Cybersecurity and Infrastructure Security Agency

Department of Homeland Security
Cybersecurity and Infrastructure Security Agency
CISA Assessments

CISA Assessments Services Catalogue
Version 4

REVISION HISTORY

Date	Version	Description	Approved By
August 29, 2011	0.1.1	Initial document	
Sept. 1, 2011	0.1.2	Incorporated comments from DHS reviewers	
December 1, 2011	1.0	Accepted and Approved by DHS	D. Link
May 1, 2012	2.0	Revised and Approved by DHS	D. Link
September 2013	2.1	Integration into ROE, with edits	
October 23, 2013	2.2	Updated Services, merged external and internal into one, will be separated based on IP addresses	R. Karas
April 21, 2016	3.0	Added new service and refreshed format and descriptions	D. Link
August 28, 2017	3.2	Removed Threat Identification	D. Link
March 9, 2018	3.23	Added War Dial	D. Link
March 9, 2018	3.23	Added Validated Architecture Design Review	R. Aikey
April 5, 2019	4.0	Added Red Team Assessment, reorganized, and updated for CISA establishment	G. Hummer

1 Risk and Vulnerability Assessment (RVA)

A CISA Assessments Risk and Vulnerability Assessment (RVA) is a one-on-one engagement with stakeholders that combines open-source national threat and vulnerability information with data collected through remote and on-site assessment activities to provide actionable risk analysis reports with remediation recommendations prioritized by severity and risk. An RVA includes the following components:

A. Penetration Test

Penetration testing evaluates the security of the requesting organization's cyber assets by attempting to gain unauthorized access into the computer system, application, or network. The process involves an active analysis of the requesting organization's cyber assets for any potential vulnerability that could result from poor or improper configuration, known and unknown software/hardware flaws, or operational weaknesses in processes and technical countermeasures. Data gathering elements such as network mapping and discovery and vulnerability scanning are a primary part of the penetration testing process. Network mapping and discovery consists of identifying assets that are accessible on an assigned IP address within the targeted IP space or network range(s). Vulnerability scanning identifies IT vulnerabilities associated with requester systems that are potentially exploitable by attackers. The analysis is carried out from the position of an adversary/hacker and involves active exploitation of any discovered vulnerabilities that allow our team to compromise cyber assets. The team will attempt to gain access and leverage that access to elevate privileges, pivot, and spread access to other hosts throughout the targeted scope.

A findings report will detail the results of the penetration test, the risk exposure for requester systems, and demonstrate how vulnerabilities can be exploited to gain access to such systems. The findings report will include suggested remediation actions to lower a requester's risk exposure.

During the Penetration Test, CISA will not delete any live data, will make every attempt not to disrupt current operations, and will not perform any Denial of Service attacks. The team will focus on discovering and exploiting vulnerabilities that provide greater access to the system or network that is in-scope of testing. CISA will limit its testing to the scope identified in the Rules of Engagement with the requester, even if the test team identifies avenues of access to or through other networks or cyber assets. To perform this service, the CISA team may use one or more of a requester's unique seal, trademark, name, or insignia in phishing emails or other services, and requester hereby grants CISA the right to use such seal, trademark, name, or insignia. The requester is responsible for obtaining any internal authorizations necessary for CISA use of its seal, trademark, name, or insignia, consistent with applicable law and procedures.

<u>Associated Activities</u>

- Perform basic open source information gathering of requester's Internet reachable network presence
- Perform active network host and service identification through the use of port scanning and host enumeration

- Perform exploitation of identified vulnerabilities. This will include automated tools and scripts that attempt to exploit systems as well as manual testing
- Attempt to access requester systems, applications, and networks through identified vulnerabilities

Deliverables
- Network enumeration report detailing system exposure (accessible hosts, services, and network ports)
- Host exploitation success / failure report (Validation of Vulnerabilities identified in Vulnerability Scanning)
- Findings report detailing vulnerabilities in requester's network and recommended remediation steps
- Narrative explanation detailing steps in the penetration process resulting in achieved access

B. Technical Phishing Assessment

The technical phishing assessment is focused on technical boundary testing will test the response and detection capability of an organization if an email phishing attack was successful. The team will generate and send a specially crafted phishing email to a targeted list of email addresses provided and agreed to by the requesting organization's technical point of contact. If a user (victim) happens to accept the email and open the attachment or click on the supplied link, the email payload will establish a backend communications channel to a command and control server at CISA. This command and control server allows the CISA team to communicate with the victim machine.

If the requesting organization has also selected the Penetration Test described earlier in this document and the victim machine is in scope, the CISA team will use the compromised machine to attempt to discover and pivot to additional hosts on the requester network. This will replicate real-life hacking attacks and security breaches from the phishing attack vector. The CISA team will identify how it gained entry and what additional access the team achieved. The CISA team will ensure firewall rules are in place to accept replies that originate from requester network ranges and that replies from non-requester networks are denied/dropped at the firewall. To perform this service, the CISA team may use one or more of a requester's unique seal, trademark, name, or insignia in phishing emails or other services.

Associated Activities
- Conduct a controlled Spear-Phishing campaign against pre-approved requester email addresses

Deliverables
- Spear Phishing campaign statistics, findings, and associated remediation steps
- Narrative explanation detailing steps in the penetration process resulting in access

C. Web Application Assessment

The Web Application Assessment provides a deep and detailed look at the security a specific

application, using automated scanning and/or manual testing.

The Web Application Scan service identifies web application-specific vulnerabilities and assesses the security posture of selected requesting organization's web applications against the Open Web Application Security Project (OWASP) Top Ten common vulnerabilities. The service looks for a wide variety of vulnerabilities such as Cross-Site scripting, SQL injection, application configuration errors, and other specific application problems. The results detail the risk exposure for a requester's web applications and demonstrate how adversaries could exploit vulnerabilities in these applications. CISA will provide suggested remediation actions to lower a requester's risk exposure. Depending on web application accessibility, CISA may conduct assessment activities remotely or onsite at the requester location. CISA may require the requesting organization to create accounts for the CISA team to access a web application.

Aside from automated scanning, a Web Application test may also involve manually engaging with and providing input to a running web application, without knowing the inner workings of the application itself, in order to find and exploit vulnerabilities. The penetration test uses knowledge gathered from a web application scan to exploit vulnerabilities discovered during the scan. CISA may also perform a manual review of the web application to identify flaws in business logic, application behavior, and a high-level examination the source code. Communications between the web client and the servers that make up the web application environment are also reviewed using a proxy for data manipulation/submission on different input fields. These tests will attempt to determine if application accounts are utilizing proper access controls and verify if adversaries can achieve unauthorized access to protected resources via the web application attack vector. The tests also verify if the application properly sanitizes all data submitted by application users.

Associated Activities

- Perform Web Application vulnerability scanning
- Perform Web Application penetration testing by exploiting identified vulnerabilities
- Perform manual Web Application security review

Deliverables

- Web Application Security Assessment Report and recommended remediation steps
- Narrative explanation detailing steps in the penetration process resulting in achieved access

D. Wireless Assessment

The Wireless Assessment includes wireless access point (WAP) detection, penetration testing or both and is performed while onsite at a requesting organization's facility.

Wireless Network Detection will occur during an onsite portion of a RVA assessment. The CISA team will conduct a walkthrough of requester facilities to identify and evaluate Wireless Communications and Wireless Access Points that exist within a requester's physical office location(s) and attempt to identify any rogue access points.

Wireless Penetration Testing analyzes the current wireless infrastructure to identify weaknesses and attempts to exploit them to gain additional access to a requester network. During the Wireless Penetration test the CISA team identifies WAPs and attempts to exploit and gain access to the network through those WAPs. Once the CISA team gains access to the wireless network, the team will attempt to map out the network and discover vulnerabilities. This service cannot be performed remotely.

Associated Activities

- Perform Wireless Site Survey
- Attempt to access requester's Wireless Access Points and internal networks

Deliverables

- Inventory of WAPs that are accessible from the requester environment
- Results report of requester network exposure from the guest wireless perspective

E. Operating System Security Assessment

The Operating System Security Assessment (OSSA) service assesses the configuration of select host operating systems (OS) against standardized configuration baselines (United States Government Configuration Baselines (USGCB) or Center for Information Security (CIS) recommended baselines. The results identify deviations from required baselines and recommended remediation steps to bring configurations into compliance. All assessment activities are conducted onsite at the requesting organization's location or over a secure connection the requester has initiated with the testing team. At a minimum, administrator or root-level access is required for this service.

Associated Activities

- Perform automated host assessment scanning against select requester OS

Deliverables

- Host/System security assessment report and recommended remediation steps

F. Database Assessment

The Database Assessment assesses the configuration of selected databases against configuration baselines in order to identify potential misconfigurations and/or database vulnerabilities. For example, the service will attempt to identify holes, weaknesses and threats to the information stored within the database. The CISA team will identify default usernames and passwords, identify patch-management issues, and review various other security vulnerabilities and configuration problems. The results identify deviations from required baselines and, insecure configurations that are applied on assessed databases. In addition, recommended remediation actions are provided. All assessment activities are conducted onsite at the requesting organization's location or over a secure connection the requester has initiated with the testing team. As part of the service a DBA username and password with admin privileges are required.

Associated Activities

- Perform network database discovery
- Perform automated database vulnerability scanning

Deliverables

- Database Security Assessment Report

G. War Dial

War Dialing involves actively scanning or dialing a requesting organization's phone numbers to identify hosts, systems, or devices that are connected and accessible via modems and other phone connections. This type of connectivity typically involves a slower speed connection and resides outside of the security perimeter, which can allow direct access to the target host, system, or device.

The CISA team will dial lists of phone numbers or exchanges provisioned by and assigned to the requester, as specified and provided separately to CISA by the requester. By listening for a response to each call, the CISA team will identify if any phone numbers are connected to a host, system, or device. When a number is called, CISA will listen for approximately 5-10 seconds to determine if any devices are available for hardware handshake; Human users or voice mail services that answer the call will experience 5-10 seconds of silence following by a disconnection.

If the requesting organization has selected the Penetration Test offering described earlier in this document, the information gathered during the War Dial will be used to attempt to access any connected host, system, or device identified during the war dial, identify what security controls are in place on the telephone-connected devices or networks, and determine whether the CISA team can pivot or identify alternative gateways into other assets within the environment.

Associated Activities

- Perform host, system, or device identification through war dialing

Deliverables

- War Dialing statistics, findings, and associated remediation steps

2 Phishing Campaign Assessment

The Phishing Campaign Assessment focuses on user behavior and measures the susceptibility of a requesting organization's personnel to social engineering attacks, specifically email phishing attacks. The CISA team will generate and send a series of phishing emails to a targeted list of email addresses provided and agreed upon by the requester. Within the emails, a user are asked to click on a suspicious/malicious link. The team will be able to track the percentage of users that clicked on the link as well as the time it takes users to click the link, providing insight into the effectiveness of a security awareness program or measure the susceptibility of an attack from this vector. During the behavior-based phishing assessment there is no attempt to compromise the workstation or network; the assessment is only a metrics-gathering and training validation exercise. To perform this

service, the CISA team may use one or more of a requester's unique seal, trademark, name, or insignia in phishing emails or informative landing pages. The requester is responsible for obtaining any internal authorizations necessary for CISA use of its seal, trademark, name, or insignia, consistent with applicable law or procedures. All testing activities are conducted from CISA testing facilities.

Associated Activities

• Conduct a controlled phishing campaign against pre-approved requester email addresses

Deliverables

• Phishing campaign statistics, findings, and associated remediation steps

3 Validated Architecture Design Review (VADR)

The Validated Architecture Design Review (VADR) is a table-top assessment based on standards, guidelines, and best practices. The assessment can encompass both Information Technology (IT) and Operational Technology (OT) systems and networks. The assessment provides an architecture design review, system configuration and log file review, and a sophisticated analysis of network header data and related non-content provided by the requester.

CISA will request Network and system information for use during the assessment. Some of the requested network information may consist of access control lists, Virtual LANs, Virtual Private Networks/remote connection points, routers/switches/firewall locations and details, and some captures by the requesting organization of network header data and similar non-content information. Requested system information may include Operating System inventories, Internet Protocols (IP), inventories of connections to other systems, approved application lists, log files, hardware inventory lists, software inventory lists, and group policy configurations.

Associated Activities

- Review the asset owner's IT and OT system and program practices against best practices by asking a series of detailed questions about system components and architectures, as well as operational policies and procedures
- Perform Network Architecture Review
- Perform Network Header Data Analysis
- Perform System Log Review
- Review system configuration files

Deliverables

- Report detailing observed strengths and discoveries identified
- Each discovery identified is linked to the Cybersecurity Framework, NIST 800-82, or NIST 800-83, an associated consequence, and a recommendation for mitigation

4 Red Team Assessment (RTA)

A CISA Assessments Red Team Assessment (RTA) is a comprehensive evaluation of an IT environment where the CISA team attempts to gain unauthorized access into and persistence within the requesting entity's network through emulation of Advanced Persistent Threat (APT) activities. The CISA team will quietly connect to and probe a requesting entity's network using APT tactics, techniques, and procedures to determine the security posture of the entity's cyber assets and the effectiveness of their response capabilities to a sophisticated adversarial presence.

As CISA specifically designs RTAs to test the people, processes, and technologies defending a network, only a bare minimum of employees at the requesting organization should be aware of CISA conducting an RTA. Ideally, only one or two trusted and strategically-positioned requester representatives would be aware of an in-progress RTA.

RTA Phase One consists of an emulation of APT tactics, techniques, and procedures using publicly available tools and data to surreptitiously access, navigate, and persist in a customer's environment. The CISA team will create custom phishing emails for targeted users which will induce the individuals to compromise the security of their system and network.

Depending on the unique aspects of each assessment, the CISA team could:

- Perform basic open source information gathering of any aspect of requester's Internet reachable network presence
- Perform active network host and service identification through the use of open source information gathering and scanning
- Perform exploitation of identified vulnerabilities and misconfigurations. This may include manual tools and scripts that attempt to exploit specific system vulnerabilities
- Attempt to access requester systems, applications, and networks through identified vulnerabilities or misconfigurations
- Utilize social engineering to collect information from requesting entity employees to be used to access the requesting entity's network
- Utilize previously compromised information that may be publicly available to access the requester's network resources
- Physically access a customer environment and IT infrastructure with weak physical security measures
- Attempt to introduce compromised media into the customer's environment
- Establish a presence within the network environment by creating user, remote, and administrator accounts on necessary workstations, servers, or network devices, documenting all accounts created.

The CISA team will not:

- Access any IP addresses that are out of range of the provided authorization
- Utilize Disruption or Denial of Service attacks, whether distributed or otherwise, or any attacks, such as buffer or stack overflows, that would knowingly result in severe performance degradation of a network or computing resource.
- Manipulate or delete any requesting agency data, including log files

- Engage with any non- requesting entity parties for the purposes of social engineering
- Modify device configurations in a manner to introduce vulnerabilities

Once persistence is achieved within the network, Phase Two consists of the CISA team conducting a series of activities, called Measurable Events, which are initiated and specifically intended to provoke a security response by the requesting entity's Security Operations Center (SOC) or network security monitors. Phase Two measures the effectiveness of the people, processes, and technologies defending a customer's network as determined by observable, response-driven metrics. For example, measurable events which should result in a security response may include but are not limited to:

1. Port Scanning & Host Enumeration
2. Data Exfiltration
3. Malicious Traffic Generation
4. Antivirus Detection & Response
5. Account (local admin, domain admin) Creation
6. Domain Admin Logon Event Activity
7. Ransomware Emulation

The CISA team will evaluate SOC personnel responsiveness to measurable events that the CISA team generates within the environment. The same measurable event may occur multiple times within numerous portions of the network, with varying degrees of complexity and at different time periods and intervals. The trusted and strategically-positioned requester representatives who are aware of an in-progress RTA will be informed of the nature and timing of any measurable events to ensure such events do not unreasonably distract SOC employees and prevent them from detecting or responding to any actual events that may be occurring within the network.

To perform this service, the CISA team may use one or more of a requester's unique seal, trademark, name, or insignia in phishing emails or other services, and requester hereby grants CISA the right to use such seal, trademark, name, or insignia. The requester is responsible for obtaining any internal authorizations necessary for CISA use of its seal, trademark, name, or insignia, consistent with applicable law and procedures.

The assessment closes out with two onsite briefings: one for senior leadership detailing the business impact of the assessment, and a second focused on a technical review detailing the tools, lateral moves, and indicators that Security Operations Center analysts could and/or should have identified during the course of the assessment. Approximately 6 weeks after CISA personnel conduct the close out briefings, the CISA Red Team will deliver an assessment report detailing the method of attack utilized in Phase One and the indicators of compromise and corresponding SOC response metrics collected used in the Phase Two Measurable Events phase.

Associated Activities

- Multi-platform phishing with payload deployment and exploitation
- Voice and Mobile (SMS) Phishing, deceptive pre-texting, and open source internet research for social engineering purposes
- Scanning or probing of public facing network and physical infrastructure

- Accessing network and physical infrastructure for vulnerability exploitation
- Establishing a presence within a network environment through account creation
- Coordinating measurable events with trusted representative and initiating events to determine and document SOC personnel responsiveness
- Emulation of other Advanced Persistent Threat (APT) Tactics, Techniques and Procedures (TTPs)

Deliverables

- Weekly summaries
- Executive Out-brief
- Technical Out-brief
- Assessment Report