www.novacybersecurity.com

NETAŞ

Netas provides innovative end-to-end value added systems integration and technology services in information and communications technologies (ICT). Its customers range from telco providers to public and private enterprises in domestic and international markets. Netas's constant focus on productivity is based on its next generation competencies around technology skillset and expertise. The company holds a track-record of 50 years and continues its foray in the next generation technologies, supported with its experienced, best of breed research and development teams.

The company, provides its customer with solutions in various domains such as networking, cyber security, unified communications, virtualization, cloud computing, broadband mobility, optical and carrier Ethernet, GSM-R. Netas is a leader in IT integration services, managed services and software development solut¬ions. Netas also plays an important role in the modernization of the Turkish Armed Forces' communication networks. Also, the company serves armed forces of some other countries in North Africa, Asia-Pacific and the CIS.

NOVA
Cyber Security Solutions
by NETAŞ

Are you aware that you are vulnerable to many threats on the Internet?

With increasing voice and video transmission over IP and emerging new technologies such as 4G LTE and 5G, data vulnerabilities and lack of security are the main concerns due to the nature of IP infrastructure systems. Reports show that most of attacks occur in the application layer. Therefore our products and services focus on the application layer security. Discover vulnerabilities, detect and prevent attacks, enable secure media communication with our solution.

Find out your vulnerabilities and protect your network with NOVA!

Create and operate a secure VoIP infrastructure with comprehensive VoIP Penetration Test relies on, NOVA PENTEST Services via NOVA V-SPY Vulnerability Scanning and Analysis Tool.

V-SPY is an automated enriched VoIP penetration test suite including rich variety of VoIP attack modules, detailed reports of security measures via expert system.

Detect and prevent VoIP threats using VoIP Application Firewall, NOVA V-GATE.

V-GATE is ready to guard your VoIP infrastructure by performing deep packet inspection, statistical and behavioral analysis, detecting anomalies and preventing VoIP attacks, VoIP monitoring and operational management.

Detect telecommunication frauds using Fraud Management System, NOVA FMS.

FMS offers an intelligent, agile and economical solution that can perform security analysis on massive data volume with machine-learning techniques in real-time to detect frauds and threats.

Make a secure multimedia communication via Secure Media Communication Platform, NOVA S/COM.

S/COM can achieve secure media transfer with its support for various security methods and flexible crypto algorithm, enabling secure voice and video communication, whiteboard usage, file and message transfer.

Maintain a secure operation in UC network, VoIP ad Web applications with NOVA Product Family.

NOVA is a product name of NETAS Cyber Security Technology Development Group developments. VoIP, Web, IoT, Mobile security are the main areas with real time data analysis, artificial intelligence, big data analytics methods usage.

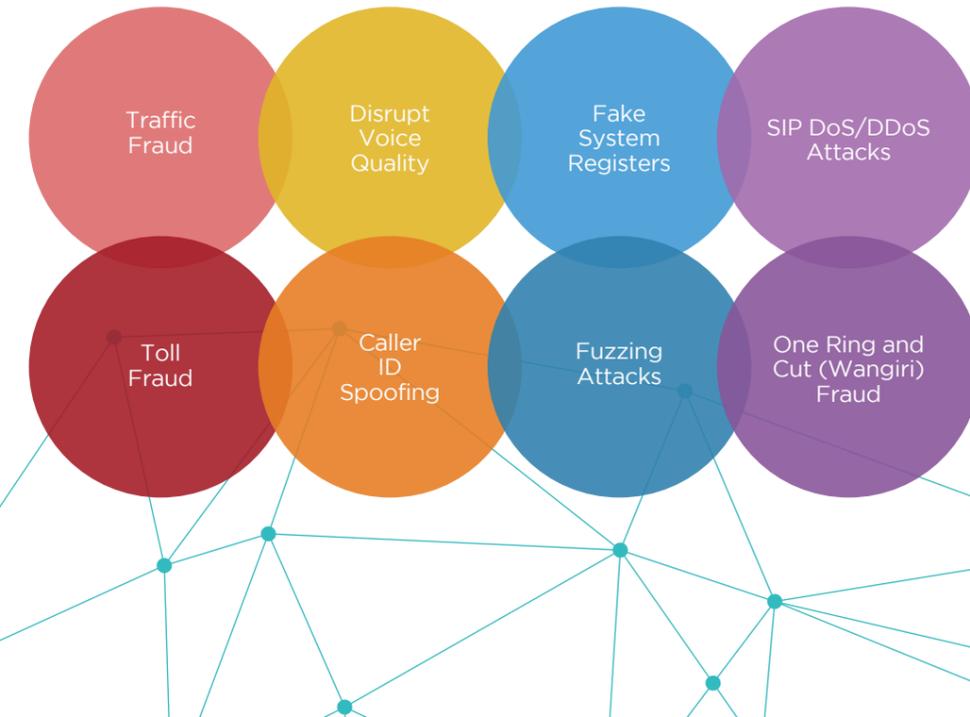## NOVA PENTEST

PENTEST SERVICES
via NOVA V-SPY

NETAŞ

Unified Communications Security Testing

NOVA Pentest Services test the network, applications, infrastructure and devices to ensure that they are protected from attacks on Network, VoIP, Web and Unified Communications systems. Our own developed product **NOVA V-SPY** are used in our pentest services.

NOVA V-SPY is an automated enriched VoIP penetration test suite including the rich variety of VoIP attack modules, detailed reports of security measures via the expert system.

It is a modular, high-performance vulnerability scanning framework that can execute comprehensive scanning enumeration, fuzzing and MITM attacks aimed towards helping penetration testers and administrators that evaluate the security of VoIP applications.

Traffic Fraud

Disrupt Voice Quality

Fake System Registers

SIP DoS/DDoS Attacks

Toll Fraud

Caller ID Spoofing

Fuzzing Attacks

One Ring and Cut (Wangiri) Fraud

Crucial for a secure VoIP Infrastructure

There is a demand for an automated tool that will examine the whole security infrastructure of the latest VoIP/UC systems of various manufacturers, from end-user phones to call servers. This application would also report the configuration issues within the system.

NOVA V-SPY can discover all the clients and services in even a large network topology instantaneously, regardless of the manufacturers of the VoIP devices. It gathers information on the services provided by these devices and tests them with the vulnerabilities in its database. Afterwards, it reports the issues based on how critical they are.
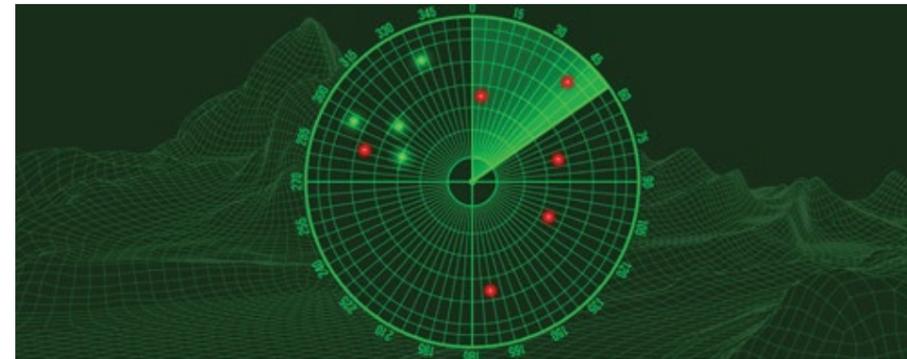
It can hide while testing to prevent being blocked by IPS/IDS and SIEM products. The tests run by **NOVA V-SPY** do not only search for vulnerabilities in the application layer but also on other OSI Layers.

NOVA Pentest Services have a holistic penetration testing strategy and performs both network and application level pentest. New attacks are created in application level with the information found on network level or vice versa. The side effects of a vulnerability in one level to the other is reported as wells as the guidelines for necessary precautions.

Key Features & Benefits

NOVA V-SPY is a modular, high performance vulnerability scanning framework aimed towards helping penetration testers and administrators that evaluate the security of VoIP applications.

- Simple web based graphical user interface
- Stateful and stateless fuzzing attacks powered with more than 10 million scenarios
- Various type of VoIP DoS, DDoS, TDoS attacks
- Fake SIP packets creation and injection
- Stateful SIP scenarios creation with drag & drop graphical components easily
- Integration to penetration tools to find the best vulnerabilities
- Port and Host scanning to target SIP enabled device over UDP\TCP
- Advanced penetration testing tools, such as the SIP Protocol Fuzzer
- Extensive reporting facilities including Expert System evaluation
- Fully automated test-case execution
- Multithread tasks-Unlimited IP address limit
- Vendor independent assessment
- Man in the middle attacks (Call recording and DTMF tone harvesting)
- CWE-CVSS standards supported reports

Components

Network Sniffing Module
Sniff all the SIP/RTP and TFTP transmissions going through the network adapter.

Reporting
Provides Security Advice Report for Vulnerabilities.

Signal/Media Manipulation Module
Toll/Traffic Frauds, Tear Down Attacks, ARP Poisoning.

Packet Creation and Flooding Module
Enables the NOVA V-SPY to simulate SIP packet creation, traffic, call generator and rich variety of VoIP DoS/DDoS flood attacks

Scanning and Enumeration Module
Conducts various scanning activities in order to obtain the required information for an attack.

Fuzzing Module
Sending numerous template based stateful fuzzy scenarios to detect security vulnerabilities on target system.

Expert Attack Module
Brute Force, Wangiri scam, Caller ID spoofing, Call recording and DTMF tone harvesting.