Cyber Security

Penetration Testing

Penetration testing is becoming industry standard tool for Risk and Security Assessment. We simulate environments and scenarios through Penetration testing to identify possible vulnerabilities. With different tools and practices, organizations can reduce the chances for any possible attack by a malicious user on any layer, application, hardware or network.

Security Research

We address the increasingly complex problems of protecting mission-critical systems and national cyber infrastructure through a broad range of advanced research, including insider threat detection, intrusion detection and reaction, computer network defense, smart phone security, program analysis techniques for malicious code detection, cryptography and privacy.

Wi-Fi/Bluetooth/NFC (IoT)

Despite the security concerns many of us share regarding wireless technology, it is here to stay. In fact, not only is wireless here to stay, but it is growing in deployment and utilization with wireless LAN technology and Wi-Fi as well as with other applications, including cordless telephones, smart homes, embedded devices, and more it is essential to test the security of those products.

Mobile Devices Pentest

Mobile devices or smartphones and tablets are more increcebly becoming a profitable target for hackers due to the fact they hold vast amount of personal data on the user.

Mobile Networks Pentest

We offer pentest services for mobile carriers to test out their infrastructure and services like SS7 and SMS/MMS for vulnerabilities that can be used by malicious hackers.

Cars Pentest

Cars are likely the most complex connected devices we see. The attack surface is immense – Internet, GSM, Bluetooth, RF, DAB, USB, diagnostics, telematics and more.

There are three kinds of Pentesting that we perform

Black box – No knowledge of infrastructure. Black Box penetration testing is carried out without the knowledge of the destination network or systems. Black Box test simulates a real attack. The attacker must collect all kinds of information about the target, strengths and weaknesses, defense systems, IP addresses, users.

Gray box – Limited knowledge of infrastructure. Gray box penetration testing is based on limited knowledge. Penetration tester may know the interactions between systems but not detailed internal software functions and operations.

White box – Collaboration with IT department. White Box penetration testing is done by the opposite method of black box testing. Penetration tester has full knowledge of network, systems and infrastructure. This information allows the penetration tester to focus on testing code and weaknesses ofthe systems. Security Audit for vulnerabilities is a powerful tool for information security resource. For example, audit web site for vulnerabilities – a complex of works to identify errors in the code of the site and server software, using which attackers can attack and hack the site. As a rule, this work includes such activities as scanning the site for vulnerabilities, manual analysis of site content, search and identify errors in the logic of the script and web application components.

To avoid hacking by hackers, site should be regular audits of security and to strictly follow the recommendations of experts.