Privia SECURITY

Network Security Service

Professional Offensive Security Services

"Secure Network, Secure Communication!"

The information contained in this document is related to the Professional Offensive Services provided by Privia Security Information and Consulting Services and is of a general nature. All information presented in this document is publicly available.

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

“To ensure secure communication, we identify network vulnerabilities through penetration testing and help implement preventive measures against potential threats.”

Network security is one of the most critical needs for businesses in today’s digital landscape. Our comprehensive network-based penetration tests, conducted by expert cybersecurity teams, assess your network infrastructure from the perspective of a cyber threat actor to identify security weaknesses.

Our Network Security Service offers an extensive range of simulated attack techniques, including DDoS attack simulations, load testing, wireless network security assessments and Man-in-the-Middle (MITM) attacks. Each technique is designed to evaluate different aspects of your network and identify potential attack vectors. Through Attack Surface Assessment, we analyze all your digital assets to uncover weak points and protocols that could be exploited by attackers.

Throughout the entire process, our team provides a detailed report that includes the technical details of identified vulnerabilities along with tailored remediation recommendations. With our Network Security Service, our goal is not only to detect vulnerabilities but also to support you in developing the most effective strategy to remediate them.

Service Components

DDoS Testing

DDoS (Distributed Denial of Service) testing evaluates the resilience of systems against high-traffic attacks. During these tests, artificial traffic is directed at servers and networks to assess their performance under stress. This helps in planning security measures to mitigate potential service disruptions. Based on test results, recommendations such as capacity upgrades and firewall optimizations are provided.

Wireless Network Security Testing

Wireless networks are analyzed by targeting various encryption standards (e.g., WEP, WPA, WPA2). The testing process includes attempts at unauthorized access and evaluations of password cracking probabilities. Vulnerabilities related to signal strength and access points are identified, exposing potential risks. Recommendations are made to strengthen security policies and improve network resilience.

MITM (Man-in-the-Middle) Testing

MITM tests assess the risks associated with attackers intercepting communication flows, focusing on data confidentiality. The likelihood of unauthorized access to user credentials, passwords and sensitive data is evaluated. Encryption protocols are tested for effectiveness and weaknesses are identified. Practical measures are recommended to enhance communication security and ensure data is safely transmitted between source and destination.

Attack Surface Assessment

Attack Surface Assessment enables a comprehensive evaluation of all digital assets from an attacker’s perspective. Public-facing services, open ports, outdated software versions and misconfigurations are meticulously analyzed to uncover vulnerabilities. This evaluation highlights the most exposed parts of the network and prioritizes risks. Based on the gathered data and findings, detailed recommendations are provided to reduce the attack surface and enhance asset security.

Reporting

Following the network security testing, all identified vulnerabilities and potential security risks are compiled into detailed reports. Each finding is examined with technical explanations and its impact on business processes. Proposed remediation steps are shared with the organization's security team. These reports not only address current vulnerabilities but also offer long-term strategies for continuous security improvement.

FAQ

What is a network security test?

A network security test is an assessment service conducted to identify vulnerabilities and potential threats within network infrastructure. These tests analyze the security of firewalls, routers, servers and network devices, enabling the remediation of weaknesses before they can be exploited.

Why is a network penetration test important?

A network penetration test uncovers security vulnerabilities using techniques similar to those employed by real-world attackers. By identifying and addressing risks proactively, organizations can prevent data breaches and operational disruptions before any attack occurs.

How are DDoS attack simulations performed?

DDoS (Distributed Denial of Service) simulations involve overwhelming systems with a large volume of simulated traffic to test their response capacity. This process helps determine necessary infrastructure optimizations to prevent service interruptions.

What is the difference between internal and external network security testing?

Internal testing focuses on threats originating from within the organization’s network, while external testing targets publicly accessible services over the internet. Together, these approaches provide comprehensive protection against a broad range of threat vectors.

Why is wireless network security critically important?

Wireless networks are particularly attractive targets for attackers due to the limited physical protections in place. Misconfigured wireless networks can allow unauthorized access, enabling attackers to move freely within the network and access sensitive data.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "Privacy For You" we bring a fresh, innovative perspective to security and privacy—ensuring that our clients' digital futures are secure.

Privia
SECURITY