark (https://www.wireshark.org)▪ TCPView (https://www.microsoft.com)▪ NetFlow Traffic Analyzer (https://www.solarwinds.com)▪ Stealthwatch (https://www.cisco.com)▪ netstat (http://netstat.net)▪ nbtstat (https://www.microsoft.com)▪ tracert (https://www.microsoft.com)▪ Packet Capture (https://www.netscantools.com)▪ ManageEngine NetFlow Analyzer (https://www.manageengine.com)▪ ntopng (www.ntop.org)▪ Capsa Portable Network Analyzer (https://www.colasoft.com)▪ Zeek (https://zeek.org)▪ Splunk Enterprise Security (https://www.splunk.com)
Linux-based Network Analysis Tools	<ul style="list-style-type: none">▪ Nmap (https://nmap.org)▪ Wireshark (https://www.wireshark.org)▪ netstat (http://netstat.net)▪ tcpdump (http://www.tcpdump.org)▪ Nagios XI (https://www.nagios.org)▪ NetHogs (https://github.com) Command Line Tools <ul style="list-style-type: none">▪ traceroute▪ ARP▪ ifconfig▪ tracepath▪ ping▪ dig▪ ss▪ mtr

	<ul style="list-style-type: none"> ▪ nslookup ▪ lsof ▪ dd ▪ grep ▪ lastlog ▪ cat ▪ ps aux
Linux-based Session Management Tools	Command Line Tools <ul style="list-style-type: none"> ▪ w/who ▪ rwho ▪ Lastlog
Vulnerability Analysis Tools	<ul style="list-style-type: none"> ▪ SanerNow (https://www.secpod.com) ▪ Nexpose (https://www.rapid7.com) ▪ Tenable.io (https://www.tenable.com) ▪ Qualys (https://www.qualys.com) ▪ Nessus (https://www.tenable.com) ▪ GFI LanGuard (https://www.gfi.com) ▪ Intruder (https://www.intruder.io) ▪ OpenVAS (https://www.openvas.org)
Suspicious Network Events Detection and Validation Tools	<ul style="list-style-type: none"> ▪ Suricata (https://suricata.io) ▪ Flowmon ADS (https://www.flowmon.com) ▪ ntopng (https://www.ntop.org) ▪ Wireshark (https://www.wireshark.org) ▪ Colasoft Network Analyzer (https://www.colasoft.com) ▪ OmniPeek (https://www.liveaction.com) ▪ Observer Analyzer (https://www.viavisolutions.com) ▪ PRTG Network Monitor (https://www.paessler.com) ▪ NetFlow Analyzer (https://www.manageengine.com)
Network Log Analysis Tools	<ul style="list-style-type: none"> ▪ Solarwinds Loggly (https://www.solarwinds.com) ▪ Kiwi Syslog Server (https://www.solarwinds.com) ▪ ManageEngine Log360 (https://www.manageengine.com) ▪ InsightOps (https://www.rapid7.com) ▪ Splunk Enterprise Security (https://www.splunk.com) ▪ Logz.io (https://www.logz.io) ▪ Graylog (https://www.graylog.org)

ARP Poisoning Detection Tools	<ul style="list-style-type: none">▪ Wireshark (https://www.wireshark.org)▪ Capsa Portable Network Analyzer (https://www.colasoft.com)▪ ArpON (http://arpon.sourceforge.net)▪ ARP AntiSpoofers (https://sourceforge.net)▪ ARPStraw (https://github.com)▪ shARP (https://github.com)▪ ARPShield (https://github.com)
Promiscuous Detection Tools	<ul style="list-style-type: none">▪ Nmap (https://nmap.org)▪ NetScanTools Pro (https://www.netscantools.com)
Tools for Detecting Firewall and IDS Evasion Attempts	<ul style="list-style-type: none">▪ Snort (https://www.snort.org)
Tools for Detecting Password Spray Attacks	<ul style="list-style-type: none">▪ Stealthwatch (https://www.cisco.com)
High Resource Utilization Detection Tools	<ul style="list-style-type: none">▪ AIDA64 Extreme (https://www.aida64.com)▪ HWiNFO (https://www.hwinfo.com)▪ OCCT (https://www.ocbase.com)▪ InsightCat (https://insightcat.com)▪ SysGauge (https://www.sysgauge.com)▪ HWMonitor (https://www.cpuid.com)
Malware Detection and Analysis Tools	<ul style="list-style-type: none">▪ Kiwi Log Viewer (https://www.solarwinds.com)▪ Splunk Enterprise Security (https://www.splunk.com)

Tools for Detecting DoS/DDoS Incidents	<ul style="list-style-type: none">▪ KFSensor (https://www.kfsensor.net)▪ SNORT (https://www.snort.org)▪ Security Event Manager (https://www.solarwinds.com)▪ Suricata (https://suricata.io)▪ FastNetMon (https://fastnetmon.com)▪ Kentik (https://www.kentik.com)
Tools for Detecting Missing Security Patches	<ul style="list-style-type: none">▪ GFI LanGuard (https://www.gfi.com)▪ Solarwinds Patch Manager (https://www.solarwinds.com)▪ Kaseya Security Patch Management (https://www.kaseya.com)▪ Software Vulnerability Manager (https://www.flexera.com)▪ Ivanti Endpoint Security (https://www.ivanti.com)▪ Patch Connect Plus (https://www.manageengine.com)
DoS/DDoS Protection Tools	<ul style="list-style-type: none">▪ Anti DDoS Guardian (https://beethink.com)▪ Imperva DDoS Protection (https://www.imperva.com)▪ DOSarrest DDoS protection service (https://www.dosarrest.com)▪ DDoS-GUARD (https://ddos-guard.net)▪ Cloudflare (https://www.cloudflare.com)▪ F5 DDoS Attack Protection (https://www.f5.com)
Network Security Tools	<ul style="list-style-type: none">▪ Solarwinds Security Event Manager (https://www.solarwinds.com)▪ Nagios XI (https://www.nagios.com)▪ Splunk Enterprise Security (https://www.splunk.com)▪ SecPod SanerNow (https://www.secpod.com)▪ LogRhythm NDR (https://logrhythm.com)▪ AlienVault USM (https://cybersecurity.att.com)