WHITE ROCK CYBERSECURITY

NJECC
Leading, Inspiring, & Transforming Education through Technology

NETREAPER LABS

NJECC: When was your last Penetration Test?

Penetration Testing helps K-12 schools identify and fix cybersecurity vulnerabilities before they can be exploited. By simulating real-world attacks, schools gain insight into risks across networks, devices, cloud platforms, and applications. Testing supports compliance with regulations like FERPA and CIPA, strengthens defenses against ransomware and phishing, and builds confidence in digital learning environments.

NIST Cybersecurity Framework (CSF) I Detect & Respond

NJECC cooperative discount:

NJECC NetReaper Full Cyber Assessment (internal, external, dark web) **$11,789**
NJECC NetReaper Internal Network Assessment (pen testing) **$6289**
NJECC NetReaper External Network Assessment (pen testing) **$4689**
NJECC NetReaper OSINT/Dark Web Assessment (up to 10 domains) **$2309**
NJECC NetReaper Incident Response Planning, Assessment (80-150 pages; onsite, 2 days, includes travel expenses) **$8609**
NJECC NetReaper Tabletop Exercise (onsite, 2 days, includes travel expenses) **$8209**
NJECC NetReaper Hourly Pro Services – consulting and implementation (M-F 8a 0 6p ET) **$240/hr**

NETREAPER -LABS-

Netreaper Labs delivers cybersecurity solutions, including penetration testing, network engineering, vulnerability assessments, training, and incident response. Their expert team provides tailored reports, secure architecture design, and hands-on support to help you meet threats, ensure compliance -without breaking the budget.

In the testing, no network impact (denial-of-service) or direct exploits will be leveraged; vulnerabilities will be identified for exploit success probability. External - performed remotely. Internal - performed on-site (travel included in the cost). OSINT Dark Web - performed remotely. Assessments will also include network mapping and proposed recommendations for any remediations. Netreaper Labs Security Engineers will provide in-depth reporting and analytics of all network devices, and any subsequent vulnerabilities that are identified.

External Network Assessment

Netreaper Labs' remote assessment scans all internet-facing assets to uncover vulnerabilities, map resources, and test domain integrity. It includes web app testing and optional deep credentialed scans-delivering actionable insights with zero network impact. In this testing phase, security engineers from Netreaper Labs will run multiple web-based, or public facing network scans against the target network. This will include all devices hosted on the target network that have direct inbound Internet Access.

Base external assessment includes:

1. Full network analysis of all identified resources. This list will be compared against customer provided information for accuracy.
2. Full Domain Name Services review for all external domains, domain records, and integrity.
3. Full vulnerability testing of all external resources, including web applications.

a. Credentialed testing is optional.
b. Scans include up to 10,000 levels deep in all public facing resources.

Internal Network Assessment

Netreaper Labs' onsite assessment uncovers internal vulnerabilities through hands-on testing, including malware simulations, firewall audits, wireless/wired exams, and Active Directory reviews. In this testing phase, security engineers from Netreaper Labs will run multiple reconnaissance, vulnerability scans, and exploit utilities on the target network. This testing will be used to identify any known or unknown security vulnerability that may be on the internal network.

Odessa Criales-Smith I odessa@wrsecure.com I 214-613-1568

Contact Odessa and let's schedule your next Pen Test!

Base internal assessment includes:

1. Examination of wireless and wired connectivity and network access
    a. Includes active penetration testing for both WIFI and Wired Networks
2. In-depth review of existing security solutions, this includes firewall configurations, services, and rule audit.
3. Advanced HTTP/S Evasion Exploit testing
4. Data breach liability
5. Data archiving and recovery
6. Network intelligence and monitoring
7. Review of IP routing and physical network(s) architecture and performance
8. Full network sweep of all hosts for vulnerability detection and exploit success probability
    a. Optional credentialed or uncredentialed testing, or both.
9. Active Directory audit and review (includes Azure & 0365 configurations)
    a. Includes review of high-level domain statistics and usage
    b. User Behavior Analysis Report
    c. Full Asset Detail Report
10. Malware & Ransomware simulations
11. Firewall Configuration Review (Supports all brands, makes, and models)

OSINT/Dark Web Assessment

Netreaper Labs scans over 150 sources across the Web, Deep Web, and Dark Web to uncover leaked credentials, exposed data, phishing sites, and impersonation risks. Information contained on the Dark Web could identify existing potential exploits that may already be attacking and/or exfiltrating confidential sensitive data. This one-time scan service will provide a detailed dark web analysis of the network domain(s) including searching for lists of stolen credentials, exposed documents, leaked source code, breached IT systems, phishing websites and pages, fake accounts in social networks, possible trademark infringements, or potential squatted domain names. This scan will include all users and members of the network domains.

Deliverables & ***Scheduling***

Notes

The final report is prepared and delivered via secure file soft upon completion of the assessments. Electronic copies are provided through secure electronic delivery.

Executive Summary- A highlight of the major problems found and high-level recommendations that address the specific issues, tailored for an executive-level audience. An overall risk analysis rating relative to the discovered findings will also be assigned and described in this section.

Methodology-A complete description of all testing performed, including instructions for re-creating the test scenarios so the organization can re-test after mitigating controls have been implemented, as available.

Findings -A complete description of each major vulnerability found, including details on how it was exploited and what information or level of access was obtained as a result.

Supporting Data Archive -Archive of all tool output and vulnerability scan reports. The results of any specific testing (as applicable). For example, password policy review, wireless assessments, social engineering, and port scanning will be included. Each vulnerability or exposure will be documented in the format described above.

Contact Odessa at White Rock Cybersecurity for a formal quote.

odessa@wrsecure.com | 214-613-1568

Odessa Criales-Smith | odessa@wrsecure.com | 214-613-1568