Penetration Testing Solution Terms

Effective October 2022

This Penetration Testing Solution Terms (SOW) is issued according to the CyFlare Master Service Agreement located at https://www.cyflare.com/master-service-agreement/ ("Agreement"). This SOW is subject to the terms and conditions in the Agreement between the parties and is made a part thereof. Any term not otherwise defined herein shall have the meaning specified in the Agreement. In the event of any conflict or inconsistency between the terms of this SOW and the terms of the Agreement, the terms of this SOW shall govern and prevail.

Definitions

- **Normal Business Hours** are Monday-Friday, 8:00 am to 5:00 pm local time, excluding state, regional and national holidays.
- **Post-Exploitation** is used to determine the value of the machine compromised and to maintain control of the machine for later use. The device's value is determined by the sensitivity of the data stored on it and the machine's usefulness in further compromising the network. The methods described in this phase are meant to help the tester identify and document sensitive data, identify configuration settings, communication channels, and relationships with other network devices that can be used to gain further access to the network, and set up one or more methods of accessing the machine at a later time.
- **Lateral movement** is when an attacker gets hold of one asset within a network and then spreads their reach from that device to others within the same network.
- **Privilege Escalation** consists of techniques adversaries use to gain higher-level permissions on a system or network.
- **Password Cracking** is obtaining user hashes using various mechanisms, such as network packet sniffing or getting password hashes from a compromised host, then attempting to decrypt the hashes to identify the plain text login credentials.
- **CyFlare External Infrastructure Penetration Test** provides organizations with the necessary information to mitigate risks posed by vulnerable external (publicly accessible) systems, including network/network security devices, websites, servers, vulnerable applications, and insecure authentication mechanisms. In addition, we leverage many threat intelligence feeds, dark web scraping, and proprietary data breach databases to uncover business risks to the organization. This will permit the companies to protect sensitive information from unauthorized access or attacks and educate their employees on their role in protecting sensitive company information.
- **CyFlare Web Application Penetration Test** provides organizations with the necessary information to mitigate risks posed by vulnerable web applications. Using an AI-powered automated penetration testing platform to analyze and exploit web applications offers a distinct advantage over manual web application penetration testing. Unmatched efficiency and accuracy are two of the most prominent benefits. We allow our clients to obtain an in-depth analysis of their web application's security posture with zero false positives while delivering rapid, actionable results. A bonus of this offering is the ability to directly integrate automated web application penetration testing into CI/CD (continuous integration, continuous delivery) workflows. This unmatched ability to conduct comprehensive penetration testing during pre-deployment and post-deployment of web applications enables our clients to integrate secure coding into their development lifecycle effortlessly.

- **CyFlare Internal Penetration Test** provides organizations with the necessary information to mitigate risks posed by vulnerable systems inside their enterprise, including network/network security devices, workstations, servers, printers, peripherals, vulnerable applications, and insecure authentication mechanisms. Using a machine-based penetration test, we deploy hundreds of hacking tactics and techniques without the possibility of human error or fatigue. This allows for a safer penetration test and a continuous penetration test during the allotted timeframe covering a more extensive scope of enterprise assets than is possible by humans. In addition, automated penetration testing verifies security policies and their proper implementation, pointing to outliers and exceptions in security measure instrumentation.
- **Corporate Risk Exposure & Intelligence** leverages the art of dark web scraping, monitoring, and analysis to identify and correlate information on an organization that can be used (or is already being used) against an organization by a malicious actor. CyFlare's risk validation offering is unique. It includes network intelligence about the risks of an organization's Internet-facing networks, e-Crime intelligence, social media monitoring, financial fraud intelligence, compromised credential monitoring, and botnet intelligence (identify botnets threatening your reputation and customers). The real differentiator, however, lies in the operatives. CyFlare partners with and contracts dark web operatives to execute on-demand External Threat Reports (ETRs).

Leveraging these operatives, we can provide intelligence on deep and dark web sources to gain a comprehensive insight into the resources and information bad actors have in their arsenal to attack and intimidate organizations. We aim to provide this information before it is used against an organization for malicious purposes and to prevent attacks.

Our focus is on identifying exploitable threat vectors and providing proactive remediation recommendations to prevent attacks. Remediation collaboration with CyFlare's team is an additional $250/hour fee.

Assessment Methodology

CyFlare uses a mix of automated and manual processes to identify and exploit vulnerabilities in an organization's IT security perimeter.

External Infrastructure Penetration Tests

1) Initial Plan & Validation
    a) Provided all information in the required scoping documents has been completed
        i) If necessary, validate that the attack IP address is correctly whitelisted on the Client's infrastructure
2) Reconnaissance / Enumeration
    a) Conduct Open Source Intelligence (OSINT) to identify publicly accessible data and domains/sub-domains
    b) Create custom attack dictionaries based on OSINT, combined with Threat Intelligence, Dark Web Scraping, and credentials discovered in data breaches
        i) Automated weak password identification
    c) Network Discovery Scan - Active ports and services for target IPs, domain names

CyFlare, LLC
21 Goodway Drive, Suite L4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com

3) Vulnerability Scan
   a) Scan IPs and URLs for known vulnerabilities
      i) Includes Operating Systems, Applications, and Network Devices
4) Exploit
   a) Review results of the Vulnerability Scan and identify potential exploit attack vectors
   b) Conduct exploit reconnaissance to determine optimal attack vectors and prioritize exploits
   c) If logins are identified, leverage custom attack dictionaries to compromise
   d) Attempt exploits for potentially exploitable vulnerabilities and record results
      i) If exploits are successful, criticality will be measured, and if it is determined that an exploitable vulnerability or compromised account is critical or severe, the X point of contact will be notified immediately
   e) If agreed upon, conduct post-exploitation efforts to identify possible lateral movement and further exploitation either between systems or deeper inside the client organization
5) Review Results
   a) Discuss findings and recommendations
   b) Prepare and present the full set of detailed reports (PDF, XLS)
   c) Define action items & near-term recommendations
   d) Provide suggested timeline and milestones for action items
   e) Questions & Answers

Internal Penetration Tests

1) Initial Plan and Validation of Readiness
   a) The tested segment will include a **maximum of 1,000 Active IP Addresses** (hosts/devices).
      i) This includes segments in other geographic locations pending validation of remote access and network configurations
   b) **For remotely executed internal penetration tests**, the following technical requirements must be met:
      i) Access to a physical Windows or Linux machine with administrative user privileges
         (1) The physical machine will be hosted on an active user LAN segment
         (2) The physical machine will be connected via an Ethernet cable (not WiFi)
      ii) TCP/443 outbound (static IP address can be provided if necessary)
      iii) Whitelisting of CyFlare asset MAC Address if NAC or 802.1x enabled
   c) Start initial sanity check for discovery (up to 25 IPs), identify initial scope, vulnerabilities, and password sniffing
   d) Initial validation scan to run for a maximum of 10 – 15 minutes
2) Execute Primary Penetration Test
   a) Review the initial discovery scan
   b) Define and execute primary penetration testing tasks for up to 72 hours
      i) Based upon accepted parameters under the Scope of Work section of this Agreement
3) Execute Supplemental Penetration Tests (optional based on the length of primary run)
   a) Define additional targeted testing scenarios such as "Grey-Box" to evaluate user privileges, lateral movement, password policy complexity, etc. Testing duration: up to 24 hours
   b) Validate key domains and security controls. For example:
      i) Endpoint Protection - test multiple methods to bypass the Endpoint Protection (AV/EPP) – validate detection/response
      ii) Overall Detection level of activity by the SOC. Test multiple scenarios in different "Stealthiness" levels. Validate detection and identify how to improve detection mechanisms
      iii) Privileged Users: validate control over privileged users, including domain users and local

administrators

iv) Open Shares are both authenticated as well those accessible via low privileged domain users. Check for accessibility of sensitive user data

4) Review Results
   a) Discuss findings and recommendations
   b) Prepare and present the full set of detailed reports (PDF, XLS)
   c) Define action items & near-term recommendations
   d) Provide suggested timeline and milestones for action items
   e) Questions & Answers

Web Application Penetration Tests

1) Initial Plan & Validation
   a) Provided all information in the required scoping documents has been completed
      i) If necessary, validate that the attack IP address is correctly whitelisted on the Client's infrastructure
2) Execute Penetration Test

   Our automated web application penetration testing does not need or use a vulnerability database or patterns. Due to the complexity of web applications, vulnerability scanners typically lead to many false positives as they rely on patterns and signatures.

   a) Reconnaissance / Enumeration
      i) Automated collection of all host information from the Client's environment and web platforms associated with the defined targets
      ii) Using the collected information, train unsupervised machine learning models to develop classifiers associated with the collected information dynamically
   b) Attack
      i) Using the classifiers developed from the reconnaissance phase, dynamic composition of payloads and attack vectors are created.
      ii) Execution of discriminatory process to reduce the search space for attack vectors and unnecessary payloads unfit for the target environment
      iii) Attempt exploitation against web applications

3) Review Results
   a) Discuss findings and recommendations
   b) Prepare and present the full set of detailed reports (PDF, XLS)
   c) Define action items & near-term recommendations
   d) Provide suggested timeline and milestones for action items
   e) Questions & Answers

Corporate Risk Exposure & Intelligence

- Intelligence Collection and Analysis
- Compromised credentials based on corporate email domain
- Network device exposure, based on client external IP net ranges
- Global field operative analysis of the named Client's dark web status if applicable.
- Threat analyst report preparation and recommendations if applicable

Intelligence correlation report to include correlation analysis of all Client provided information and extracted/discovered information

Scope of Work

CyFlare shall provide the Services and Deliverable(s) to meet the scoped environments provided by the Client in a completed scoping document. Any services not specifically detailed herein or in the scoping document are excluded from the services provided under this SOW.

Deliverable Materials

External penetration testing reports:

1. Executive summary report
2. Detailed findings report, including prioritized remediation guidance

Internal penetration testing reports:

1. Executive summary report
2. Detailed findings report, including prioritized remediation guidance

Corporate Risk Exposure & Intelligence report:

1. A comprehensive report of analyzed intelligence collected
2. Current compromised credentials list
3. Access details for compromised account monitoring subscription

Additional formal deliverables can be defined for project-specific work and agreed upon as deemed desirable by the Client.

Timelines

The projected time to completion for this project will be four weeks unless mutually agreed upon by both parties.

This timeline is identified as follows:

1) Engagement start date: Date of test execution
2) Engagement end date: The date the final report is delivered

CyFlare and Client Responsibilities

In the delivery of the service, CyFlare's responsibilities will be to:

1) Provide trained and certified personnel to perform the activities identified in this document's Scope of Work Section.
2) Perform the activities identified in this document's Scope of Work Section promptly.
3) Respond promptly to the Client's requests to perform services included in the Scope of Work or amended Scope of Work.

Provide all software and hardware required to perform tasks defined in the SOW.

In the delivery of the service, the Client's responsibilities will be to:

1) Provide access to client systems as required as part of the Scope of Work.
2) Respond promptly to requests for access to client site(s), device login, configuration, and security information. Any delays may cause delays in the agreed-to timeline.
3) Provide complete, accurate, and up-to-date information as necessary for CyFlare to complete services.
4) Provide external POCs for services hosted externally to the Client, as necessary.

**If there is a schedule delay not exclusively caused by CyFlare, or a change in scope or deliverables, there may be a mutually agreed-to price increase.*

CyFlare, LLC
21 Goodway Drive, Suite L4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com

Fee Schedule

This engagement will be conducted on a one-time basis. The services will be invoiced, and payment will be due as indicated in the CyFlare quote attached.

The Client will be invoiced monthly for above-and-beyond T&L expenses (including, without limitation, costs and fees associated with meals, lodging, local transportation, and any other applicable business expenses). All expenses will only be incurred with prior Client approval.

Completion Criteria

The Contractor shall have fulfilled its obligations when it accomplishes the Contractor activities described within this SOW, and the Client accepts such activities and materials without unreasonable objections. No response from the Client within 2-business days of deliverables being delivered by the Contractor is deemed acceptance.

CyFlare, LLC
21 Goodway Drive, Suite L4
Rochester, NY 14623

P: +1 877-729-3527
E: sales@cyflare.com