SAFETAG

A Security Auditing Framework and
Evaluation Template for Advocacy Groups

Audit Guide Overview

Internews
Local voices. Global change.

Contents

License

Attribution for content from other Licenses

Introduction

The Security Auditing Framework and Evaluation Template for Advocacy Groups (SAFETAG) is a professional audit framework that adapts traditional penetration testing and risk assessment methodologies to be relevant to small, non-profit, human rights organizations based or operating in the developing world.

SAFETAG is based upon a set of principles, activities, and best practices to allow digital security auditors to best support at-risk organizations by working with them to identify the risks they face, the next steps they need to take to address them, and guidance on how to seek out support in the future.

SAFETAG audits are targeted at serving small scale civil society organizations or independent media houses who have strong digital security concerns but do not have the funds to afford a traditional digital security audit. The traditional security-audit framework is based upon the assumption that an organization has the time, money, and capacity to aim for as close to perfect security as possible. Low-income at-risk groups have none of these luxuries. These audits are both far too expensive, and produce output that is too complex for these organizations to act upon.

info@safetag.org | https://safetag.org

Disclaimers

- **SAFETAG should not be attempted without the proper expertise.** The SAFETAG process requires both technical and facilitation expertise. As such, while the process is built to allow a single auditor, the process can easily be split between a facilitator/trainer and a technical auditor. In fact, if an auditor does not have both the required technical expertise and experience facilitating structured activities with at-risk groups, we **highly recommend** working with a specialist who can fill the missing role. *Inexperienced or untrained auditors can possibly hinder the mission of the host organization or put them at risk.*"
- **SAFETAG does not provide in depth training to a host organization.** SAFETAG audits often include short, targeted support on specific issues, but these are not substitutes for in-depth training of personnel. The audit does not itself resolve any of the issues uncovered - it's purpose is to find vulnerabilities relevant to the organizations needs in the short time on-location, and equip the organization to understand and respond to these in a rapid, resilient, effective, and cost-efficient manner. Because of this a large part of the SAFETAG post-audit practice is focused on helping an organization understand how they can identify the training and technical support that they may need to respond to their digital security needs.
- **SAFETAG audits are not a replacement for the implementation of security controls, or maintenance of system security.** SAFETAG is focused on helping small at-risk organizations prioritize and develop a digital security process from the ground up that respects their constraints of limited time, funding, and emotional energy. SAFETAG hopes to guide an organization to begin a ongoing digital security process, not replace it.
- **SAFETAG audits do not provide an exhaustive and verifiable outputs that a professional industry standard security-audit would provide.** Many low-income vulnerable groups have neither the money, time, or manpower to respond to a full security audit. SAFETAG uses a customized combination of selected assessment techniques derived from standards in the security auditing world to provide an organization driven risk assessment and mitigation consultation that aims to help this type of organization identify practices and resources that will allow them to strategically move towards greater security.

The SAFETAG Process

SAFETAG, as shown in Figure 1 on the next page, uses a customized combination of selected assessment techniques derived from standards in the security auditing world and best-practices for working with small scale at-risk organizations to provide organization driven risk assessment and mitigation consultation.

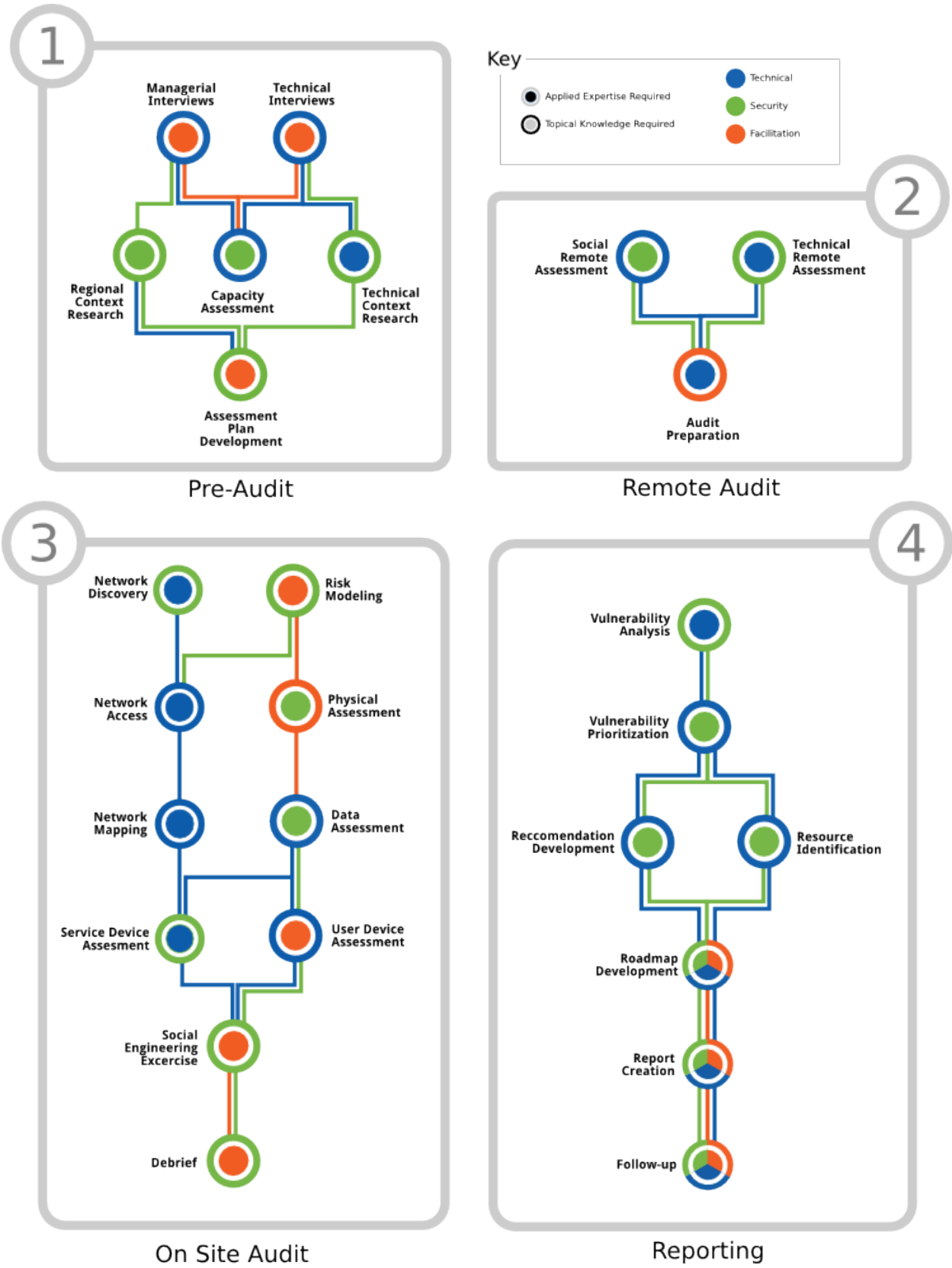

Figure 1: The Safetag Audit Process

PART ONE: Agreement and Information Gathering

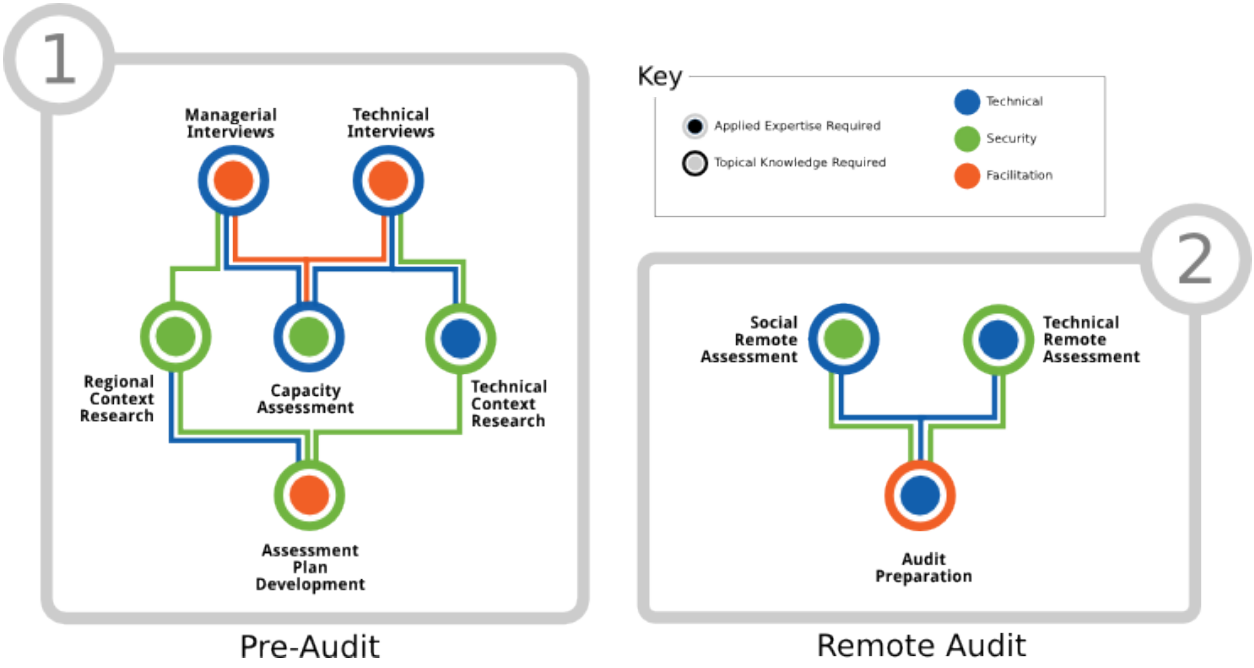

Figure 2: The Pre-Audit Process

Operational Security

"*Also be aware that local groups may not be able to accurately gauge the safety of their communications with you. Sometimes they underestimate the likelihood of risk - at other times, they can wildly overestimate the risk. Either way, trainers need to navigate this issues carefully and respectfully with a "do no harm" approach that respects the reported needs, context, and experiences of your local contact and potential trainees.*

Some easy tools that may reduce (but not guarantee) the safety of communications with a local contact (assuming that their device has not been compromised) is chat with OTR or Cryptocat, as these are two of the easier communication tools to set up and use without advanced technical skills. (Secure encrypted VoIP using Ostel is a strong alternative that is easy enough for most users to set up and use as well, although it requires more steps than the previous recommendations.) In any case, it's important to always provide an "opt-out" of handing over sensitive information." - *Needs Assessment: Level-Up* [1]

Summary

Below are the baseline operational security guidelines for a SAFETAG audit. In the mini and full guides activity specific operational security guidelines are contained within each section.

Purpose

An audit uncovers an array of sensitive information about an organization. For some at-risk populations the mere act of getting a digital security audit can increase their likelihood of being actively attacked by an adversary. The foundation of the SAFETAG process is the goal of increasing the safety of the host organization, its staff, and the auditor. It is vital that an auditor weigh the possible risk and audit may incur on the organization or the auditor against the possible outcomes of an audit.

General Guidelines

- Data storage security
  - Keep ALL data related to the audit secured per the Pentest Standards for data security, from interview and research notes through audit findings and reporting outputs. Additional notes per section.
- Communications security
  - Conduct all communication with the client over at least minimally secure channels where the communication is encrypted in transit at all times per the Pentest Standards for data security.
  - Higher levels of security (such as PGP, truecrypt, or minilock) should be used for all file and document transfers.

[1] Event Planning Inputs - Level-Up

Interviews

"*Keep in mind that the most sensitive and efficient way to interview a participant is through an 'in-person' conversation (that is, face-to-face or by telephone). If this is not possible, e-mail is an alternative. However, ensure that this is a secure e-mail conversation. It may be best for facilitators and participants to open separate secure e-mail accounts for this purpose – 'hushmail' is just one example, but note that e-mail security levels can change over time and in different geographic locations, so it is best to check with communication security experts to identify the most secure option. Bear in mind, too, that participants may find the questions more difficult to answer by e-mail.*" - *Integrated Security: The Manual* [2]

Summary

The auditor conducts interviews with a management staff member (usually their primary point of contact), and the lead technical staff member when available.

The management interview explores what issue areas the organization works on, how they currently use technology, the importance of digital media for the organization's work, and their practices for building skill/capacity among their staff.

In the technical interview, the auditor explores what technology the organization already uses (both officially and as "shadow infrastructure" such as Dropbox), their history with digital security, and any historical obstacles with adoption or use of new technology.

In both interviews, the auditor should explore how the organization perceives their current threat landscape - who are they worried about (adversarial groups opposed to their mission/community, their domestic government, foreign governments...), and what risks they perceive as active and credible - especially around any issues that have happened to their staff or partners in the past.

Purpose

The purpose of the interviews is to give the auditor a starting place for understanding the organizations use of technology, capacity to engage with digital security, and current threat landscape.

Approach

- Interview managerial staff
- Interview technical staff

Output

- Organizations' readiness, past strategies, and likelihood to succeed in engaging in technological adoption/change.
- The availability and quality of communications and electronic infrastructure.
- Threats posed to the digital and physical security of the organization and its staff, including arrests, harassment and violence.
- Threats posed to the digital and physical security of the organization and its staff by digital attacks as well as digital surveillance and communication.
- Any past security issues encountered by the organization and its partners.
- Priority security concerns.

[2] Integrated security: The Manual

- Technological hardware and software in use for protecting the physical and digital security of organizations and their staff.
- Past, current, or desired use of websites, blogs, social media and other web-based tools and platforms to conduct outreach, manage information, advocate or engage with specific groups.
- Past, current, or desired use of mobile telephony and related software and hardware for activities such as sms management and data collection.

Capacity Assessment

"*In human rights organisations where the HRDs are at risk, an organisational security plan will help to protect the workers and allow them to do their work more effectively. If your organisation acknowledges and plans for dealing with the risks, the staff and/or members will feel more supported and have increased allegiance to the organisation and its important work.*" - *Workbook on Security: Practical Steps for Human Rights Defenders at Risk* [3]

Summary

In this component the auditor reviews the interviews to identify the organization's strengths and weakness (expertise, finance, willingness to learn, staff time, etc.) to adopting new digital and physical security practices. The auditor uses this information to modify the audit scope, and recommendations accordingly.

Purpose

Knowing an organization's strengths and weaknesses will allow the auditor to provide more tailored recommendations that an organization will be more likely to attempt and achieve. The auditor will use this assessment in preparing for the audit itself as well as when evaluating the difficulty of a recommendation.

Approach

- Identify organizational areas of strength and weakness (expertise, finance, willingness to learn, staff time, etc.) when engaging in technological adoption/change.
- Identify organizational barriers to adoption. [^info_tech_adoption]
- If technical needs arise, modify the audit scope and plan the trip preparation accordingly.

Output

- Organization's ability to:
  - Adopt new technology
  - Learn from others
- Organization's resources available for technological adoption:
  - Financial resources
  - Staff time
  - Staff buy-in
  - Technical expertise
  - Technical buy-in
- Modifications to audit preparation and equipment

[3] Workbook on Security: Practical Steps for Human Rights Defenders at Risk

Context Research

"*The assessment should be relevant to the situation of the NGO locally and should therefore avoid diversions on factors which have no implications for NGO safety and security. This step is the part of the process that supports and allows the identification of general and specific threats to the NGO operation. All data collected must be relevant to safety and security of the activities which the NGO is conducting, supported as much as possible by facts and relevant deductions, and up to date.*" - *Security Risk Management: NGO Approach* [4]

Summary

This component allows the auditor to identify the relevant regional and technological context needed to provide a safe and informed SAFETAG audit. This component consists of desk research that is collected and analyzed by the auditor, as well as inputs from the Interview component.

Purpose

Analysis of context is the foundation of effective risk management. Both at-risk organizations and auditors will develop assumptions based upon their experience. It is important that an audit is based on information that is current and accurate.

Checking the assumptions both of the organization and of the auditor by researching the current regional and technological context will ensure that an auditor is basing their work on accurate assessments of the conditions the organization faces and that they are making informed operational security considerations.

Approach

- Regional Context Research
  - Identify additional adversaries not identified in interviews including: government authorities, non-state actors (organized crime. corporations, etc), and police or security forces.
  - Identify capacity and willingness of potential adversaries to act against the organization.
  - Identify any legal risks associated with conducting the audit (Secure communications and storage, network forensics, device exploitation, digital security training.) [5]
- Technical Context Research
  - Identify access to communications infrastructure.
  - Explore latest cyber security trends.
  - Explore security landscape of hardware and software identified in interviews. [6]

Output

- A summary of the most likely threats that the host and auditor may face:
  - Possible adversaries and their capacity and willingness to act against the host,
  - Latest general cyber-security threats,
  - Legal risks to host and auditor conducting a SAFETAG audit.
- Modifications to the audit plan as necessary.

[4] Security Risk Management: NGO Approach - InterAction Security Unit

[5] " Some activities common in penetration tests may violate local laws. For this reason, it is advised to check the legality of common pentest tasks in the location where the work is to be performed."

[6] "Assessors need to remain abreast of new technology and the latest means by which an adversary may attack that technology. They should periodically refresh their knowledge base, reassess their methodology-updating techniques as appropriate, and update their tool kits."

Assessment Plan

"*The assessment plan should answer these basic questions:*

1. *What is the scope of the assessment?*
2. *Who is authorized to conduct the assessment?*
3. *What are the assessment's logistics?*
4. *How should sensitive data be handled?*
5. *What should occur in the event of an incident?*" - *NIST SP 800-115, Technical Guide to Information Security Testing and Assessment* [7]

Summary

This component allows an auditor and host to come to an understanding of the rules and boundaries of the assessment as well as the processes that will be adhered to in case of an incident. This component consists of a process where the auditor collaboratively creates an assessment plan with key members of the organization.

Purpose

A core tenet of SAFETAG is building agency in organizations to improve their digital security. To that end, collaboratively creating an assessment plan with the organization helps to clarify not only the audit scope - from discussing what sensitive data may be exposed to what systems may be disrupted in the process of the audit - but it also helps reveal the ability of the organization to support and respond to the audit findings.

Approach

- Determine a point person for the audit and exchange contact information. [8]
- Explain and get approval to the scope of audit from the host. [9,10]
- Host provides auditor consent to conduct the agreed to scope of the audit in the form of a signed liability waiver. [11]
- Agree to the time-line, location, and attendees of the on-site audit. [12]
- Create procedure for incident handling in the event that auditor cause or uncover an incident during the course of the assessment. [13,14]
- Codify data security standards for audit communication and evidence handling. [15]
- If funded externally, identify what should be reported to external funder. [16]

[7] NIST SP 800-115, Technical Guide to Information Security Testing and Assessment

[8] "Obviously, being able to get in touch with the customer or target organization in an emergency is vital."

[9] " Some activities common in penetration tests may violate local laws. For this reason, it is advised to check the legality of common pentest tasks in the location where the work is to be performed."

[10] "In addition, some service providers require advance notice and/or separate permission prior to testing their systems. For example, Amazon has an online request form that must be completed, and the request must be approved before scanning any hosts on their cloud. If this is required, it should be part of the document."

[11] The auditor consent template can be found in the SAFETAG "full guide."

[12] Determining Audit Location - The Penetration Testing Execution Standard: Pre-Engagement Guidelines

[13] NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. Section 7.1 Coordination

[14] Emergency Contact and Incidents - The Penetration Testing Execution Standard: Pre-Engagement Guidelines

[15] "When handling evidence of a test and the differing stages of the report it is incredibly important to take extreme care with the data. Always use encryption and sanitize your test machine between tests."

[16] Usually when working with an external funder an engagement report, free of sensitive data about the host organization, will be created for submission the funder. The contents of this report should be clearly outlined and agreed to during the assessment plan stage.

Output

- An agreement signed by both parties outlining the scope of the audit including:
  - The start and end dates of the audit.
  - The location where the on-site audit will take place. [17]
  - The responsibilities of the host staff.
  - The responsibilities of the auditor.
  - The host names and IP ranges of any services run by the organization. [18]
  - Emergency contact information for the organization. [19]
  - The procedure the auditor will follow when handling incidents. [20]
  - The data security standards for evidence handling and communication. [21]
- A liability waiver signed by the host organization. [22]
- Approval from any third parties. [23]

[17] Determining Audit Location - The Penetration Testing Execution Standard: Pre-Engagement Guidelines
[18] "Before starting a penetration test, all targets must be identified."
[19] "Obviously, being able to get in touch with the customer or target organization in an emergency is vital."
[20] "the assessment plan should provide specific guidance on incident handling in the event that assessors cause or uncover an incident during the course of the assessment. This section of the plan should define the term incident and provide guidelines for determining whether or not an incident has occurred. The plan should identify specific primary and alternate points of contact for the assessors... The assessment plan should provide clear-cut instructions on what actions assessors should take in these situations."
[21] "When handling evidence of a test and the differing stages of the report it is incredibly important to take extreme care with the data. Always use encryption and sanitize your test machine between tests."
[22] "One of the most important documents which need to be obtained for a penetration test is the Permission to Test document."
[23] Dealing with third parties - The Penetration Testing Execution Standard

PART TWO: The Audit

Figure 3: The On-Site Audit Process

Remote Assessment

"*Good social engineering thus requires some knowledge of a target's contacts, areas of interest, and current priorities or activities. It is likely that attackers conduct some form of preliminary reconnaissance or otherwise "study up" on their targets to develop their social engineering, perhaps drawing on social media and other open source information, or leveraging information or credentials gleaned from existing access to the systems of others within the target's circle of trust (what might be called "collateral compromise"). Thus attackers appear to invest primarily in knowing their targets, rather than creating or purchasing advanced malware.*" *Communities @ Risk: Targeted Digital Threats Against Civil Society* [24]

Summary

This component allows the auditor to identify publicly available resources (such as websites, extranets, email servers, but also social media information) connected to the organization and remotely gather information about those resources.

The remote assessment methodology focuses on direct observation of an organization and their infrastructure, consisting of passive reconnaissance of publicly available data sources ("Open Source Intelligence") and active footprinting of the organization's networks and systems. This information is used to inform many of the following sections and can be done remotely.

Purpose

While much of SAFETAG focuses on digital security challenges within and around the office, remote attacks on the organization's website, extranets, and unintended information available from "open sources" all pose real threats and deserve significant attention. SAFETAG takes great care to take a very passive approach to this work, especially when done off-site, so as not to have unintended consequences on the organization's infrastructure or undermine operational security concerns.

This remote work also feeds in to the Auditor's understanding of the organization's digital presence (and their own understanding thereof), and will guide specific vulnerabilities to investigate once on site.

Approach

- Passive Reconnaisance
  - Identify availability of staff, partner, beneficiary, and current project information online. [25]
  - Search "paste-bin" sites for leaked internal information or existing exploitation of their infrastructure.
  - Create API keys for Recon-ng services to be used. [26]
  - Use recon-ng to do automated web-based open source reconnaissance. [27]
- Active Footprinting
  - Identify services being hosted or used by an organization
  - Tesearch information about identified services (e.g current versions of those services.)
  - Run vulnerability scans against websites hosted by the organization.
  - Run vulnerability scans against servers run by the organization.

[24] Communities @ Risk: Targeted Digital Threats Against Civil Society - Executive Summary
[25] Accumulating information about partners, clients, and competitors - The Penetration Testing Execution Standard
[26] Acquiring API Keys
[27] The flow of information through the Recon-ng framework. (See: "Data Flow" section)

Output

- Dossier of organizational, partner, and beneficiary “open sources” information exposed online.
  - A list of e-mail address for members of the organization.
- Identification and mapping of externally facing services and unintentionally exposed internal services.
  - Possible vulnerabilities in the websites and externally facing servers of the organization.
  - Existing information about earlier breaches identified in the paste-bin search.
- Follow the proper incident response plan if high risk problems are identified.

Preparation

Summary

This component consists of trip preparation activities that are needed to ensure the technical and facilitated components of the audit are able to be conducted effectively and within the on-site time-frame.

Purpose

A SAFETAG audit has a short time frame. Preparation is vital to ensure that time on the ground is not wasted updating systems, searching for missing hardware, or building resources needed for on the ground activities.

Approach

- Get any Visas or paperwork (letter of invitation?) needed, as well as travel tickets and hotel reservations. Note that some visas can take significant effort and may require the auditor to be without a passport while they are being processed.
- Create social engineering e-mails to reflect local context. [28]
- Generate a custom password dictionary for the host organization, using research from the Remote Assessment section, and optionally CeWL. [29]
- Pack a kit with power supply adapters, cables and relevant adapters, usb drives, external wireless cards and any other equipment needed for testing. [30,31]
- Prepare systems needed for testing:
- Updating anti-virus to latest version.
- Updating OS and tools to latest version. [32]
- Prepare storage devices and systems to reflect the required operational security.

Output

- Any Visas or paperwork needed, plus travel arragements (tickets, hotels) for auditor travel.
- Social engineering e-mails. [33]
- A custom password dictionary. [34]
- A travel kit. [35,36]
- Systems updated and ready for testing.

[28] Auditor Tool Resource List - Social Engineering
[29] Auditor Tool Resource List - Password Dictionary Creation
[30] The auditor travel kit checklist can be found in the SAFETAG "full guide."
[31] "Traveling teams should maintain a flyaway kit that includes systems, images, additional tools, cables, projectors, and other equipment that a team may need when performing testing at other locations."
[32] See the auditor trainee resource list
[33] Auditor Tool Resource List - Social Engineering
[34] Auditor Tool Resource List - Password Dictionary Creation
[35] The auditor travel kit checklist can be found in the SAFETAG "full guide."
[36] "Traveling teams should maintain a flyaway kit that includes systems, images, additional tools, cables, projectors, and other equipment that a team may need when performing testing at other locations."

Risk Modeling

"*Many structured approaches to threat modeling actively inhibit flow in both beginners and experts, and a few allow it to emerge. The documented and common elements of flow include the following:*

1. *The activity is intrinsically regarding*
2. *People become absorbed in the activity*
3. *A loss of the feeling of self-consciousness*
4. *Distorted sense of time*
5. *A sense of personal control over the situation or activity*
6. *Clear goals*
7. *Concentration and focusing*
8. *Direct and immediate feedback*
9. *Balance between ability level and challenge...*

Flow is the most important test of an approach, methodology, or even task for threat modeling. Knowing who will find flow in an approach is a key to architecting for success. If your audience can't find flow, their ability to find threats will be dramatically inhibited. Without flow, threat modeling is a chore..." - *Threat Modeling: Designing for Security* [37]

Summary

This component allows an auditor to lead the host organization's staff in a series of activities to identify and prioritize the processes that are critical for the organization to carry out its work. These activities will also reveal the consequences if those critical processes were interrupted or exposed to a malicious actor. This results in the staff creating a risk matrix which is used as the foundation of the auditor's recommendations.

Purpose

Having the host organization central to the risk assessment process allows the auditor to put their threats and recommendations into the host's own narrative. With greater ownership of the process the staff will be more engaged in addressing the threats identified when the audit is complete. [38] By engaging as many staff as possible the auditor also is providing a framework for staff to examine future concerns when the auditor is gone. The existing in/formal security practices captured during this process will be used to remove organizational and psyco-social barriers to starting new practices.

Approach

Carry out activities that allow you to do the following:

- Identify and map critical organizational *processes*.
- Identify *threats* to those processes.
- Identify the *impact* to the organization if those threats occur.
  - Rank the severity of the impacts identified.

[37] See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 408.

[38] "CSOs should gradually build a culture in which all staff, regardless of technical background, feel some responsibility for their own digital hygiene. While staff need not become technical experts, CSOs should attempt to raise the awareness of every staff member, from executive directors to interns - groups are only as strong as their weakest link—so that they can spot issues, reduce vulnerabilities, know where to go for further help, and educate others."

- Identify *adversaries* (people or groups) who may attempt to carry out threats and their capabilities.

Note that the order which you identify each component will vary depending upon what the host participants want to focus on first.

Throughout the activities:

- Identify existing in/formal security practices that the participants use to address risks.

After the activities are complete the auditor has tasks that build upon the outputs of the activities. These can be completed offsite.

- Create a risk matrix placing *impacts* against a range of likelihood.
- Clean up critical process maps for use in reporting.
- Create a list of all services or assets that were identified during the activity that were not already known by the auditor.

Output

- A host driven risk-matrix.
- Maps of critical processes.
- A list of organizational assets.

Network Discovery

"*Testing must specifically target only [wireless emissions] from personnel who are under direct legal contract with the scope owner, computer systems on the property of the scope owner, and EM or MW signals or emanations of power level great enough to disrupt or harm wireless communications within the scope. Analysts must make efforts to not invade upon a person's private life such as listening to or recording personal communications originating within the scope, where that private life has made efforts to separate itself from the scope.*" - *Open Source Security Testing Methodology Manual (OSSTMM)* [39]

Summary

This component allows the auditor to show the "visibility" of an organization's wireless network and identify devices using that network. This component consists of wireless scanning, device identification, and wireless signal mapping.

Purpose

The value of the network discovery component depends on the risk assessment of the organization. In many cases, an organization may not want the name of their wireless network to be associated with to their organization. Device beacons are also of interest, as they can reveal organizational links, as well as travel, favorite hotspots, and more. Beacons can "de-anonymize" an obfuscated network name as well as provide rich content for social engineering attacks. This provides an only-lightly-invasive introduction to discuss the trackability of devices, particularly mobiles and laptops.

Approach

- Scan for wireless networks near the organization.
- Determine/guess the office network(s).
- Confirm identified wireless network is the office network.
- Identify range of wireless network outside of office space.
- Monitor traffic of that network and capture wireless handshakes, beacons, and MAC addresses.

Output

- The name of wireless access points used by the host.
- airodump logs with key handshakes for wireless traffic on each relevant access point.
- A map or photos indicating the range of each relevant wireless access point.

[39] Open Source Security Testing Methodology Manual (OSSTMM) p. 140.

Network Access

"*Most people demonstrate a cognitive response to digital threat, but there is very little emotional reaction. We know that these things are dangerous, but we don't feel threatened. Security trainers need to help people feel the danger, not merely think about it...*

So the question remains, how do we evoke the healthy emotional responses that motivate adult human beings to protect themselves against dangers that they were not warned about as children? Merely describing the threat in an abstract way is unlikely to be effective. Rather, we need to emphasize the human impact of the threat and its relevance to the individual. This is most easily accomplished by telling stories!" - *The Psychological Underpinnings of Security Training* [40]

Summary

This component allows the auditor to test the strength of defenses the host has in place to protect their local area network. This component consists of gaining access to the local area network through a wireless access point and unsecured physical channels (such as an ethernet jack).

Purpose

This section is one of the few sections where the SAFETAG audit does go through attack scenarios, from attempting to "break in" to the wireless network to testing exposed ethernet jacks for connectivity. The reasons for this are threefold. First, access to an organization's internal network tends to reveal sensitive data and "shadow" infrastructures (such as dropbox usage) that lead to many recommendations to improve access control and discussions of the value of defense in depth. Second, the specific act of breaking the wifi password allows for a discussion on password security without attacking any specific user's password. Finally, with wireless networks treated as equivalent to wired networks in many offices, reminding the organization that wireless networks extend beyond the physical walls of the office is useful in discussing password rotation and guest network policies.

Approach

- Determine the security of the wireless access point (WAP).
- Gain client access to the WAP.
- Gain administrative access to the WAP.
- Test unused ethernet ports for live network connectivity.

Output

- Wireless access point (WAP) client password/key.
- Wireless access point (WAP) administrator password/key.
- Administrator access to the WAP.
- List of unused ethernet jacks with network connectivity.

[40] The Psychological Underpinnings of Security Training - Craig Higson-Smith

Network Mapping

"*A surprisingly common response from IT administrators, when confronted with a significant local vulnerability, is something like, 'Sure but that's all inside the firewall, right?' Often, this statement is technically correct—that is, after all, the point of a firewall—but one hears this even from staff who are well aware that their wireless password is the name of the organization.*"

Summary

This component allows the auditor to identify the devices on a hosts local area network, the services that are being used by those devices, and any protections in place. This component consists of network and device scanning and traffic monitoring.

Purpose

Mapping an organization's network exposes the multitude of devices connected to it – including mostly forgotten servers – and provides the baseline for later work on device assessment. This process also reveals outside service usage (such as google services, dropbox, or others) which serve – intentionally or not – as shadow infrastructure for the organization. In combination with beacon research from the network discovery process, many devices can be associated with users.

Approach

- Map hosts, servers, and other network hardware on LAN.
- Map the operating systems and services on each host.
- Capture and decrypt wireless network traffic.
- Identify commonly used external services.
- Identify vulnerable services and practices that can be exploited.[41]

Output

- A list of hosts, servers, and other network hardware on LAN
- The operating systems and services on each host.
- Services used by the host as identified by decrypted wireless network traffic.
- Possible vulnerable services and practices.[42]

[41] See: Vulnerability Analysis
[42] See: Vulnerability Analysis

Physical Assessment

"*No matter how much effort you have put into building a digital barrier around your computer, you could still wake up one morning to find that it, or a copy of the information on it, has been lost, stolen, or damaged by any number of unfortunate accidents or malicious acts. Anything from a power surge to an open window to a spilt cup of coffee might lead to a situation in which all of your data are lost and you are no longer able to use your computer. A careful risk assessment, a consistent effort to maintain a healthy computing environment and a written security policy can help avoid this type of disaster.*" - *Security in a Box* [43]

Summary

This component allows the auditor to flag potential risks related to physical access to digital assets and suggest new policies and practices.

This component consists of a staff led tour of the hosts offices during the day, and another walk-through with the auditors and the organizational point of contact, after the staff have gone home.

Purpose

While the SAFETAG framework is focused on the security of data, the physicality of devices, backup drives, servers, and even hard-wired networks cannot be overlooked.

Organizations face a variety of risks of malicious interference and device seizure, even within their office space. Easily accessible open network ports, particularly in more publicly accessible areas of the office provide entry points into trusted networks, and an insecure external backup drive could provide an adversary more valuable information than any amount of network or account based attacks would.

Ensuring that devices with data are physically secured and access to network ports, devices, and servers is limited provides a baseline level of protection from theft. Drive encryption, covered under Device Assessment, provides additional security.

Approach

- With your point of contact, walk around the office to meet staff and take note of device usage and storage.
- With your point of contact, repeat the guided tour without staff present
- Through interviews, enumerate the list of everyone who has access to the office space.

Output

- Notes on day and night time device storage and security.
- A list of everyone who has access to the office space.

[43] How to protect your information from physical threats - Security in-a-box

Data Assessment

"*One of the greatest challenges of defending your data from those who might want it is the sheer size of the information you store or carry, and the ease by which it can be taken from you. Many of us carry entire histories of our contacts, our communications, and our current documents on laptops, or even mobile phones. That data can include confidential information of dozens, even thousands, of people. A phone or laptop can be stolen, or copied in seconds.*" - *Surveillance Self Defense* [44]

Summary

This component allows the auditor to identify what sensitive data exists for the organization, where it is stored, and how it is transferred.

This component consists of a group activity where participants list the critical data within the organization, where that data resides, who currently has access, and who should be dis/allowed to access that data.

Purpose

Sensitive files are often stored across multiple devices in different levels of security. By researching not only centralized file shares, but also backups, local copies on laptops and computers, and organizational and personal use of cloud-based systems and the protections against unathorized access, the audit can recommend secure storage solutions which best meet the organizations risk assessment and workflow needs.

While the auditor has insight on some of this based on the Network Access and Network Mapping work, cross-staff understanding and agreement on what constitutes sensitive data will support later organizational change.

Approach

- Guide staff through an activity to have them list private data within the organization (e.g. Using the "personal information to keep private" handout. [45])
- With support from the Auditor, staff identify where that data is currently (what devices/physical locations), who has access (physical access, login access, and permissions), and who needs to have access to get the organizations work completed.

Output

- A map of the staff's understanding of critical organizational data:
  - what that data is,
  - where it is stored,
  - who has access,
  - who needs access.

[44] Keeping Your Data Safe - Surveillance Self-Defense
[45] The "personal information to keep private" handout can be found in the SAFETAG "full guide."

Device Assessment

"*Many important issues in computer security involve users, designers, implementors, and managers. A broad range of security issues relate to how these individuals interact with computers and the access and authorities they need to do their job. No IT system can be secured without properly addressing these security issues.*" - *Generally Accepted Principles and Practices for Securing Information Technology Systems (NIST)* [46]

Summary

This component allows the auditor to assess the security of the individual devices on the network.

This component consists of interviews, surveys, and inspection of devices.

Purpose

Compromised devices have the ability to undermine nearly any other organizational attempt at securing information. Knowing if devices receive basic software and security upgrades and what core protections against unauthorized access exist is vital to designing a strategy to make the host more secure.

Approach

- Interview individual staff
  - Identify the work and personal devices that they use to accomplish their work.
  - Have staff take the password use survey for ALL devices used for work. [47,48]
- Inspect and record information on user devices (work & personal) for security concerns (patch levels, user privileges, drive encryption, ports/services running, anti-virus capabilities)
- Inspect and record information on all devices providing services to the host organization for security concerns (patch levels, user privileges, drive encryption, ports/services running, anti-virus capabilities)
- Identify all odd/obscure/one-off services. [49]
- Run vulnerability scans against newly identified servers run by the organization.
- Using the list of software versions and patches, identify attacks and (if possible) identified malware that devices in the office are vulnerable to.

Output

- List of all assets in the organization and whom they belong to.
- List of software running on staff devices.
- List of known vulnerabilities, and identifiable malware, that the office is vulnerable to.
- List of malware found by running updated anti-virus on office computers (if anti-virus installed during device inspection.)

[46] NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems
[47] The password Survey can be found in the SAFETAG "full guide."
[48] The "password security: guides and manuals" resources list can be found in the SAFETAG "full guide."
[49] The "Identifying Odd/One-Off Services" resource list can be found in the SAFETAG "full guide."

Social Engineering Exercise

"*Individual targeting can lead to embarrassment for those individuals if testers successfully elicit information or gain access. It is important that the results of social engineering testing are used to improve the security of the organization and not to single out individuals.*" - *Technical Guide to Information Security Testing and Assessment (NIST)* [50]

Summary

This component allows the auditor to gauge staff awareness of social engineering risks. The staff take part in activities to explore what phishing look like based on sample "phishing campaign" style emails sent by the auditor as examples. The auditor and staff will discuss the consequences of having their devices compromised.

Purpose

The educational activities within this section are provided as an alternative to actual social engineering attacks against the organization. Audits of individual level behavior have a high chance of embarrassing or alienating the targeted staff. The result of this embarrassment can range from increased enthusiasm for the process to disengaging entirely. Supporting post-audit investment in the process is a core component of many activities. The possibility of derailing the investment the auditor has built during the audit makes social engineering attacks too large of a risk. [51] The security of a organization requires an investment by the entire staff. [52] Activities like the social engineering activity aim to empower staff to start identifying their responsibility for the organizational safety.

Approach

- Inform staff of the sample "phishing" emails being sent for inspection.
- Send emails to staff.
- Bring staff together for an activity where the staff members announce what they thought was suspicious, and the auditor helps reveal anything they missed.
- Lead staff in an activity identifying what critical data (as identified in during the Data Assessment) would be available to a hacker if malware were to get access to different devices.

Output

- Participants are better able to identify possible phishing attempts.
- Participants have a better understanding of how malware on one machine exposes organizational data.

[50] NIST SP 800-115, Technical Guide to Information Security Testing and Assessment

[51] "I once performed a social engineering test, the results of which were less than ideal for the client. The enraged CEO shared the report with the whole organization, as a way of raising awareness of social engineering attacks. This was made more interesting, when I visited that same company a few weeks later to deliver some security awareness training. During my introduction, I explained that my company did security testing and was responsible for the social engineering test a few weeks back. This was greeted with angry stares and snide comments about how I'd gotten them all into trouble. My response was, as always, "better to give me your passwords than a genuine bad guy"." - The Art of Writing Penetration Test Reports

[52] "CSOs should gradually build a culture in which all staff, regardless of technical background, feel some responsibility for their own digital hygiene. While staff need not become technical experts, CSOs should attempt to raise the awareness of every staff member, from executive directors to interns - groups are only as strong as their weakest link—so that they can spot issues, reduce vulnerabilities, know where to go for further help, and educate others."

Debrief

Summary

This component allows an auditor to take any immediate action needed and ensure the staff can return to their normal routine.

This component consists of any critical spot training or technical support needed, providing basic pressure relief through group and individual follow up, and planning future follow up with the host and key individuals.

Purpose

The debrief allows the auditor to ensure that they leave the host and its staff ready to start addressing their digital security. By providing some immediate outcomes to the host and its staff with a training or security consult the auditor can ensure that the host sees the audit as a guide instead of a condemnation. SAFETAG is an auditing framework designed to connect small civil society organizations and independent media outlets to the digital security services they need. But, more than that it is designed to provide audits that increase an organizations agency to seek out and address security challenges within their organization. This can be an auditor's last in-person chance to engage with the staff to shape their perspective of the audit.

Approach

- Provide assistance for any immediate action needed (Spot Training, Tool Fixes, Security consult on upcoming projects)
  - If you determine a spot-training may be necessary, consult Level Up for sample curricula and exercises.
- Discuss next steps and points of contact going forward for the host.
- Provide psyco-social care and re-framing as needed.
- Initiate follow-up with host (organizational and individual).

Output

- A date scheduled for sending in the report.
- Additional points of contact (with identified secure communications channels) if needed.

PART THREE: Analysis and Reporting

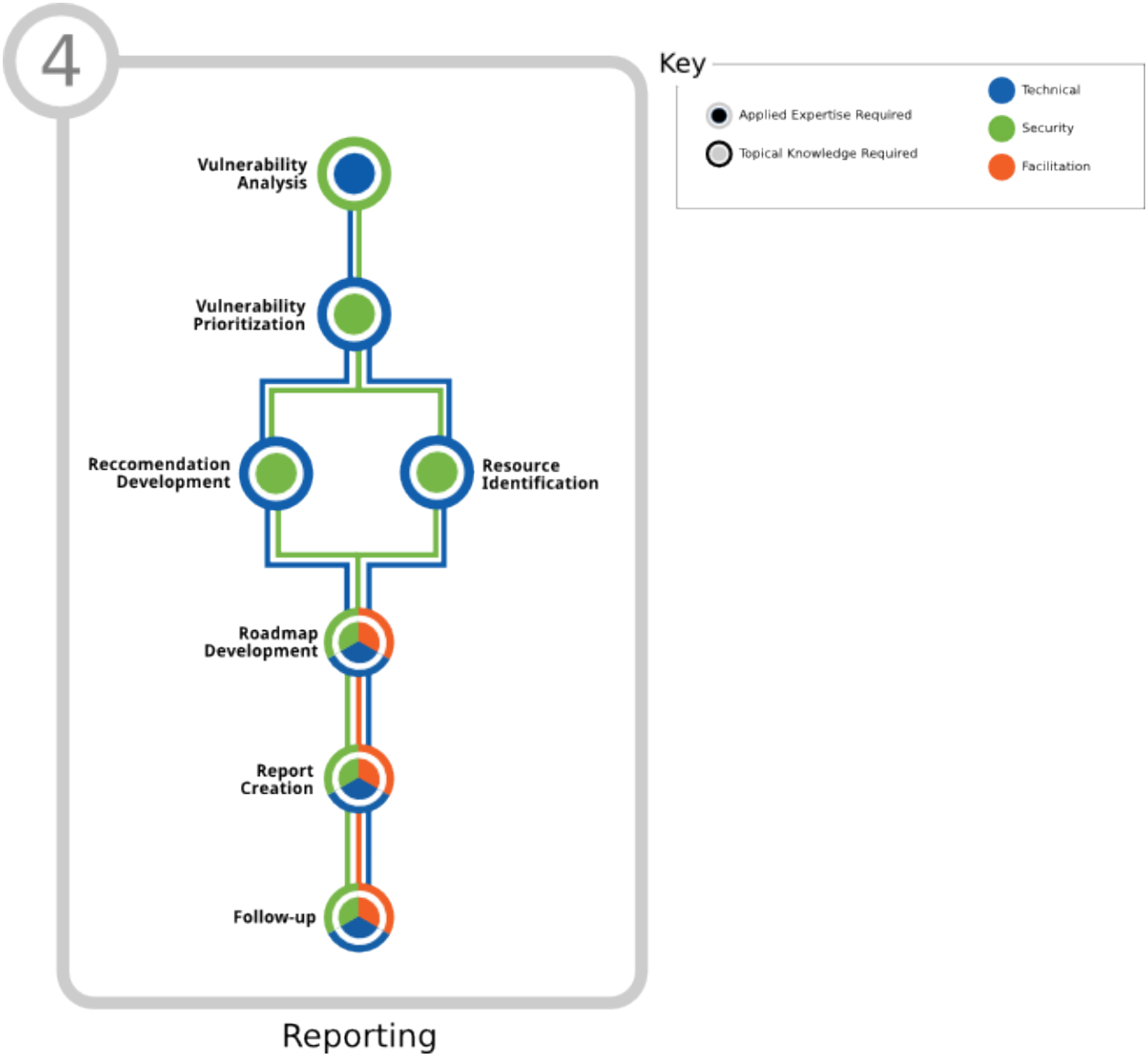

Figure 4: The Post-Audit Process

Vulnerability Analysis

"*Vulnerability testing is the process of discovering flaws in systems and applications which can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration, or insecure application design. Although the process used to look for flaws varies and is highly dependent on the particular component being tested, some key principals apply to the process.*" - *Vulnerability Analysis - The Penetration Testing Execution Standard* [53]

Summary

This component allows the auditor to discover possible flaws in host or service configuration, application design, or network design.

This component consists of comparing the services, applications, and operating systems of identified hosts against a variety of online and offline resources (vulnerability and exploit databases, vendor advisories, and virtualized replica testing) to identify if known vulnerabilities exist. Basic vulnerability analysis should be occurring along-side the other activities so that evidence can be gathered from the network, however, deeper research into identifying existing exploits can and should happen after the on-site audit to fully take advantage of the short time the auditor has on site.

Purpose

Usually penetration tests exploit possible vulnerabilities to confirm their existence. [54] But, the use of exploits puts the organization's systems at a level of increased risk [55] that is unacceptable when neither the organization nor the auditor has the time or finances to address the issue. The SAFETAG methodology only uses relatively safe exploitation of vulnerabilities for targeted outcomes. For instance, cracking the wireless access point password allows us to demonstrate the importance of good passwords without singling out any individual's passwords. [56]

Approach

- Explore Vulnerability Databases (OVAL, CVE, vendor advisories) for potential risks of systems and software used on servers, user devices, and online services (including the organization's website/CMS)
- Search Exploit Databases to find examples of exploitation of possible vulnerabilities identified.
- Explore default configurations for vulnerabilities such as default passwords or users.

Output

- Lists of OVAL/CVE identifiers for each possibly vulnerable service/system.
- Examples of live exploits for vulnerabilities where possible.
- A short write up of each vulnerability including how it was identified.
- The cleaned up output from any tests used to identify the vulnerability.

[53] Vulnerability Analysis - The Penetration Testing Execution Standard

[54] "While vulnerability scanners check only for the possible existence of a vulnerability, the attack phase of a penetration test exploits the vulne rability to confirm its existence."

[55] "Penetration testing also poses a high risk to the organization's networks and systems because it uses real exploits and attacks against production systems and data. Because of its high cost and potential impact, penetration testing of an organization's network and systems on an annual basis may be sufficient. Also, penetration testing can be designed to stop when the tester reaches a point when an additional action will cause damage." - NIST SP 800-115, Technical Guide to Information Security Testing and Assessment

[56] Network Access

Vulnerability Prioritization

"*Finding threats against arbitrary things is fun, but when you're building some-thing with many moving parts, you need to know where to start, and how to approach it.*" - *Threat Modeling: Designing for Security* by Adam Shostack [57]

Summary

This component consists of the auditor organizing the vulnerabilities identified during the audit and prioritizing them within the risk matrix.

Purpose

As part of SAFETAG's dedication to building agency and supporting organizational adoption of safer practices, a careful prioritization of vulnerabilities is invaluable in keeping audit results from appearing overwhelming. In addition, this component ranks the vulnerabilties identified using the risk-matrix developed with the host organization's staff. Using the host-created framework will allow for a deeper understanding of the impact of vulnerabilities and encourage greater investment in addressing them.

Approach

Vulnerability prioritization is a critical process. It is vital that the reasoning an auditor uses during this stage are documented and available within the report. If an auditor does not create accurate associations between the host identified impact or uses an inaccurate assessment of adversary capabilities it can lessen the credibility of the recommendations made.

- Identify vulnerabilities environment and impact (per vulnerability)
  - Identify the possible impact of the vulnerability.
  - Identify any threats to critical process' the vulnerability makes possible.
  - Identify the process with the greatest impact if interrupted.
  - Identify the possibility of exploitation.
  - Identify the level of resources required to exploit the vulnerability.
  - Compare the resources required against the capabilities identified in the risk modeling activities and the contextual research you completed.
  - Position the vulnerability on the risk matrix in relation to its likelihood and its impact.

Output

- A risk matrix with all vulnerabilities ranked on it.
- An overview of the risks the organization is accepting until they address each vulnerability.
- A short overview of the how the likelihood was determined for each vulnerability.
- A listing of the process, impact, and likelihood for each vulnerability.

[57] See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 125.

Recommendation Development

"*For each threat in your list, you need to make one or more decisions. The first decision is your strategy: Should you accept the risk, address it, avoid it, or transfer it? If you're going to address it, you must next decide when, and then how?*" [58]

Summary

This component consists of an auditor documenting the possible actions the organization could take on to address the vulnerabilities found during the audit and the difficulty of taking on those actions.

Purpose

The host needs to be able to take action after an audit. The recommendations that an auditor provides to address vulnerabilities must cover a range that allows an organization to address them in both the short-term and more comprehensively in the long-term. Based on conversations with the host it is also important to identify any vulnerabilities or adversaries that were identified that the auditor cannot identify any reasonable recommendation to protect against.

Approach

- Identify possible actions to address each vulnerability.
- Write explanations for why any adversaries or threats that the auditor identifies as "un-addressable" with the organizations current capacity.

Output

- Short-term recommendations to address each vulnerability.
- Long-term recommendations to address each vulnerability.
- Summaries of why recommendations were not given for any vulnerabilities or adversaries.

Resources

- *Guide:* "Mitigation Recommendation" (NIST SP 800-115)
- *Overview:* "How Is Risk Managed?" (An Introduction to Information System Risk Management)
- *Book:* "Digging Deeper into Mitigation's - p. 130" (Threat Modeling - Adam Shostack)[59]

[58] See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 167.
[59] "Threat Modeling: Designing for Security" by Adam Shostack

Resource Identification

Summary

In this component the auditor documents resources that the host may be able to leverage to address the technical, regulatory, organizational, or behavioral vulnerabilities identified during the audit.

This can include, but is not limited to, local technical support and incident response groups/trade organizations, places to obtain discount software, trainers, and guides/resrouces they can use to support their up-skilling.

Purpose

A SAFETAG auditor has an opportunity to act as a trusted conduit between civil society organizations in need and organizations providing digital security training, technological support, legal assistance, and incident response. As SAFETAG auditors develop deep knowledge of regional and global resources available the organizations they audit will have a greater chance of identifying resources that they can use. As auditors share resources they have identified back to the SAFETAG network, each auditor's possible impact can be increased.

Approach

- Identify trusted resources that the organization can leverage to accomplish the identified recommendations.

Output

- Lists of organizations that can assist the host accomplish their task.
- Lists of educational resources the organization can use for training.
- Contact information for recommended trainers who can help with digital security training.

Roadmap Development

"*When you are developing your security plans, consider how elements of acceptance, protection and deterrence can expand the menu of options you have at your disposal.*

Also, where there is an organisational commitment and culture of security the individual is more likely to adhere to agreed security measures. The risk of individual security plans is that they become personal good intentions that get thrown out when things are hectic." - *Workbook on Security: Practical Steps for Human Rights Defenders at Risk* [60]

Summary

This component consists of an auditor sorting their recommendations in relation to the organizations threats and capacity. The auditor builds an actionable roadmap for the organization as well as an "implementation matrix" to allow the organization to make their own informed choices about possible next steps as they move forward.

The recommendations are also placed on a time-line that includes the existing practices of the organization to show that this process is a continuation of the hosts existing in/formal security practices. [61]

Purpose

Building from the Vulnerability Prioritization work, a roadmap provides recommendations for action that are in relation to the organization's existing practices. This removes the barriers the host may feel about "starting from nothing." [62].

There are many trade-offs that have to be made when addressing threats. An organization needs to be able to weigh their possible paths forward against the time lost from program activities, the cost to implement the threat, and the other threats that they are not addressing. If the host can see how recommendations actively address threats ranked against their risk matrix to the critical processes they have identified they will be more likely to be engaged in putting those recommendations in place.

Roadmapping is used to give the host the tools to make these decisions and provide them with a recommended path forward that will allow them to make immediate gains towards protecting themselves.

Approach

- Per recommendation, create an "implementation matrix." with the urgency of the threat addressed balanced by the difficulty of implementation given available organizational capacity.
- Create a roadmap for addressing the threats faced by the organization, as revealed by Auditor research and the organization's risk matrix.
- Based upon the organizational capacity assessment, build a menu that builds upon the organizational strengths to create a path forward that provides achievable outcomes, maintains agency, and steps towards long-term difficult outcomes with high reward for the host.

Output

- An "implementation matrix" showing each recommendation in relation to its difficulty to implement and its urgency.

[60] Workbook on Security: Practical Steps for Human Rights Defenders at Risk
[61] See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 298.
[62] See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 298.

- A roadmap for a “recommended path” to address the threats the host faces.
- A short description of why a recommendation (and corresponding threat) was ranked with the urgency it was assigned.

Report Creation

"*A good analysis might turn the threats into stories so they stay close to mind as software is being written or reviewed. A good story contains conflict, and conflict has sides. In this case, you are on one side, and an attacker is the other side.*" - *Threat Modeling: Designing for Security* [63]

Summary

This component consists of an auditor compiling their audit notes and recommendations into a comprehensive set of documents the shows the current state of security, the process by which the auditor came to that assessment, and recommendations that will guide the hosts progression to meet their security goals.

Purpose

Once an auditor has left, the report is the auditor's chance to continue a conversation (albeit a static one) – even if the organization never talks to the auditor again. If written with care it can be a tool to encourage agency and guide adoption. The report has many audiences who will need to use it in different ways. For the auditor and the organization, it acts as documentation of what an auditor accomplished. For the organization, it will be guide for connecting vulnerabilities to actual risks, a rallying cry for change, and proof of need for funders. For those the organization brings in to support their digital security, it provides a roadmap towards that implementation and a task-list for future technologists and trainers paid to get the host there - as well as a checklist for validating that threats have been addressed.

Approach

- Create charts and visuals for roadmap, risk-matrix, implementation matrix, and critical processes.
- Compile approaches, impact, risk, recommendations and resources for each vulnerability.
- Prepare narrative components.
- Collect agreements & scope.
- Document tools used for testing where needed.
- Update glossary where needed.
- Compile full report contents.
- Send the report to client. [64]

Output

- A completed report delivered securely to the organizational point of contact.
- Documented process examples to submit back to SAFETAG.

[63] See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 401.

[64] "When a pilot lands an airliner, their job isn't over. They still have to navigate the myriad of taxiways and park at the gate safely. The same is true of you and your pen test reports, just because its finished doesn't mean you can switch off entirely. You still have to get the report out to the client, and you have to do so securely. Electronic distribution using public key cryptography is probably the best option, but not always possible. If symmetric encryption is to be used, a strong key should be used and must be transmitted out of band. Under no circumstances should a report be transmitted unencrypted. It all sounds like common sense, but all too often people fall down at the final hurdle." - The Art of Writing Penetration Test Reports

Follow Up

Summary

This component allows an auditor to explain and get feedback on their report as well as evaluate the success of the process over time through a continued relationship with the host.

This component consists of the final meeting with the host and following up with them after a period of a few months to see if they need further assistance, are willing to share their experience working with any of the recommended resources, or as new resources are identified.

Purpose

Follow up can be a valuable tool for encouraging an organization to continue their digital security process. But, follow up needs to be desired by an organization and achievable for the auditor. As such, follow up must be minimally intrusive on both the auditor and the host's time.

Approach

- Have a follow up call to discuss report.
- Make introduction between host and known resources as needed.
- Follow up with host after a few months to check on progress, get long-term feedback and connect with any new resources.

Auditor Trainee Tool Resource List

Recon-ng

- *Site:* "Recon-ng: Website" (Bitbucket)
- *Type:* "Recon-ng: Usage Guide" (Bitbucket)
- *Demonstration:* "Look Ma, No Exploits! – The Recon-ng Framework - Tim"LaNMaSteR53" Tomes" (Derbycon 2013)
- Other Recon-ng articles and guides [65,66,67,68]

Password Dictionary Creation

- *Documentation:* "John the Ripper password cracker" (OpenWall)
- *Password Dictionaries:* "Password dictionaries" (Skull Security)
- *Project Site:* "CeWL - Custom Word List generator" (Robin Wood)
- *Presentation:* "Supercharged John the Ripper Techniques" (Rick Redman - KoreLogic)
- *Project Site:* "Hashcat: advanced password recovery" (hashcat.net)
- *Guide:* "KoreLogic's Custom rules" (Rick Redman - KoreLogic)
- *Guide:* "Creating custom username list & wordlist for bruteforciing" (Nirav Desai)
- *Source Code:* "JohnTheRipper: bleeding-jumbo branch"

Searching

- *Online Courses:* Power Searching and Advanced Power Searching online courses (Power Searching With Google)
- *Online Course:* Advanced Power Searching By Skill (Power Searching With Google)
- *Cheat Sheet:* Google Search Operators (Google Support)
- *Cheat Sheet:* Google Hacking and Defense Cheat Sheet (SANS)
- *Cheat Sheet:* Google Searchable Filetypes (Google Support)
- *Cheat Sheet:* Google Search Punctuation Operators (Google Support)
- *Cheat Sheet:* Google Power Searching Quick Reference Guide (Power Searching With Google)
- *Database:* Google Hacking Database (Exploit Database)

[65] Tektip ep26 - Information gathering with Recon-ng Video Tutorial
[66] toolsmith guide to Recon-ng
[67] The Recon-ng Framework : Automated Information Gathering
[68] Professionally Evil Toolkit - Recon-ng

Social Engineering Toolkit

- *Guide:* "Hack Like a Pro: How to Spear Phish with the Social Engineering Toolkit (SET) in BackTrack" (WonderHowTo)
- *Guide:* "Phishing and Social Engineering Techniques 3.0" (INFOSEC Institute)
- *Source Code Repository:* "Social Engineering Toolkit source code repository" (GitHub)
- *Overview:* "Overview of The Social Engineering Toolkit" (The Penetration Testing Execution Standard)

Social Engineering (Alternatives to Social Engineering Toolkit)

- *Game:* "Cybersecurity Lab" (NOVA Labs)
- *Cartoons:* "Oops… I clicked! A Phishing Cartoon Collection." (Security Cartoon)
- *Quiz:* "PHISHING QUIZ: Think you can Outsmart Internet Scammers?" (OpenDNS)
- *Guide:* "10 Tips on How to Identify a Phishing or Spoofing Email (Lauren Soares)
- *Guide:* "How to recognize phishing email messages, links, or phone calls" (Microsoft Safety & Security Center)
- *Guide:* "Identifying fraudulent"phishing" email" (Apple Support)

Website Vulnerability Scanning

- *Site:* "OWASP ZAP Project Site" (OWASP)
- *Guide:* "The OWASP Testing Project Guide" (OWASP)
- *User Guide:* "OWASP Zap User Guide" (Google Code)
- *Video Tutorials:* "OWASP ZAP Tutorial Videos" (Google Code)
- *Guide:* "7 Ways Vulnerability Scanners May Harm Website(s) and What To Do About It" (White Hat Sec Blog)

System Vulnerability Scanning

- *Project Site:* "OpenVAS Project Site" (OpenVAS)
- *Manual:* "OpenVAS Compendium" (OpenVAS)
- *Guide:* "How To Use OpenVAS to Audit the Security of Remote Systems on Ubuntu 12.04" (Digital Ocean)
- *Guide:* "Getting Started with OpenVAS" (Backtrack Linux)
- *Guide:* "Setup and Start OpenVAS" (OpenVAS)
- *Video Guide:* "Setting up OpenVAS on Kali Linux" (YouTube)
- *ListServ:* "OpenVAS Discussion ListServ" (OpenVAS)
- *Comparison:* "Nessus, OpenVAS and Nexpose VS Metasploitable" (HackerTarget)

Nmap Scanning

- *Guide:* "The Official Nmap Project Guide to Network Discovery and Security Scanning" (Gordon "Fyodor" Lyon)
- *Cheat Sheet:* "Part 1: Introduction to Nmap" (Nmap Cheat Sheet: From Discovery to Exploits)
- *Cheat Sheet:* "Part 2: Advance Port Scanning with Nmap And Custom Idle Scan" (Nmap Cheat Sheet: From Discovery to Exploits)
- *Cheat Sheet:* "Part 3: Gathering Additional Information about Host and Network" (Nmap Cheat Sheet: From Discovery to Exploits)
- *Cheat Sheet:* "Part 4" (Nmap Cheat Sheet: From Discovery to Exploits)
- *Cheat Sheet:* "Nmap Cheat Sheet" (See-Security Technologies)
- *Overview:* "The Purpose of a Graphical Frontend for Nmap" (Zenmap GUI Users' Guide)
- *Guide:* "Zenmap GUI Users' Guide" (Zenmap GUI Users' Guide)
- *Guide:* "Surfing the Network Topology" (Zenmap GUI Users' Guide)
- *Guide:* "Host Detection" (nmap Reference Guide)

Setup Aircrack-ng

- *Guide:* "Aircrack-ng Newbie Guide for Linux" (Aircrack-ng Wiki)
- *Tutorial:* "Injection test" (Aircrack-ng Wiki)
- *Tutorial:* "Is My Wireless Card Compatible?" (Aircrack-ng Wiki)
- *Guide:* "Compatibility, Drivers, Which Card to Purchase" (Aircrack-ng Wiki)
- *Guide:* "Installing Drivers" (Aircrack-ng Wiki)
- *Guide:* "Tutorial: How To Patch Drivers" (Aircrack-ng Wiki)

Wireless Access Guides & Resources

- *Documentation:* "Aircrack-ng" (Aircrack-ng Wiki)
- *Documentation:* "Airodump-ng" (Aircrack-ng Wiki)
- *Documentation:* "Aireplay-ng" (Aircrack-ng Wiki)
- *Tutorial:* "Bypassing MAC Filters on WiFi Networks" (techorganic.com)
- *Tutorial:* "Simple WEP Crack" (Aircrack-ng Wiki)
- *Tutorial:* "Simple Wep Cracking with a flowchart" (Aircrack-ng Wiki)
- *Tutorial:* "How to Crack WPA/WPA2" (Aircrack-ng Wiki)
- *Guide:* "Hacking my own router with Reaver, guide to brute forcing Wifi Protected Setup" (Nathan Heafner)
- *Guide:* "WPS – How to install and use Reaver to detect the WPS on your home router" (University of South Wales)

- *Tutorial:* "Resetting WPS Lockouts" (Kali Linux Forums)
- *References:* "Links, References and Other Learning Materials" (Aircrack-ng Wiki)
- *Project Site:* "wifite: automated wireless auditor" (Google code)
- *Source Code:* "wifite" (GitHub)
- *Guide:* "Cracking WPA2 WPA with Hashcat in Kali Linux" (darkmoreops.com)
- *Guide:* "Cracking WPA/WPA2 with oclHashcat" (Hashcat wiki)

[^HCD_toolkit]"IDEO Human-Centered Design Toolkit"

[^Techscape_indicators]"TechScape Indicators - the engine room"