TOOELE COUNTY CORPORATION
CONTRACT # 21-10-14

TOOELE COUNTY

Tooele County Council
Agenda Item Summary

Department Making Request:	**Meeting Date:**
I.T./Clerks Office	10/19

Item Title:

Cybersecurity Assessments Rules of Engagement with U.S. Dept. of Homeland Security

Summary:

The IT Department recently went through a security audit for the County Clerk's Office for the upcoming Election. During this time the Cybersecurity Advisor, Rick Gardner, advised me that he can do the same Risk Assessment, pen test, table top test, etc for Tooele County at no cost to the county. Rick Gardner works for U.S. Department of Homeland Security and this a service that is available on no cost to state and local government.

Denise sent out for signature.

CYBERSECURITY ASSESSMENTS

RULES OF ENGAGEMENT

Between the

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

And

Tooele County Council

April 23, 2020

Version – SLTT 4.03

Prepared By:

U.S. Department of Homeland Security

Cybersecurity and Infrastructure Security Agency

THIS PAGE INTENTIONALLY LEFT BLANK.

Table of Contents

1 Introduction

1.1 Purpose organization

This document establishes the Rules Of Engagement (ROE) for cybersecurity assessments requested by Tooele County Council (TCC) from the Cybersecurity and Infrastructure Security Agency (CISA).

1.2 Scope

This ROE applies to TCC and CISA for all services documented through the procedures described herein. In addition, it applies to all CISA personnel who may access data obtained or generated under this ROE. This ROE does not include services for any classified computer, system or network nor access to any classified information.

1.3 Background

CISA utilizes a defined strategy and methodology for testing, assessing and analyzing target systems with state-of-the-art tools and highly trained security experts to conduct Vulnerability and Threat Assessments. The purpose of these Assessments is to assist TCC in developing a strategy for improving cybersecurity posture and aligning it with enterprise architecture and mission objectives.

CISA conducts comprehensive assessments of federal and non-federal networks, including critical infrastructure networks, under authority of Title XXII of the Homeland Security Act (6 U.S.C. § 651 et seq., *see especially* section 2209 (6 U.S.C. § 659)) and the Federal Information Security Modernization Act (FISMA) (44 U.S.C. §§ 3551 et al.). CISA teams assess unclassified networks to evaluate the security posture when compared to best practices, regulations, policies and standards relating to cybersecurity. CISA team services include various cybersecurity assessment activities such as network mapping, vulnerability scanning, host based assessment, database and web application scanning, phishing, red teaming, and rogue wireless access point detection. The CISA teams include both federal government employees and contractor support personnel. All contractors serving on CISA teams have signed valid DHS 11000-6 Non Disclosure Agreements.

Insert Establishment Background (Optional)

2 Procedures and Authorizations Prior to Service

2.1 This ROE is effective when signed by the TCC CIO or equivalent authorized official and the CISA Assessments Branch Chief.

2.2 Pursuant to this ROE, TCC may request CISA team services by completing an Appendix A in advance, each time service is requested. The CISA team will only perform those services specifically selected by TCC in the Appendix A and will only access systems and/or IP addresses identified by TCC in the Appendix A, during the period of time agreed upon in that Appendix A. Each new

Appendix A will be sequentially marked, e.g., Appendix A-1, Appendix A-2, Appendix A-3. The Appendix A is complete and becomes part of this ROE when all relevant information has been provided, including the selection of the Site Monitor, and Appendix A is signed by both the Site Authority (either the Site Monitor or the relevant CIO/authorized official) and the CISA Team Lead. Prior to the start of CISA team services, the TCC Site Monitor shall provide signed copies of the complete Appendix A to the TCC CIO or equivalent authorized official and the CISA Team Lead shall provide the same to the CISA Assessments Branch Chief.

2.3 In the event that any site/IP address proposed to be in-scope of requested CISA team services is operated by a TCC sub-entity whose CIO or equivalent authorized official has unique or exclusive authority over that site/IP address, the sub-entity CIO or equivalent authorized official must complete and sign a separate Appendix A authorizing CISA to conduct requested services within that site/IP address range.

2.4 In the event that any site/IP address identified by TCC in an Appendix A is operated or maintained by a third party (e.g. contractor or cloud-service provider) on behalf of TCC, TCC will ensure that the third party provides authorization for testing by either filling out and signing the form at Appendix B or completing the third party's authorization process and providing proof of authorization to the CISA team. Appendix B is complete and becomes part of this ROE when signed by an authorized representative of the third party. Each new Appendix B will be labeled with the corresponding Appendix A number and a sequential alpha character. For example, an Appendix B for two third parties under TCC's fourth request for services would involve Appendix A-4 and Appendix B-4a and Appendix B-4b, respectively. Prior to the start of CISA team services, signed copies of each complete Appendix B will be provided by the Site Authority to the TCC CIO or equivalent authorized official and by the CISA Team Lead to the CISA Assessments Branch Chief.

2.5 Services provided by the CISA team are described in the Services Catalogue at Appendix C. The Services Catalogue may be updated at any time by notice to TCC. Correspondingly, the template for Appendix A may be updated by notice to TCC to reflect new or changed services offered by the CISA team in an updated Services Catalogue.

2.6 Some CISA services described in the Appendix C Services Catalogue may require use of one or more of TCC's unique seal, trademark, name, or insignia in phishing emails. TCC hereby grants CISA the right to use such seal, trademark, name, or insignia. TCC is responsible for obtaining any internal authorizations necessary for CISA use of its seal, trademark, name, or insignia, consistent with applicable law and procedures.

2.7 Some CISA services described in the Appendix C Services Catalogue will involve scanning or other network traffic originating from IP addresses or similar identifiers belonging to CISA or entities that CISA has contracted with, including cloud service providers. Such IP addresses or similar identifiers will be made known to the Site Monitor, when appropriate. CISA will also notify the Site Monitor should the IP addresses or other identifiers change.

2.8 TCC certifies that its log-on consent banners or notices; terms-of-use policies or user agreements; computer training programs; and any other mechanisms used to notify users and obtain their consent to the terms and conditions of computer use clearly demonstrate to TCC computer users and obtain their consent that:

"Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from this network/system. Any communications or data transiting, stored on or traveling to or from this network/system will be monitored and may be disclosed to third parties, including other governmental entities, or used for any lawful government purpose."

3 **Site Preparation**

The TCC Site Monitor identified in Appendix A is an TCC authorized representative responsible for preparing the site, serving as TCC 's primary point of contact for the CISA team, and monitoring CISA team services at that site for the agreed upon time and services identified in the Appendix A. Prior to the start of any CISA team services:

3.1 The Site Monitor and the CISA Team Lead will review the Appendix A and ensure that either an additional Appendix A and/or a completed Appendix B have been provided, if applicable, for all sub-entities or third parties.

3.2 The Site Monitor will coordinate and ensure, as appropriate, the involvement of TCC officials and adherence to TCC policies and standard operating procedures that could have an impact on the scanning activities and the information systems being assessed.

3.3 The Site Monitor will identify to the CISA team potentially sensitive TCC devices prior to testing.

3.4 The Site Monitor is responsible for ensuring system backups have been performed and restore processes are validated prior to the start of external or internal CISA team services.

3.5 The Site Monitor will provide the CISA team with information about the internal IT environment.

3.6 Certain CISA team services may require administrator or other specific user access to the networks or systems being tested. The Site Monitor is responsible for ensuring access for the CISA team. If administrator provisions are required, access will be granted by either (1)Either TCC or CISA establishing a separate administrative account for testing (e.g., "CISATeam"), or (2) through the use,

under TCC supervision and control, of an existing administrator account. It is recommended that separate testing accounts will be established prior to the arrival of the CISA team.

3.7 The Site Monitor, on behalf of TCC and in coordination with other TCC officials as appropriate, will use best efforts to identify to CISA in advance any categories of data, which may be encountered by CISA during the selected services, that are sensitive in nature or protected from disclosure by statute, regulation, or other authority, including personally identifiable information, and will provide CISA instructions on how to identify and handle such data if encountered by the CISA team. The Site Monitor and CISA Team Lead will work together to structure the engagement to ensure that the CISA team does not come into contact with such data to the maximum extent possible or that appropriate data handling requirements have been put into place. The Site Monitor and CISA Team Lead will also discuss in advance what initial actions should be taken in the event that unforeseen sensitive data is encountered during CISA team services.

3.8 For assessments conducted onsite at the TCC facility, the Site Monitor may request and is permitted to authorize TCC IT staff or security personnel to scan the CISA team assessment equipment for vulnerabilities prior to network connection using agreed upon vulnerability scanning tools. However, assessment equipment contains code and technical references, which are not to be viewed, distributed or evaluated by external organizations. Under no circumstances will the CISA team's Government Funded Equipment (GFE) be relinquished from the control of the CISA team.

3.9 The Site Monitor may request that the CISA team conduct scanning activities on-site or remotely through a virtual private network.

3.10 For assessments conducted on-site at the TCC facility, the Site Monitor will ensure that office or conference room-type workspace with AC power and a minimum four internal network jacks/drops with a live connection at the identified facility is available and provided to the CISA team. Personnel from TCC IT staff or security personnel are encouraged to observe the CISA team on-site.

3.11 For assessments conducted remotely, TCC is responsible for providing a virtual private network connection. The Site Monitor will provide any information and support necessary for the CISA team to connect remotely.

3.12 In order to prepare for and conduct certain assessments, the CISA team may passively compile data from publicly-available and commercially-available resources, including information regarding TCC 's employees, network (e.g., registered network ranges and applications), and organization.

This information, to the degree that it is not incorporated into the final report, will be deleted upon completion of the selected assessment(s).

4 Assessment

During the assessment:

4.1 The CISA team will use GFE, Government Off-The-Shelf (GOTS), Commercial Off-The-Shelf (COTS) and open-sourced software and hardware. Use of any particular software or hardware by the CISA team is not a government endorsement or sponsorship of any product, service or company. A brief description of any software or hardware used by the CISA team can be furnished in advance upon request.

4.2 The CISA team will conduct any external assessment selected in Appendix A during the dates specified in Appendix A.

4.3 The CISA team will conduct any internal assessment selected in Appendix A by connecting GFE to TCC 's network, either on-site or through a virtual private network provided by TCC as determined by the Site Monitor, during the dates selected in Appendix A.

4.4 The CISA team will collect and analyze data from TCC systems, networks, and processes to assess capability gaps in order to identify a road map for an enterprise-level risk based mitigation strategy.

4.5 For on-site assessments, the CISA team will provide to the Site Monitor a brief overview of daily activities and an outbrief at the conclusion of the assessment.

4.6 The CISA Team Lead will notify the TCC Site Monitor if a perceived significant event occurs during the assessment. The Site Monitor is responsible for having appropriate knowledge and understanding of the TCC networks and systems, identification and/or confirmation of a significant event, and taking appropriate action, which may include suspension and/or termination of the assessment. In the event a significant event occurs that warrants termination of the assessment, the CISA Team Lead and the Site Monitor will promptly provide to the TCC CIO or equivalent authorized official, the TCC Site Authority, and the CISA Assessments Branch Chief a written account of the conditions and actions that led to the termination of the assessment. If the CISA Team Lead and Site Monitor cannot agree on the account, both accounts will be provided.

4.7 In the event a disagreement arises between TCC and the CISA team during the assessment, best efforts will be made to resolve such a disagreement at the lowest level possible.

5 Data Protection

5.1 Consistent with 5 U.S.C. § 552(b), CISA will not disclose under the Freedom of Information Act ("FOIA") any information provided by TCC under this request that is exempt from disclosure, including: Exemption (b)(3) as matters specifically exempt from disclosure by statute, Exemption (b)(4) as trade secrets and commercial or financial information that is privileged or confidential, and Exemption (b)(7)(A)-(F) as records or information compiled for law enforcement purposes.

5.2 Without limiting the previous sentence, TCC understands that this obligation will apply to any written CISA notes of observations of TCC facilities and equipment (including computer screens), that CISA will make determinations regarding FOIA requests on a case by case basis consistent with its obligations under FOIA, CISA FOIA regulations, and its own internal guidance, and that any determinations regarding specific FOIA exemptions will be made at the time that the responsive records are processed. CISA shall provide TCC an opportunity to object to disclosure as provided by applicable law.

5.3 TCC understands that information provided by TCC that meets the definition of cyber threat indicator or defensive measure as defined in the Cybersecurity Information Sharing Act of 2015 (the "2015 Act"), 6 U.S.C. § 1501-1510, and that is provided in accordance with the 2015 Act's requirements, will be protected as provided by the 2015 Act (including protection from release under FOIA). See the Non-Federal Entity Sharing Guidance under the Cybersecurity Information Sharing Act of 2015 published by the Department of Homeland Security and the Department of Justice, available at https://www.us-cert.gov/ais.

5.4 Further, the 2015 Act may offer disclosure protection for the final report when in TCC 's possession, as the 2015 Act provides a basis in federal law for state, local, and territorial (SLT) governments to exempt vulnerability information received from CISA from disclosure under any STL freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records. *See* 6 U.S.C. 1503(d)(4)(B). This exemption applies to a "cyber threat indicator or defensive measure;" the 2015 Act explicitly defines "cyber threat indicator" to include "a security vulnerability" (See 6 U.S.C. § 1501(6)(C)) and defines "defensive measure" to include any action, procedure, technique, or other measure to prevent or mitigate a known or suspected cybersecurity threat. *See* 6 U.S.C. § 1501(7)). STL governmental entities, rather than CISA, are responsible for asserting this basis for withholding in response to any such requests under their own STL disclosure laws.

5.5 Collected data and assessment results may be anonymized and used to support government-wide trending analysis. Any data or assessment results used in trending status reports will be non-attributable to TCC.

5.6 CISA will not share TCC's specific data and final report except as may be required by law.

6 **Post-Assessment**

6.1 The CISA team will provide TCC with a final report within 30 days. The final report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in the final report or otherwise. Further dissemination of the final report may be governed by a Traffic Light Protocol (TLP) marking in the header, if present. For more information about TLP, see http://www.us-cert.gov/tlp/.

6.2 TCC understands that it is under no obligation to implement any changes to its information systems that CISA may recommend.

7 **Dispute Resolution**

Disputes will be resolved at the lowest level possible.

8 **Amendment**

Unless otherwise specified, this ROE may be amended by the mutual written agreement of the TCC CIO or equivalent authorized official and the CISA Assessments Branch Chief at any time.

9 **Termination**

This ROE may be terminated either bilaterally by the mutual written agreement of the TCC CIO or equivalent authorized official and the CISA Assessments Branch Chief at any time or unilaterally with thirty (30) days written notice.

10 **Approval**

By signing below, the approving TCC official certifies the following:

- TCC authorizes the CISA team to provide services on TCC networks and systems in each Appendix A;
- TCC agrees to obtain and provide to CISA a written authorization using the form at Appendix B from every third party that operates or maintains TCC networks/systems listed in each Appendix A;
- TCC agrees to ensure that TCC network users have received notice and consent in accordance with this ROE;
- TCC accepts that, while the CISA team will use its best efforts to conduct its activities in a way that minimizes risk to TCC systems and networks, all of the tests described above,

and especially penetration testing or a red team assessment (if selected) create some risk to TCC systems and networks;

- TCC accepts the risks to TCC systems and networks that may occur as a result of activities described in this ROE;
- TCC acknowledges that CISA provides no warranties of any kind relating to any aspect of the assistance provided under this ROE;
- TCC accepts the risk of any damage that may result from implementing any guidance provided by DHS; and
- TCC has authorized you to make the above certifications on its behalf.

James A Welch Digitally signed by James A Welch Date: 2021.10.07 16:39:27 -06'00' 10/7/21
(Signature, Chief Information Officer or Equivalent) (Date)

James A Welch, County Manager awelch@tooeleco.org / 435.843.3150
(Print Name and Title) (Email and Telephone Number)

CISA Assessments Branch Chief (Date)

APPROVED AS TO FORM:

Colin Winchester 10/15/2021
Colin R. Winchester
Deputy Tooele County Attorney

For CISA Use Only – ROE S/N:

Cybersecurity and Infrastructure Security Agency

Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

CISA Services Catalog Version 5

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
April 23, 2020	4.04	Removed assessments terminology from "CISA Assessments" to "CISA"	J. Giguere
May 21, 2020	5	Removed /War Dialing	K. Sullivan
May 26, 2020	5	Added RPT Assessment	J. Giguere

1) Risk and Vulnerability Assessment (RVA)

A CISA 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.

Associated Activities

- 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 inachieved 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

2) Phishing Campaign Assessment (PCA)

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 is 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 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 accessthe 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 logfiles
- Engage with any non- requesting entity parties for the purposes of socialengineering
- 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

5) Remote Penetration Test (RPT)

Remote Penetration Test (RPT) This service utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways. RPTs are similar to risk and vulnerability assessments but focus only on externally accessible systems with a tradeoff made for more service capacity at the expense of assessment scope. As a remote service, it is less costly and more scalable than on-site offerings; however, it is more limited in organizational insight and context.

Scenarios:

- External Penetration Test: Verifying if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.
- External Web Application Test: Evaluating web applications for potential exploitable vulnerabilities; the test can include automated scanning, manual testing, or a combination of both methods.
- Phishing Assessment: Testing through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.
- Open Source Intelligence Gathering: Identify publicly available information about the stakeholder environment which may be useful in preparing for an attack.