A CVE Verified Service-Disabled Veteran Owned Small Business

Penetration Testing Services

A penetration test, also known as a pen test, is a simulated cyber-attack on a computer system, network, or web application to test its defenses. The goal of a penetration test is to identify vulnerabilities in the system that an attacker could exploit and to determine how well the system can withstand an attack.

It's important to note that penetration testing should be carried out by experienced professionals who have a thorough understanding of the latest tools and techniques used by attackers. Additionally, the testing should be done in a controlled environment to minimize the risk of damage to the system or network being tested.

The value of having a penetration test done is that it can help an organization identify and address vulnerabilities in its systems and networks and improve its overall security posture. By identifying and addressing vulnerabilities, a penetration test can help an organization reduce the risk of a security breach which could result in significant financial losses and damage to an organization's reputation. It can also help an organization comply with regulations that require regular security assessments and build trust with customers and other stakeholders by showing that the organization is taking steps to protect its systems and data.

Overall, the value of a penetration test lies in its ability to help an organization improve its security posture and reduce the risk of a security breach.

There are several steps involved in performing a penetration test:

1. Define the scope of the test: This involves identifying the systems and networks that will be tested, as well as any constraints or limitations that should be taken into account.
2. Perform reconnaissance: This involves gathering information about the target system or network, such as its IP address range, network architecture, and security controls.
3. Identify vulnerabilities: This involves using tools and techniques to scan the target system or network for known vulnerabilities, such as missing patches or misconfigured security settings.
4. Exploit vulnerabilities: This involves attempting to exploit the vulnerabilities that were identified in the previous step in order to gain unauthorized access to the system or network.
5. Evaluate results: This involves analyzing the results of the penetration test and determining whether the target system or network is adequately protected against cyber attacks. The results of the test should be documented and shared with the relevant stakeholders, along with recommendations for addressing any vulnerabilities that were identified.

Penetration Testing Costs

KNC Strategic Services Penetration Testing Services typically run between **$35,000 - $50,000** depending on the full scope of the assessment.

KNC Strategic Services
701 Palomar Airport Rd Suite 300, Carlsbad, CA 92011
(833) 562-7700 | www.kncss.com
CAGE Code: 825L7
SB/DVBE, SDVOSB/VOSB

Penetration Testing Services

The Penetration Testing Process

The assessment will simulate an advanced hacking team who is using multiple methods to obtain access into the Customer network. During the assessment, a standardized methodology and framework called the MITRE ATT&CK is utilized to maintain a consistent approach to the testing. The use and understanding of this standard provide consistency, targeting to specific compliance requirements, the ability to reproduce similar assessments in the future and a consistent reporting approach.

KNC Strategic Services will perform an assessment based on the assessment requirements as understood by KNC Strategic Services, however the MITRE ATT&CK methodology will be adapted to meet the Customer's individual needs. This adaptation will be applied through the following phases requested by the customer.

External Penetration Test

KNC Strategic Services conducts testing to identify and exploit vulnerabilities with the objective of acquiring key logical targets defined by. These targets consist of various types of data (i.e., personally identifiable information and non-public information such as customer information, credit card information, social security numbers, confidential employee information, etc.) and types of system access (Windows domain administrator privileges, root access to UNIX/Linux systems, administrative access to network devices, etc.). KNC Strategic Services will use a variety of "Open-Source Intelligence Software Tools," to mine the Internet for detailed Information about company infrastructure. Internet sources are mined for data considered open-source intelligence (OSINT). This form of collection management involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence.

The OSINT phase is designed to passively gather information about the customer. This information is mined using online resources both from the regular internet and the Dark Web. Information we are looking for during this phase includes, but is not limited to:

- IP addresses owned/in use by the customer
- Registered domains and subdomains
- Employee social media profiles
- Email addresses
- Breached/leaked passwords
- Publicly accessible documents
- DNS Enumeration
- Technologies in Use (ex: O365 vs on premise exchange, third party applications, etc.).

Once this information is gathered, the findings are sent to the client for review and verification. This information will then be used in the latter phases of the engagement.

Penetration Testing Services

KNC Strategic Services for a period of up to 10 days will attempt to attack the customers external systems leveraging ethical hacking techniques (KNC Strategic Services will perform no DDOS attempts on any customer external or internal systems/controls). These attempts will be done with little to no customer support or intervention.

If KNC Strategic Services is unable to gain access through all exhausted Blackbox methods, we will contact the customer coordinate a temporary ease of security controls to conduct an ethical hacking set of tests via grey and white hat approaches. The attacks will be conducted on all external network(s) in hopes of gaining internal access. If KNC Strategic Services can gain internal network access of the customer's network due to external factors, the test will be halted immediately. At that time, the KNC Strategic Services Team will inform the customer that external to internal security controls have been compromised and an immediate course of action can then be determined.

Internal Penetration Test

KNC Strategic Services will conduct a remote internal penetration test of the customer's internal network. KNC Strategic Services team will leverage the same ethical attack methods above, but we require full customer participation. KNC Strategic Services will ship an appliance and/or provide a VM to the customer to be plugged directly into core network. KNC Strategic Services will use common attack methods and manual attempts to circumvent existing internal security controls. The goal of the testing is to determine the potential risk associated with the vulnerabilities identified from the activities above. After verification of the information from the testing, KNC Strategic Services would then recommend a mitigation plan to secure the data and network to prevent the information from being accessed and to report on what was accessed by the review of logs from the IDS or other systems. KNC Strategic Services will perform non-credential and credentialed scans across the internal network.

KNC Strategic Services will use common attack methods and manual attempts to circumvent existing internal security controls. The goal of the testing is to determine the potential risk associated with the vulnerabilities identified from the activities above. After verification of the information from the testing, KNC Strategic Services would then recommend a mitigation plan to secure the data and network to prevent the information from being accessed and to report on what was accessed by the review of logs from the IDS or other systems.

Non-Authenticated Testing
Using no information about the client environment and taking the vantage point of a rogue insider with no credentials or account, KNC Strategic Services will perform an assessment of the network including the following items. These items are also in line and referenceable with the MITRE ATT&CK framework.

Recon and Discovery
KNC Strategic Services will attempt to locate all assets and hosts on the customer network and map said assets to IP address, hostname, and joined domain (if the assets discovered are Windows machines). This will give the customer insight as to what is on their network and if all devices on the network are company approved devices. These results are presented to the client prior to any scanning and enumeration to confirm the scope of the assessment. Testing during this phase includes the following elements:

Penetration Testing Services

- Active Scanning and Vulnerability Identification
- Host Identification and Fingerprinting
- Network Enumeration and Identification
- Account Discovery
- Cloud Infrastructure Discovery

Once this testing is complete, the results are compiled and used for further testing against the corporate network.

Threat Emulation and Kill chain Testing

Using common vulnerabilities both exploited by white hat penetration testers and black hat hackers, KNC Strategic Services will attempt to gain domain administrative access by using techniques that are known to typically evade Antivirus and SIEM/EDR systems. These methods include items such as chaining man-in-the-middle exploits such as lack of SMB signing, LLMNR and WPAD with more advanced evasion techniques using WMIExec, C# shellcode runners, domain fronting while exfiltrating data, amongst other techniques. Some of these methods are advanced and are only required if the network has a very mature network security posture. Various Resource Development and Initial Access techniques are used during this phase, including

- Compromise Infrastructure
- Establish Accounts
- Obtain and Stage Capabilities
- Trusted Relationships
- Valid Accounts

Analysis and Exploitation

Using data and findings gained while performing vulnerability scanning activities, KNC Strategic Services will examine the vulnerabilities, affected systems, and determine the best course of exploitation for the vulnerabilities. The goal of this phase is to compromise the host without causing any stability issues or triggering any defense mechanisms.

KNC Strategic Services will evaluate how effective the installed AV product is and if the product can be bypassed. This process is designed to detect blind spots within the antivirus product and identify any configuration changes that could be made to further strengthen the installed AV.

The tactics used during this phase include the following

- Command and Scripting Interpreter
- Exploitation for Client Execution
- Native Windows API
- Windows Management Instrumentation
- System Services

Credential Access and Abuse

Credential Access consists of techniques for stealing and abusing hashes, account names, passwords, and other items that could lead to host, network, or domain compromise. Some elements of this phase overlay with prior phases in the engagement process.

Penetration Testing Services

- Adversary Man in The Middle
- Brute Forcing
- Credentials and Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Modify Authentication Process
- Network Sniffing
- OS Credential Dumping
- Kerberos Abuse

Lateral Movement

Lateral movement consists of techniques that threat actors will use to enter systems, control systems, and rapidly spread infection to other systems on the network. This involves pivoting and use of multiple systems and accounts to gain privileged access to critical systems on the network. Elements of lateral movement include the following.

- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Software Deployment Tools
- Alternate Authentication Methods

The above will be used when user and/or local administrative access is gained from the hosts that are deemed in scope for the engagement.

Domain User Authenticated Testing

Using account information provided by the customer or account information gained during the assessment, KNC Strategic Services will use a regular domain user account and examine the following areas of the client environment as it relates to active directory, group policy, privilege and device and network hardening.

- Group Policy Discovery
- File and Directory Discovery
- Network Share Discovery
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Group Discovery
- Process Discovery
- Remote System Discovery
- Software Discovery
- System Service Discovery

Where relevant, findings and recommendations will be made on each of the above areas.

Penetration Testing Services

Domain Administrative Authenticated Testing

Using domain administrative credentials, KNC Strategic Services will log into each machine on the customer domain and perform the following tests.

Patching Audit

By logging into each machine on the domain, KNC Strategic Services will audit missing KB's, patches, and registry changes that are indicative of missing patches and identifies deficiencies within the patch management system and process.

Running Services Audit

KNC Strategic Services will log into each machine and determine what services are running on said machines. The goal of this assessment is to determine if the machines are running malicious or non-business-related software, identify the affected machine(s) and guide remediation of said services and associated findings.

Web Application Security Test

Customer will provide the URL for the web applications to be tested. The methodology of the testing is based heavily on the OWASP 2021 testing framework, specifically the OWASP 2021 testing guidance which is constantly being updated and revised. The scope of the assessment will involve the following audit areas as they relate to the OWASP 2021 Top 10.

1. A01: Testing for Broken Access Control
2. A02: Testing for Cryptographic Failures (previously known as Sensitive Data Exposure in 2017 framework)
3. A03: Testing for Injection Based Attacks
4. A04: Testing for Insecure Design (new for 2021)
5. A05: Testing for Security Misconfigurations (replaces XXE for 2021)
6. A06: Testing for Vulnerable and Outdated Components
7. A07: Testing for Identification and Authentication Failures (previously called Broken Authentication in the 2017 framework)
8. A08: Testing for Software and Data Integrity Failures (new for 2021)
9. A09: Testing for Security Logging and Monitoring Failures
10. A10: Testing for Server Side Request Forgery

The above testing will use both an authenticated and non-authenticated approach unless stated otherwise in the pricing table. KNC uses the above, combined with the OWASP Web Security Testing Guide (OWSTG) to perform and carry out all web application testing.

Wireless Network Security Assessment

KNC will attempt to breach the wireless security network(s) of the customer by performing various wireless network-based attacks. These attempts involve the following

- **Wireless Discovery** - KNC will perform a wireless network discovery in attempts to locate any malicious, rogue, or cloned wireless networks within the vicinity of the client location.

Penetration Testing Services

- **WPA2 Pre-Shared Key Capture:** This phase involves capturing an authentication handshake packet and using an AWS cloud-based password cracker to attempt to crack the handshake.
- **Wireless Phishing:** The process of "WIFI Phishing" is to create a rogue wireless network that replicates the corporate wireless network. Users will then join, sometimes automatically, the network and a captive portal will appear. If users enter their network credentials into the captive portal, these results are then sent to KNC, upon which the credentials are then used to potentially gain network access and access to other cloud and externally hosted services and systems.

Social Engineering

Social Engineering is an umbrella term used for several manipulative activities performed to extract information from individuals. Social engineering activities involve psychological manipulation so that a certain individual unknowingly gives up sensitive information or makes a mistake, which becomes too costly for an organization.
Our team tests the human aspect of security, relying on several advanced techniques to gain information about the network and systems. We will do a wide range of campaigns based on the desired scope.
KNC Social Engineering campaigns will attempt to access privileged information such as:

- Usernames and Passwords
- Account numbers
- Key codes
- Personnel names and Phone numbers
- Email addresses
- Systems and network technical information, networks, and non-public URLs

One of the most popular techniques used to extract information is contact via social media platforms. Attackers initiate their descent through collection and analyses of publicly available information about an individual before connecting to him or her. The attackers then initiate a conversation and start gaining victim's trust. Slowly, the attacker starts collecting the information shared by the victim and uses it for getting access to the organization's system. Social Engineering is considered one of the most dangerous techniques as it relies heavily on human errors, not software or applications. Hence, mistakes made by authorized users are harder to be predicted and identified. We propose a Spear Phishing Attack against the employees (computer users).

Device Security Review

Using administrative login credentials provided by the customer, KNC will login to each appliance to review their current configuration. The goal of the assessment is that each device is optimally set and using best practices in order minimize an attacker from breaching the external perimeter and gaining unauthorized access to the internal network. Examples of test that will be performed during the assessment are shown in the list below:

- Are there any firewall rules with "ANY" in the source, destination, service/protocol, application or user fields, and permissive action?
- Are there rules that allow unsafe services from the DMZ to the internal network?
- Are there rules that allow unsafe services inbound from the Internet?
- Are there rules that allow unsafe services outbound to the Internet?
- Are there rules that allow direct traffic from the Internet to the internal network (not the DMZ)?

Penetration Testing Services

- Are there any rules that allow traffic from the Internet to sensitive servers, networks, devices, or databases?

Active Directory Review

Using a domain user account that is provided by the customer, KNC will perform multiple queries to the Active Directory server in order to establish if users, security groups and devices on the network are using best practices. Some of queries that are performed during the assessment will look for items such as:

- Verify all workstations using LAPS.
- Verify that domain users' passwords expire.
- Verify that if domain user accounts have explicit all rights to domain joined machines?
- Verify that domain-joined machines are not using unsupported software.
- Verify that domain user accounts are not subject to Kerberoasting.

The findings found during the assessment will be combined into the final assessment report with the corresponding recommendations and remediation advice.