Cyber Assessment/Testing

Service Overview

46040 Center Oak Plz, Ste 165
Sterling, VA 20166-6595

phone 703-203-7500

Chris@disruptivesol.com
www.disruptivesol.com

Table of Contents

Service Outlines: Cyber Assessments and Testing

Vulnerability Assessments [Documenting the Infrastructure]

Discovering in-scope customer assets and their public/private services, identifying software version information, and then pairing this information with data on the most up-to-date Common Vulnerabilities and Exposures (CVE's) and threat intelligence. No attempts at exploitation will be made. Operational Security (OPSEC) will not be a factor. Data for these engagements can either be customer-supplied (i.e. Disruptive takes the customer's asset and vulnerability data from an existing product) or Disruptive can collect its own data using off-the-shelf, corporate vulnerability management tools (like Nessus/Nexpose/Qualys) using both authenticated and unauthenticated discovery.

Disruptive produces a report for the customer outlining the greatest risks to their security (by enriching the data with experience, open-source intelligence (OSINT), threat intelligence, and existing customer data), provide steps/recommendations for vulnerability remediation/risk-mitigation, and offer validation, post remediation. Disruptive may perform the remediation for the customer. Compared to Penetration Testing, this service does the most to avoid exploitation and security alert generation, while spending more time documenting observed over plausibly exploitable vulnerabilities. Compared to all other services, this is an exhaustive list of all vulnerabilities and weaknesses that does not necessarily represent how likely or plausible a customer compromise would be. Includes secure code review, as a service.

Penetration Testing [Testing the Infrastructure]

Discovering in-scope customer assets and their public/private services, identifying software version information, examining application functionality, and then pairing this information with data on the most up-to-date Common Vulnerabilities and Exposures (CVE's), Common Weakness Enumeration (CWE's) concepts, threat intelligence, and active attempts at exploitation. Operational Security (OPSEC) will not be a factor. Disruptive will collect the data for these engagements by using both off-the-shelf, corporate vulnerability scanning tools (e.g. Nessus, Nexpose, Qualys, Burp) and our own collection of exploitation tools (e.g. tools, custom scripts, anything in Kali, our own capabilities).

Disruptive produces a report for the customer outlining our findings during the engagement, ranking said findings by risk (i.e., a combination of the Common Vulnerability Scoring System (CVSS v3) and threat intelligence), providing steps/recommendations for vulnerability remediation/risk-mitigation, and offer validation, post remediation. Disruptive may perform the remediation for the customer. Compared to Vulnerability Assessments, this service concentrates on exploiting all observable services over comprehensively documenting all possible vulnerabilities. Compared to all other services, this is an exhaustive demonstration of risk on all observable in-scope vulnerabilities and weaknesses, suggesting areas in which customers may experience a compromise.

Red Teaming [Testing the SOC]

Defining the scope of the engagement, establishing how much information Disruptive will have about the customer's environment, covertly identifying vulnerabilities, and demonstrating risk via exploitation. Operational Security (OPSEC) will be a factor - Red Team operations will start engagements with means and goals at the pinnacle of stealth and complexity, slowly working towards louder, less-stealthy attacks

and methods. Red team engagements will be conducted via mostly manual efforts, using a diverse set of publicly-available, custom, and private tools, scripts, and attack infrastructure, depending on the scope of the engagement. Disruptive produces a report with a narrative describing what the red team did, why/how they did it, and how to prevent it, in support of compromising the in-scope infrastructure. Final reporting should target Security Operations Center (SOC) analysts and internal security teams. This differs from Purple teaming by limiting SOC/security-team interaction to post-engagement communication, serving as a test of the customer's security infrastructure and operations. This differs from all other services by demonstrating what a compromise looks like versus what the customer would have detected, through a limited number of researched attack paths.

Purple Teaming [Teaching the SOC]

Defining the scope of the engagement, establishing how much information Disruptive will have about the customer's environment, establishing communication channels with the customer's Security Operations Center (SOC), covertly identifying vulnerabilities, demonstrating risk via exploitation, and actively working with SOC analysts to improve detection and preventative capabilities. Operational Security (OPSEC) will be a factor - Purple team operations will start engagements with means and goals at the pinnacle of stealth and complexity, slowly working towards louder, less-stealthy attacks and methods, to identify where blue team alerting and protections break down. Purple team engagements will be conducted via mostly manual efforts, using a diverse set of publicly available, custom, and private tools, scripts, and attack infrastructure, depending on the scope of the engagement.

Disruptive produces a report with a narrative describing what the team did, why/how they did it, how well the SOC was able to detect/prevent activity, any steps taken by the SOC to improve abilities, and recommendations for improving SOC functionality, in support of compromising the in-scope infrastructure. Final reporting should target Security Operations Center (SOC) analysts and internal security teams. This differs from Red teaming by establishing constant communication with the SOC/security-team, allowing the customer to tailor their experience and actively improve blue team skills. This differs from all other services by demonstrating what a compromise looks like directly to the customer's detection capabilities, through a limited number of researched attack paths, while building real-time improvement and knowledge.

Adversary Simulation [Exercise Training with the SOC]

Defining an extremely loose scope and end-goal including customer production abilities, exercising extreme Operational Security (OPSEC), identifying attack paths, and executing direct attacks against operations. Communications with the customer after the engagement has begun are kept to an absolute minimum. All technical details of the engagement are time-stamped and recorded. Experimentation will be kept to a minimum, using mostly tested and verified attack capabilities.

Disruptive will produce a report that tells a story, from the perspective of the adversary, on how the end-goal was achieved. This service differs from all other services by removing the ideas of scope and customer safety, where Disruptive becomes an adversary.

Common Toolsets

Coding/Scripting:
Python, PowerShell, C#/VBScript/Anything .NET, C/Java, Ruby, Perl, Javascript, Bash, Batch, Lua, Go, Rust, SQL, HTML/CSS, TypeScript, packet dumps, various data formats (e.g. XML, JSON, YAML), Assembly

Development Environments:
Visual Studio/Code, PowerShell ISE, Notepad++, Vim, Eclipse

Reconnaissance:
Nmap, Wireshark/tcpdump, OS-native tools (e.g. ping, netstat, arp, traceroute, nslookup, dig, dir/ls, cat, powershell), dnsenum/map/recon/walk, snmpwalk/enum/check, OSRFramework, Recon-ng, Spiderfoot, parts of Metasploit, 3rd-party services like Shodan, Google/Bing/DDG, Tor, hardware taps, custom tools and scripts

Vulnerability Discovery:
Nmap, Metasploit, Burp Suite, Wireshark/tcpdump, Bloodhound, pacu, hashcat, hardware taps, custom tools and scripts

Exploitation:
Metasploit, Burp Suite, Social Engineer Toolkit, pacu, ysoserial, sqlmap, RouterSploit, PRET, ntlmrelay/proxy, service honeypots, various hardware RF packages, custom tools and scripts

Research:
Ghidra, BinaryNinja, Ida, VMware/VirtualBox/QEMU, gdb, WinDbg, various hardware snooping tools, Burp Suite, Google

Possible Approach: Vulnerability Assessment and PenTesting

Disruptive Solutions conducts custom penetration test in either a covert or overt fashion, located onsite or offsite. The project is typically conducted in two phases: Phase I consists of Reconnaissance, Footprinting, and Vulnerability Scans, and Phase II moves on to Penetration Testing and Exploitation of the network.

Phase I: Reconnaissance, Footprinting, and Vulnerability Scans

During this phase, Disruptive Solutions may:

- Conduct reconnaissance of the organization to identify exposed data and network openings, which could be exploited by an attacker
- Footprint the network to ascertain the network's topology and identify resources that would likely be targeted during an attack
- Conduct vulnerability scans of the network. The vulnerability scans may consist of:
    - Enumeration of devices on the network
    - Identification of operating systems
    - Verification of configuration settings
    - Identification of vulnerabilities and a listing of those vulnerabilities with known exploitations
    - Analyzing servers and workstations to determine:
        - Security configuration settings
        - Administrators and administrator groups
        - User accounts
        - Network shares and permissions
        - Group policy settings
        - Auditing functionality and logging
        - Missing security updates

Phase II: Penetration Testing and Exploitation

The penetration test consists of a variety of methodologies, tactics, techniques, trade craft, and exploits for the purpose of:

- Identifying the methods and vulnerabilities available to elevate user privileges on the client's network
- Conducting an exploitation of one or more vulnerabilities identified on the network with the intention of obtaining access to sensitive information stored within the network.
- Moving through the client's network by exploiting vulnerabilities within a network to gain access to additional network hosts and the sensitive information contained therein

At the conclusion of the penetration test, Disruptive Solutions provides a detailed report listing:

- What level of privileges were obtained
- How those elevated privileges were obtained
- What systems were compromised
- What sensitive data would these compromises expose
- Recommendations to "harden" the security posture of the network

Assumption of Breach Option

Many customers have taken the approach of assuming a breach will happen and prefer to concentrate on answering whether an attacker can successfully move throughout their network. Given a foothold into the client network, Disruptive Solutions can start the penetration test with an "assumed breach" scenario for the purpose of identifying:

- The methods and vulnerabilities available to elevate user privileges on the client's network with the ultimate goal of obtaining Domain Administrator privileges

- The ability to move through the client's network by exploiting vulnerabilities within a network to gain access to additional network hosts and the sensitive information contained therein

The penetration test consists of a variety of methodologies, tactics, techniques, trade craft, and exploits. Disruptive Solutions proposes the test be conducted in three (3) phases:

1. Access Phase: provide the client with the exploit, receive credentials, and gain access
2. Review and Planning Phase: once provided with access, Disruptive Solutions will conduct an initial review of the network, footprint, and security measures in place. This review will be used to create an attack plan and identify areas for potential vulnerability research.
3. Execution Phase: consists of a series and cycles of probes, executions, and reach-back research to facilitate network movement, access to information, and escalation of privileges.

Possible Approach: Adversary Simulation/Purple Team

Adversary Simulation Exercises are conducted in a Purple team fashion and involve a combination of methodologies to include Penetration Testing, Red Teaming, and Threat Hunt Training.

Adversary Simulation/Purple Teams

Disruptive Solutions provides a customized adversary simulation using known threat actor profiles. This method of testing achieves the goals of a traditional penetration test with the added benefit of training your security team on identification, response, and hunting of real threats.

The Adversary Simulation methodology includes:

- Adversary profiling of the types of malware used, network signatures, artifacts left on compromised systems, and general actor objectives
    - Select from a pre-profiled list, or request a specific threat actor
- Over-the-wire indicators (e.g., HTTP Get / Post Requests)
- Known Adversary TTPs
    - Active during known operating schedule
    - Mimic files dropped onto system
    - Mimic registry key entries
    - Target same information as threat actors
- Hosted infrastructure including redirectors, C2 servers, spear phishing servers, and malware hosting servers

The benefits of the customer Adversary Simulation include:

- Allows Security Team to conduct a full response plan to include detection, forensics, threat intelligence and response
- Coordination with simulation director to release Indicators of Comprise (IOCs) after a predetermined amount of time has elapsed to assist with threat hunting efforts
- Learn to recognize and hunt for malicious activity and identify threat actor by IOCs
- Provide instant feedback via hotwash/review with Security Team or Service after each threat actor iteration to evaluate and discuss their ability to detect and identify the threat

- A final report that documents the adversary profile, kill chain, infrastructure creation, target exploitation, Security Team coordination/response times, evaluation of support/coverage/resources