SAFETAG

A SECURITY AUDITING FRAMEWORK AND EVALUATION TEMPLATE FOR ADVOCACY GROUPS

Guide

Internews
Local voices. Global change.

LICENSE

ATTRIBUTION FOR CONTENT FROM OTHER LICENSES

USAGE OF "SAFETAG"

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.

SAFETAG uses a customized combination of selected assessment activities 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. SAFETAG auditors lead an organizational risk modeling process that helps staff and leadership take an institutional lens on their digital security problems, conduct a targeted digital security audit to expose vulnerabilities that impact the vital processes and assets identified, and provide post-audit reporting and follow up that helps the organization and staff identify the training and technical support that they need to address needs identified in the audit, and in the future.

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

The SAFETAG Audit Framework Core

The SAFETAG audit consists of multiple information gathering and confirmations steps as well as research and capacity-building exercises with staff organized in a collection of objectives, each of which supports the core goals of SAFETAG, creating a risk assessment while also building the capacity of the organization.

These objectives provide collections of approaches and activities to gather and verify information in both technical and interactive/social methods, assess and build capacity, and targeted exercises with walk-through instructions for many of these.

These are not meant to be a "checklist" or even a prescribed set of actions -- indeed, experienced auditors will deviate strongly from many of the specific activities. These provide a focused "minimal set" of activities only.

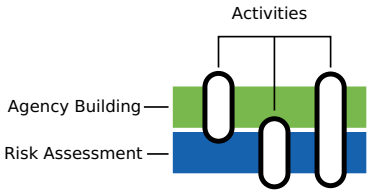
Indeed, many objectives and their specific exercises overlap or can be done together -- on-site interviews with staff can coincide with assessing their devices and keeping one's eyes open for physical security issues. The data assessment exercises may provide enough information that other staff engagements are unnecessary.

THE LIFE CYCLE OF AN AUDIT

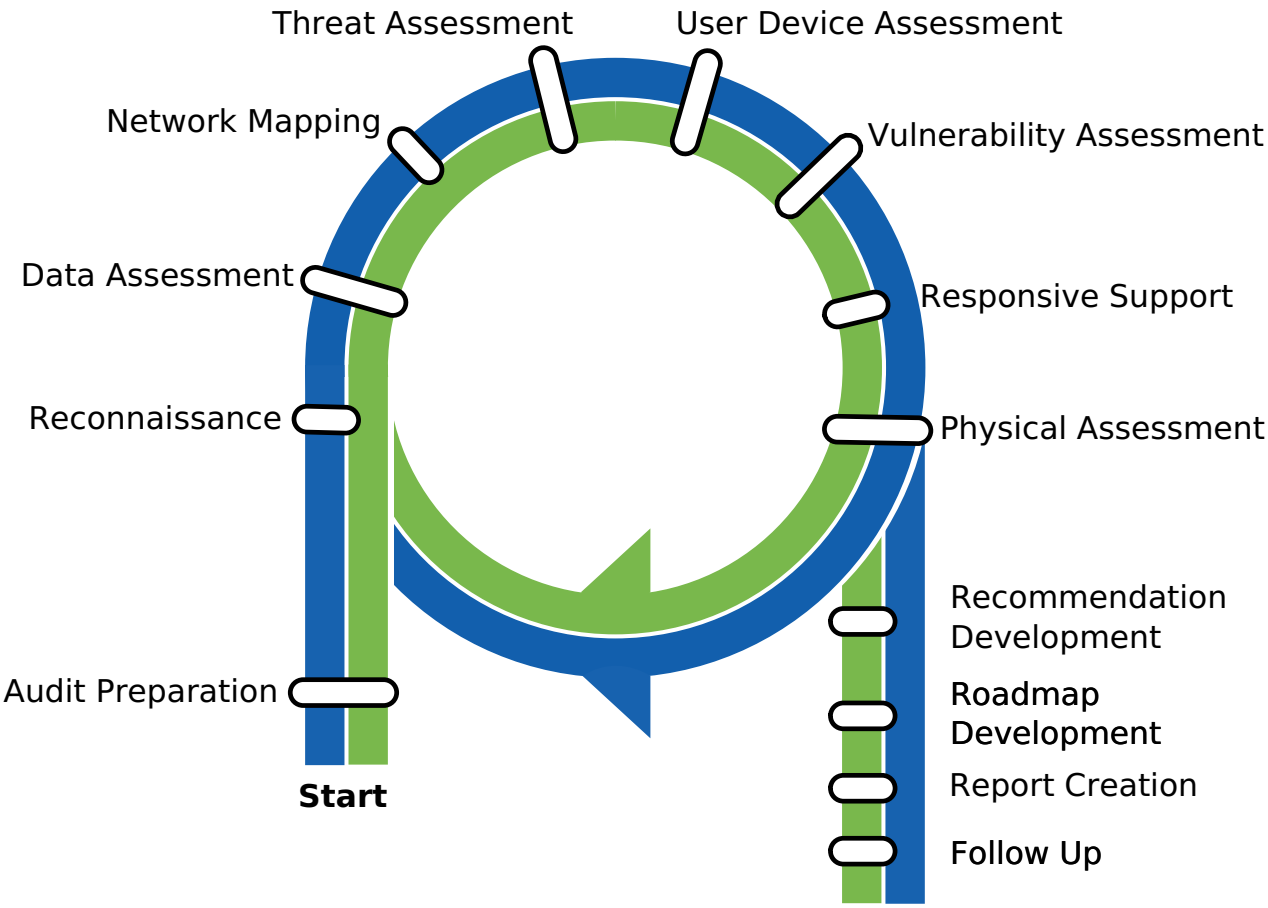
Audit Flow

SAFETAG

Activities Overview



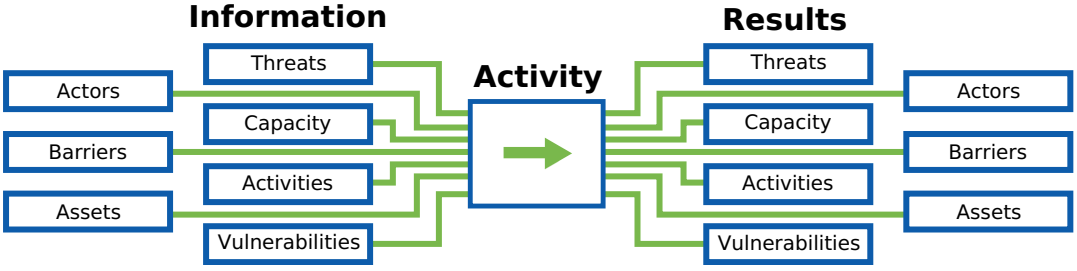
Legend



SAFETAG Activities

The audit process in very cyclical. Newly identified threats, vulnerabilities, capabilities, and barriers impact activities that have and have yet to be run. At the same time the auditor, through conversations, training, and group activities is actively building the organization's agency and addressing time-sensitive or critical threats that are possible within the time frame. This iterative process eventually leads to a point where the auditor is confident they have identified the critical and low hanging fruit, and is confident the organization is capable of moving forward with their recommendations.

Each objective requires a certain base of information, and outputs more information into this cyclical process. Each objective has a "map" of the data flow that it and its specific activities provide based on this map:



While more completely defined below in the Risk Assessment and Agency Building sections, a brief overview of the data flow components:

- **Actors** Actors are the people connected to an organization include an organization's staff, board members, contractors and partners. Actors could also include volunteers, members of a broader community of practice, and even family members. Actors also include potential adversaries of the organization such as competing groups.
- **Activities** Activities are the actions and processes of an organization. While most NGO work revolves around mission-based concepts, activities also include things like payroll.
- **Capacity** Indicators of capacity include staff skills and a wide variety of resources that an organization can draw from to affect change.
- **Barriers** Barriers are specific challenges an organization faces that might limit or block its capacity.
- **Assets** Assets are most easily conceptualized as computer systems - laptops and servers, but also include both the data stored on them and can also be services like remote file storage, hosted websites, webmail, and more. Offline drives, USB sticks, and even paper printouts of relevant or sensitive information can also be included
- **Vulnerabilities** Vulnerabilities are specific flaws or attributes of an asset susceptible to attack.
- **Threats** A Threat is a specific, possible attack or occurrence that could harm the organization. If a bucket of oily rags is a vulnerability, a fire is the threat - and mitigations would be rules against leaving oily rags around as well as fire extinguishers, smoke detectors, remote backup policies, and evacuation planning.

To make SAFETAG approachable, a core evaluation template which links together a series of specific objectives, each with a variety of linked activities, that contribute towards the goals and their required information needs is represented here. Experienced Auditors will likely come up with their own approaches, and the SAFETAG project welcomes such contributions.

RISK ASSESSMENT & ANALYSIS

Functionally, SAFETAG is a digital risk assessment framework. Risk assessment a systematic approach to identifying and assessing risks associated with hazards and human activities. SAFETAG focuses this approach on digital security risks. A SAFETAG audit will work to collect the following types of information in order to assess the risks an organization faces.

Risk is the current assessment of the possibility of harmful events occurring. Risk is assessed by comparing the threats an actor faces with their vulnerabilities, and their capacity to respond to or mitigate emergent threats.

The SAFETAG evaluation revolves around collecting enough information to identify and assess the various risks and an organization and its related actors face so that they can take action strategically.

$$\text{RISK} = \frac{\text{THREAT} \times \text{VULNERABILITY}}{\text{CAPACITY}}$$

The Risk Equation

PROGRAM ANALYSIS

Program analysis identifies the priority objectives of the organization and determine its capacities. This process exposes the activities, actors, and capacities of an organization.

Activities

Definition: The practices and interactions that the organization carries out in order to accomplish their goals.

Example: This includes any activity that the organization carries out to accomplish its goals and those that allow the organization to function (publishing, payment, fund-raising, outreach, interviewing.)

- What is the main purpose of the organization?
- What are the processes the organization takes part in to carry out their work?

Actors

Definition: The staff, volunteers, partners, beneficiaries, donors, and adversaries associated with the organization.

Example: The core organizational staff, the volunteers, maintenance, cleaning, security, or other non-critical staff, the partner organizations, the individuals and groups that the organization provides services to, groups of unorganized individuals who are opposed to organizational aims, governmental and non-governmental high-power agents and organizations that are opposed to the organizations aims.

- What staff does the organization have?
- Are their volunteers, maintenance, cleaning, security, or other non-critical staff who have access to the office?
- Who does the organization serve?
- Does the organization have any partners?
- Who are the organizations beneficiaries?

VULNERABILITY ANALYSIS

Understand the organisation’s exposure to threats, points of weakness and the ways in which the organisation may be affected.

Vulnerability

Definition: A attribute or feature that makes an entity, asset, system, or network susceptible to a given threat.

Example: This can include poorly built or unmaintained hardware, software, or offices as well as missing, ignored, or poor policies or practices around security.

THREAT ANALYSIS

Threat analysis is the process of identifying possible attackers and gathering background information about the capability of those attackers to threaten the organization. The basis of this information is a potential threats **history** of carrying out specific threats, their **capability** to carry out those threats currently, and proof that the threat has **intent** to leverage resources against the target.

Threat

Definition: A threat is a possible attack or occurrence that has the potential to harm life, information, operations, the environment, and/or property.

Example: Threats can range from *fire,* or *flood,* to *targeted malware, physical harassment,* or *phishing attacks.*

Threat History

Definition: What types of threats has the attacker used historically. And, what types of actors have been targeted by those threats.

Example:

- What history of attacks does the threat actor have?
- What techniques have they used? Have they targeted vulnerabilities that the organization currently has?
- Have they targeted similar organizations?
- What is known about the types of threats used by an threat actor to attack similar organizations?

Threat Capability

Definition: The means that the attacker has to carry out threats against the organization.

Example: This includes, but is not limited to technical skill, financial support, number of staff hours, and legal power.

- Does the threat actor have the means to exploit a vulnerability that the organization currently has?
- Does the threat actor have the means to leverage widespread threats against all similar organizations, or will they have to prioritize their targets?

Threat Intent

Definition: The level of desire for the attacker to carry out threats against the organization.

Example: Intent can be goals or outcomes that the adversary seeks; consequences the adversary seeks to avoid; and how strongly the adversary seeks to achieve those outcomes and/or avoid those consequences.

- Does the threat actor currently have the desire to conduct an attack against this type of organization?
- Is the organization a priority threat target for the threat actor?

AGENCY BUILDING

SAFETAG differs from many risk assessment tools because it aims to build the host's and staff's capacity so that they are able to address the risks that the auditor has identified. SAFETAG is designed to provide in-audit activities and training that increase an organizations agency to seek out and address security challenges within their organization. To do this an auditor must collect information that allows them to identify organizational areas of strength and weakness (expertise, finance, willingness to learn, staff time, etc.)

A common refrain, among auditors, software developers and other specialists in this sector, is that digital security is not about technology; it is about people. This is undeniably true, and even the previous SAFETAG modules — despite their more direct fixation on technology — acknowledge this insight by emphasizing the educational and a persuasive roles played by your findings report.

Capacity

Definition: The combination of strengths, attributes and resources available within the organization that can be used to reduce the impact or likelihood of threats.

Example: This includes, but is not limited to technical skill, financial support, staff and management time, relationships, and legal power.

Barriers

Definition: The combination of weaknesses, assumptions, regulations, social or cultural practices, and obligations that get in the way of an organization implementing an effective digital security practice.

Example: Examples can include a lack of funding, lack of authority within an organization to mandate practices to their staff, resistance to change, high staff turnover, or digital illiteracy.

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.*" - *Needs Assessment: Level-Up* [1]

SUMMARY

Below are the baseline operational security guidelines for a SAFETAG audit. Activity specific operational security guidelines are contained within each activity.

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.

APPROACHES

- Data storage and transit security
  - Keep ALL data related to the assessment secured and compartmentalized, from interview and research notes through audit findings and reporting outputs. Auditors should note where tools (such as OpenVAS or recon-ng) store their internal data. Practically speaking, LUKS or VeraCrypt volumes are useful, secure, and portable. The auditor should modify their data storage approach based on threat information from their context research as well as ongoing inputs.
  - Consider what secure storage options the organization will need to have in place to store the final report and findings documents.
  - Consider if the raw data may be at risk during transit post-audit and plan mitigations in advance of travel (e.g. completing the report on-site or uploading to a secure remote server and securely deleting all data locally.)
  - Refer back to the agreement established with the organization.
- Communications security
  - Conduct all communication with the client over at least minimally secure channels where the communication is encrypted in transit at all times. Consider risks to the organization and the auditor(s) if the organization is actively compromised.
  - Higher levels of security with end-to-end guarantees (such as Signal, PGP, veracrypt, or peerio/minilock) should be used for file and document transfers.
  - Training and support may be required to ensure the organization is able to reliably and securely receive such communications.
- Data Deletion
  - When assessment data is to be destroyed (by the auditor or organization), ensure secure data deletion processes are followed.

RESOURCES

- *Standard*: NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (Section 7.4)
- *Standard*: Pentest Standards for data security
- *Guide*: Surveillance Self Defense (cross-platform guides for WhatsApp, Signal, PGP, and OTR secure communications)
- *Guide*: Security in a box: Secure File Storage
- *Guide*: Digital First Aid Kit: Secure Communications

SAFETAG Methods

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 and in coordination with the organization.

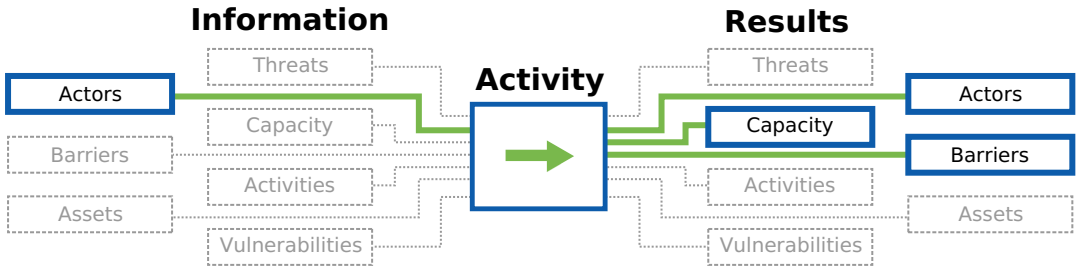
PURPOSE

A SAFETAG audit has a short time frame. Preparation is vital to ensure that time on the ground is not spent negotiating over the audit scope, updating the auditors systems, searching for missing hardware, or refreshing oneself with the SAFETAG framework. To that end negotiations with the host organization help reveal if the organization has the capacity to undertake the audit and respond to its findings.

GUIDING QUESTIONS

- Does the organization have existing digital security practice or attempted to implement them in the past?
- What is the process for procedure for incident handling in the event that auditor cause or uncover an incident during the course of the assessment?
- What are the legal, physical, or social risks for the auditor & organization associated with conducting the audit or having audit results leak? [2]
- Does the security situation of the location or organization require additional planning? Are your software tools up to date and working as expected?

THE FLOW OF INFORMATION



Preparation Information Flow

APPROACHES

- **Create an Assessment Plan:** Have a "scoping" meeting that outlines the level of access that an auditor will have, what is off limits, and the process for modifying the scope of the audit when new information arises. [3,4]
- **Negotiate a Confidentiality Agreement:** Negotiate an agreement with the organization that outlines how an auditor will protect the privacy of the organization and the outcomes of the audit.
- **Establish an Emergency Contact:** Establish a procedure for incident handling and an emergency contact in the event that auditor cause or uncover an incident during the course of the assessment. [5,6]
- **Conduct Research** (See **Context Research**) to identify potential adversaries and their capabilities, and explore the latest cyber security and topical trends, to assess risk for the auditing process itself.
- **Prepare for Travel:** Check travel logistical needs -- visa, letter of invitation, 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.
- **Prepare Systems:** Update and test your systems, A/V and audit tools. [7], prepare storage devices and systems to reflect the required operational security, and ensure you have power supply adapters, cables and relevant adapters, usb drives, external wireless cards and any other equipment needed for testing. [8]^, [9]

OUTPUTS

- Any Visas or paperwork needed, plus travel arragements (tickets, hotels) for auditor travel.
- A custom password dictionary. [10]
- A travel kit. [11,12]
- Systems updated and ready for testing.
- Risks to host and auditor conducting a SAFETAG audit.
- Modifications to the audit plan as necessary.

OPERATIONAL SECURITY

- Update your OS, software, anti-virus, firewall settings, etc. (Do not be the weakest link for the host!)
- Determine the correct visa process for your trip.
- Carefully consider packing needs and explanations

RESOURCES

- *Tip Sheet:* Facilitator Preparation Tips (Integrated Security)
- *Resource List:* Password Dictionary Creation Resources (SAFETAG)
- *Resource List:* Social Engineering Resources (SAFETAG)

Facilitation Preparation

- *Tip Sheet:* Facilitator Preparation Tips (Integrated Security)
- *Guidelines:* "Facilitator Guidelines" (Aspiration Tech)
- *Guide:* "Session_Design" (Aspiration Tech)
- *Kit:* "Resource Kit" (eQualit.ie)
- *Questions:* "Pre-Event_Questions" (Aspiration Tech)
- *Guide:* "Break Outs" (Aspiration Tech)
- *Resources:* "Be a Better Trainer" (Level-up)

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"
- *Standard:* "Pre-Engagement" (The Penetration Testing Execution Standard: Pre-Engagement Guidelines)
- *Template:* Pre-Inspection Visit (VulnerabilityAssessment.co.uk)
- *Template:* "Rules of Engagement Template" (NIST SP 800-115)
- *Article:* "Legal Issues in Penetration Testing"

Other Pre-Engagement Resources

- *Standard:* "Pre-Engagement" (The Penetration Testing Execution Standard: Pre-Engagement Guidelines)
- *Template:* Pre-Inspection Visit (VulnerabilityAssessment.co.uk)

Incident Handling Resources

- *Guide:* "Six Stages of Incident Response" (CSO Online: Anthony Caruana)
- *Guide:* "Threat Hunting Project" (http://www.threathunting.net)

Legal Considerations

- *Resource:* "Media Legal Defense Initiative" (Media Legal Defense Initiative)

Data Security Standards

Sensitive Data & Information Guides

- *Guide:* "Security Incident Information Management Handbook" (RedR UK)

Incident Handling Resources

- *Guide:* "Six Stages of Incident Response" (CSO Online: Anthony Caruana)
- *Guide:* "Threat Hunting Project" (http://www.threathunting.net)

ACTIVITIES

ASSESSMENT PLAN

Summary

This component allows an auditor and host to come to an understanding of the level of access that an auditor will have, what is off limits, and the process for modifying the scope of the audit when new information arises. [13,14] This component consists of a process where the auditor collaboratively creates an assessment plan with key members of the organization.

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.

Overview

- Determine a point person for the audit and exchange contact information. [15]
- Explain and get approval to the scope of audit from the host. [16,17]
- Agree to the time-line, location, and attendees of the on-site audit. [18]
- Codify data security standards for audit communication and evidence handling. [19]
- If funded externally, identify what should be reported to external funder. [20]

Materials Needed

- To use the SAFETAG Agreement Generator, a Debian-based Linux system with python and other requirements as detailed in the Agreement Generator README are required.

Considerations

- Consider the threat landscape of the organization when determining secure communications channels. This may require some pre-agreement work using parts of the Context Research methodology.
- In addition to the overall mandate to send information encrypted to the organization, also demand encrypted communication back from them. Failure to establish a secure planning channel also contributes towards a no-go situation by putting both the auditor and organization at risk.

Walkthrough

- 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. [21]
  - The responsibilities of the host staff.
  - The responsibilities of the auditor.
  - The host names and IP ranges of any services run by the organization. [22]
  - Emergency contact information for the organization. [23]
  - The procedure the auditor will follow when handling incidents. [24]
  - The data security standards for evidence handling and communication. [25]
- A liability waiver signed by the host organization. [26]
- Approval from any third parties. [27]

Auditors are encouraged to use, or at least reference, the SAFETAG Agreement Generator, a python script which provides a decision tree covering the above points, and builds a basic, clear-language agreement which can be translated and formalized as needed. Sample outputs and a diagram of the full decision tree are available in the "outputs" folder of the Agreement Generator repository. This replaces the draft agreement previously part of SAFETAG.

Recommendation

CONFIDENTIALITY AGREEMENT

Summary

Negotiate an agreement with the organization that outlines how an auditor will protect the privacy of the organization and the outcomes of the audit.

Overview

- Host provides auditor consent to conduct the agreed to scope of the audit in the form of a signed liability waiver. [28]

Materials Needed

Considerations

Walkthrough

See the Appendix for a DRAFT Engagement and Confidentiality Agreement. See also the in-progress SAFETAG Agreement Generator for more advanced and flexible "plain language" agreement text and guidance on selecting which clauses to incluce.

Recommendation

INCIDENT RESPONSE AND EMERGENCY CONTACT

Summary

Establish a procedure for incident handling and an emergency contact in the event that auditor cause or uncover an incident during the course of the assessment. [29,30]

Overview

- Establish what severity counts as an "incident" for the organization
- Agree on primary and secondary points of contact and relevant contact information
- Agree on security protocols around incident response
- Create procedure for incident handling in the event that auditor cause or uncover an incident during the course of the assessment. [31,32]

Materials Needed

Considerations

Walkthrough

TRAVEL CHECKLIST

See the Appendix for a sample travel kit / checklist

PASSWORD DICTIONARY CREATION

See the Appendix for creating a password dictionary.

AUDIT TIMELINE AND PLANNING

Review these notes in preparation for the audit as you begin to map out your schedule. This provides a rough, suggested outline of how to schedule your time on site for a SAFETAG audit, and some reminders of the work you need to have completed before arriving in country.

PREPARE FOR UNCERTAINTY

The SAFETAG roadmap is a crisp, clear data flow of inputs to outputs. Reality, generally speaking, is less direct. There are a few core parts of the audit process that force action, but others are more flexible. Outcomes of your discussion and exploration of the network will also de-rail the process in impossible-to-predict ways. The pre-audit interviews and your own contexts research, research on the organization, and preparation are meant to give you the best possible idea of what situation you'll walk in to, but even with all of that, frankly, shit happens.

Before Travel

- Agreements, Scope, Risk Analysis
- Remote Research
- Openly sourced data: DNS, MX, Web, research via social media and google
- Revealed information via Skype / etc. (office IP address?), nmap
- Packing and Prep
- Visas / Travel planning
- Hardware packing
- Software (run updates) and dictionary list prep (local language dictionaries, plus creation of a custom password list based on website keywords, addresses, and dates)

FIRST DAY

Priorities for the first day include meeting staff (even, possibly especially, for the more technical auditor). There is a strong temptation to dive in and get started, but establishing connections with the staff - especially those you haven't met through interviews - is key. You may discover hidden sources of talent or resistance, historical information, and new parts of the infrastructure or practices and policies that you may not have yet found.

- Meet staff, discuss operations and plan interruptions with key staff
- In-person discussions of risks, challenges, fears, questions, and experiences around digital security
- (If relevant) Attempt to crack wifi without password knowledge
- Parallel, collect wifi beacons while not associated to any one network (sending connection resets).
- Once wifi password is obtained (through cracking or asking), start a capture of decrypted traffic and run it as long as possible for later analysis
- Map out the “visible” network (nmap)

EARLY STEPS

From a data-gathering point of view, the first steps are to try and access the wireless network by password guessing, but also to connect to the network and capture traffic for analysis overnight. This provides other views on the actual technology and services used on the network, different both from the management and IT view as well as other tools discussed by staff.

First or Second day

- Associate nmap scans, MAC addresses, and beacons with people and specific systems, plus servers/networking hardware
- Scans on the captured traffic for passwords, auth cookies, suspicious traffic, unencrypted connections

Further Days (on Location) The next day you’re on location, you have hopefully looked through the research data you gathered, and have some specific follow-up things to investigate. It’s also now time to start going through the audit tasks.

- Deeper dive into what hardware is connected and what it is doing
- Begin organizing vulnerabilities and tracking against the audit framework
- External audit tasks

- Internal audit tasks
- Physical audit tasks

Final Day (on Location)

- Discuss initial findings and responses
- Suggestions for follow-up training, resources to consult, and possibly targeted trainings for relevant staff (what is a secure password? How to communicate securely?)
- Discuss next steps: SAFETAG Report, connections to trainers, how to seek help

EXPLORATION AND CHECK-INS

Throughout the entire audit, aggressively make time to engage with staff - stop for coffee, eat lunch with them, have conversations. This can be integrated in to other parts of the process, such as the user device assessments, as well as being completely independent and natural. Having better connections with staff will make the group exercises, especially the risk assessment work, flow much better.

Whenever you set off a scan (airodumping, nmap, openvas...) are good times to stand up and walk around.

DEBRIEF AND SETTING EXPECTATIONS

Largely covered in the [debrief section], making time at the end of the (often hectic) audit week is very important to making sure the next few steps are absolutely clear in terms of timelines and communication protocols.

CLEAN UP

If you have been using paper or post-it notes during the audit, be sure you securely destroy them (by shredding, burning, or tearing into small pieces) before you leave the site on the last day. By the same token, any digital reports should be stored on secure media and securely deleted from all other locations. See the operational security section and per-item notes for further details. Clean off any whiteboards used, and check any camera used to remove sensitive photos.

FOLLOW UP CARE AND REPORTING

See the reporting sections for specific details here, but a series of check-ins with the organization to support their ability to respond to any incidents, understand further topics from the debrief, and to help provide them a timeline to expect the final report is valuable in maintaining their engagement post-audit to support the needed changes.

CONTEXT RESEARCH

SUMMARY

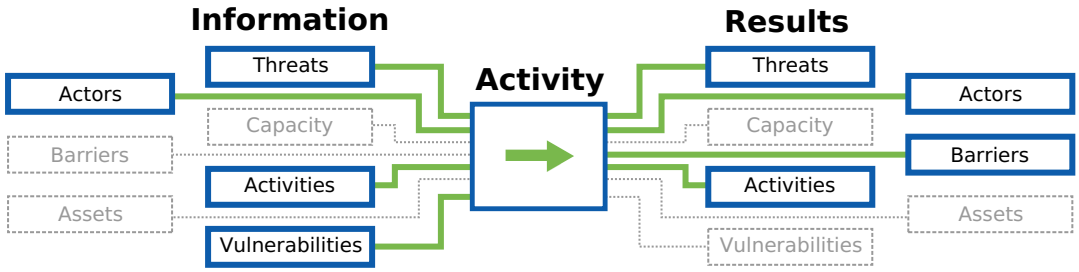
This component allows the auditor to identify the relevant regional and technological context needed to provide a safe and informed SAFETAG audit. This component consists of desk research that is collected and analyzed by the auditor, as well as inputs from the Interview component.

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.

THE FLOW OF INFORMATION



Information Flow

GUIDING QUESTIONS

- What infrastructural barriers exist in the region?
- What are the top, non-targeted digital threats in this region?
- What are the top targeted digital threats facing organizations doing this work in this region / country?
- Are there legal ramifications to digital security in the country? (e.g. legality of encryption, anonymity tools, etc.)
- Has any organization or individual made specific threats, or demonstrated intention or mindset to attack on the organization or similar organizations?

APPROACHES

- Conduct Regional Context Research to identify additional adversaries not previously identified
- Conduct Technical Context Research to discover infrastructure issues and explore the latest cyber security trends.

OUTPUTS

- 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.

OPERATIONAL SECURITY

- Use VPNs or Tor to search if conducting the search from a country that is highly competitive with the organization's country, or is known to surveil.

PREPARATION

RESOURCES

Other Context Analysis Methodologies

- *Article:* "Section 2.3 Context analysis p. 30" (Operational Security Management in Violent Environments: (Revised Edition))
- *Guide:* "Vulnerability Assessment: Training module for NGOs operating in Conflict Zones and High-Crime Areas" (Jonathan T. Dworken)

Threats to the Auditor

Have aid workers faced retribution for their work in the region?

- *Database:* "The Aid Worker Security Database (AWSD) records major incidents of violence against aid workers, with incident reports from 1997 through the present." (The Aid Worker Security Database (AWSD))

Is it safe to do digital security work in the region?

- *Survey:* "This is a survey of existing and proposed laws and regulations on cryptography - systems used for protecting information against unauthorized access. " (The Crypto Law Survey)
- *Article:* "Legal Issues in Penetration Testing" (Security Current)
- *Guide:* "Encryption and International Travel" (Princeton University)
- *Guide:* "World Map of Encryption Laws and Policies" (Global Partners Digital)

Is the area safe to travel to?

- *List:* "Foreign travel advice" (GOV.UK)
- *Alerts:* "Travel Alerts & Warnings" (US Department of State)
- *List:* "List of airlines banned within the EU" (European Commission)
- *List:* "A list of aircraft operators that have that have suffered an accident, serious incident or hijacking." (Aviation Safety Network)
- *List:* "Travel Advice" (Australian Government)

Targeted Threats for the organization

Is the group facing any legal threats because of its work?

- *Monitor:* "CNL's NGO Law Monitor provides up-to-date information on legal issues affecting not-for-profit, non-governmental organizations (NGOs) around the world." (NGO Law Monitor)

Does the organization face any targeted threats because of their work?

- Human Rights
  - Freedom House's "Freedom in the World" index is the standard-setting comparative assessment of global political rights and civil liberties.
  - Amnesty International regional news on human rights
  - Human Rights Watch - Browse by Region
- Transparency
  - Corruption Perception Index
- Public Service Delivery
- Health

- Free Media and Information
  - Threatened Voices: Tracking suppression of online free speech.
  - IREX's Media Sustainability Index (MSI) provides in-depth analyses of the conditions for independent media in 80 countries across the world.
  - Freedom House's "Freedom on the Net" index, assessing the degree of internet and digital media freedom around the world.
  - Freedom House's "Freedom of the Press" index assess' global media freedom.
  - ARTICLE 19 freedom of expression and freedom of information news by region.
  - Open Society Foundation - Mapping digital media
  - Press Freedom Index (RSF)
- Climate Issues
- Gender Issues
- Poverty Alleviation
- Community Building
- Peace promotion
- Agricultural Development
- Entrepreneurship
- Water, Sanitation
- Transportation
- Disaster Relief

General Threats for the organization

What general non-governmental threats does the organization face?

- *Map:* "A global display of Terrorism and Other Suspicious Events" (Global Incident Map)
- *Organization:* "ReliefWeb has been the leading source for reliable and timely humanitarian information on global crises and disasters since 1996." (ReliefWeb)
- *Reports:* International NGO Safety (NGO proof, subscription required, covers Afghanistan, CAR, DRC, Kenya, Mali, and Syria currently)

What cyber-security practices is the government using?

- *Reports:* Privacy International's in-depth country reports and submissions to the United Nations. (Privacy International)
- *List:* "National Cyber Security Policy and Legal Documents" (NATO Cooperative Cyber Defence Centre of Excellence)
- *Reports:* "Country Reports" (Open Network Inititiative)
- *Portal:* "Country Level Information security threats" (The ISC Project)
- *Country Profiles:* "Current cybersecurity landscape based on the five pillars of the Global Cybersecurity Agenda namely Legal Measures, Technical Measures, Organisation Measures, Capacity Building and Cooperation." (Global Cybersecurity Index (GCI))
- *Organization:* "The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, Canada focusing on advanced research and development at the intersection of Information and Communication Technologies (ICTs), human rights, and global security." (The Citizen Lab)
- *Map:* "Cyber-Censorship Map" (Alkasir)
- *Dashboard:* "At-A-Glance Web-Blockage Dashboard" (Herdict)
- *List:* "Who publishes Transparency Reports?" (James Losey)
- *Overviews:* "Cyberwellness Profiles" (ITU)

What general cyber-security threats is the organization facing?

- *Report:* "The Internet Annual Security Threat Report" (Symantec)

- *Report:* "Annual threat report" (Mandiant)
- *Reports:* "APWG Phishing Attack Trends Reports" (Anti-Phishing Working Group)
- *Reports:* "Secunia Country Reports" (Secunia)
- *Reports:* "McAfee Threat Trends Papers" (McAfee)
- *Report:* "Monthly intelligence report" (Symantec)

What level of technology is available in the region?

- *Database:* "World Telecommunication/ICT Indicators database 2014" (WT-ICT)
- *Comparisons:* "Country Comparisons" (CIA fact-book)

ACTIVITIES

CONDUCT INTERVIEWS

NOTE: Covered in full under Capacity Assessment

- Set up secure channels for communication
- Interview managerial staff
- Interview technical staff
- Use the Categories (at the end of the sample interview questions) to help scope which questions to ask
- Use the Capacity Assessment Cheat-Sheet to track topics you have covered

REGIONAL CONTEXT RESEARCH

Summary

This exercise focuses on research and re-confirmation of regional issues from general trends to specific legal restrictions and safety concerns, as well as current news and persistent challenges.

Overview

- Identify any legal risks associated with conducting the audit (Secure communications and storage, network forensics, device exploitation, digital security training.) [33]
- Determine the sensitivity of the type of work the organization conducts and if its work attracts additional potential threat actors.
- Identify potential adversaries not identified in interviews including domestic or international governments and other, non-state actors (organized crime, corporations, competition, etc).
- Identify capacity and willingness of potential adversaries to act against the organization.
- Has any organization or individual made specific threats, or demonstrated intention or mindset to attack on the organization or similar organizations?

Materials Needed

Considerations

- Use VPNs or Tor to search if conducting the search from a country that is highly competitive with the organization's country, or is known to surveil.

- Maintain data about any targeted attacks and attacks affecting the organization's line of work secure.

Walkthrough

Cross-check reports on regional threats facing organizations with their focus area.

- Targeted Threats
  - List all the relevant actors and their relationship with similar organizations.
  - List all present threats and upcoming threats to similar organizations.
  - List all documented instances of relevant actors carrying out these threats.
- Decentralized Threats
  - List all present threats and upcoming threats to similar organizations.
  - Identify the motivation for these threats.
  - List all documented instances of these threats being carried out.

Identify any legal risks associated with conducting the audit. Secure communications and storage, network forensics, device exploitation, digital security training.

- Identify any export/import controls that might put the auditor or the organization at risk.
- Identify any domestic laws and regulations that might put the auditor or the organization at risk.

Identify any infrastructural barriers to adopting digital security practices.

Explore the security landscape of hardware and software identified in interviews by conducting a basic vulnerability analysis.

TECHNICAL CONTEXT RESEARCH

Summary

This exercise focuses on research into the technical capacity of potential threat actors, including both historical attack data and any indicators of changes to their capacity. Auditors are encouraged to create a summary of their findings for inclusion in the audit report and for sharing (if operational security and the agreement with the organization permits) among trusted networks.

Overview

- Explore latest cyber security trends, focusing on the security landscape of organizational hardware and software identified in interviews. [34]
- Identify access to and ownership/centralized control of communications infrastructure.
- Identify and prepare for any infrastructural barriers
- Research known uses of surveillance, censorship, or malware in the country/region and/or affecting the organization's line of work
- Identify known technical threats and Advanced Persistent Threats impacting the region or type of work the organization conducts.
- Investigate current non-targeted digital threats affecting the region and/or type of organization.
- Investigate the top targeted digital threats facing organizations doing this work in this region / country.
- Identify any legal barriers associated with common audit recommendations (Secure communications and storage, network forensics, device exploitation, digital security training.) [35]

Materials Needed

Considerations

- Use VPNs or Tor to search if conducting the search from a country that is highly competitive with the organization's country, or is known to surveil.
- The regional or country focus of the report may reveal information about the acitivites of an auditor. If the report is to be shared, consider sharing in bulk or a significant time after any travel has been completed.
- If the report is to be shared, ensure your audit agreement with the organization covers and restrictions for sharing.

Walkthrough

Thoroughly research technical attack history for the country/region, with a focus on identifying attacks which may focus on the work of the organization. Auditors are advised to track both capability (known attacks and tools) and intent (attempts to aquire tools, changes in policies, public statements). For auditors who intend to share their research efforts, it is incredibly useful to include key quotes and data directly into relevant sections of this document, providing a reference or link back to the original report. This allows future reviewers to more immediately understand your assessment, what it has included and not, and incorporate new material.

It is useful to categorize the research into categories:

- **Surveillance** (Surveillance Technology, Encryption Regulation, Identity Tracking, Requests for User Information)
- **Targeted Attacks** (Targeting Ability, Technical Sophistication)
- **Censorship and Connectivity** (Network Ownership, Shutdowns, Targeted Censorship, Blocking apps, Blocking Circumvention)
- **Seizure and Theft** (Device Confiscation, Targeted Raids, Robbery/Theft)

Keep a separate running list for: * **Targeted Populations** (Are specific types of people targeted/surveilled due to their identity/race/background?) * **Targeted Activities** (Are specific activities abnormally targeted - e.g. protests, calls for government transparency, etc.?) * **Sensitive Events** (Are there specific historic/anniversary/holiday dates, upcoming elections (https://www.ndi.org/elections-calendar), or other known events to be noted?) * **Sources and New Additions** (What resources have you found, ?)

If the country(ies) of interest are in the Freedom on the Net report, you will be able to gather a great deal of baseline information across all the sections by reading through the relevant country reports. The key internet controls found in the Freedom on the Net report (https://freedomhouse.org/report/key-internet-controls-table-2016) guided many of the categories used here, reducing the effort required to create a baseline report. More advanced reporting could include references to the CAPEC (Common Attack Pattern Enumeration and Classification) taxonomy, and auditors may also be interested in leveraging the STIX standard to better automate sharing and further research into specific threats using threat information sharing platforms.

Additional organizations which regularly release in-depth digital security focused country reports which are strongly recommended to review in creation of an assessment are listed below. These sources often link to their primary sources or other groups doing dedicated research on the country or topic for further research. In addition, sub-sections list topic-specific research ideas.

- Digital attacks and threat information affecting NGOs and media
- Freedom on the Net Report (Country Reports)
- Human Rights Watch
- Reporters Without Borders (http://12mars.rsf.org/2014-enand http://en.rsf.org/%5BFULL-COUNTRY-NAME%5D.html)
- Privacy International (site:https://www.privacyinternational.org/ "[COUNTRY]" filetype:pdf)
- Citizen Lab (site:https://www.privacyinternational.org/ "[COUNTRY]")
- Amnesty International site:http://www.amnestyusa.org/research/reports/ [TERM] [COUNTRY]

- Information Security and Cyber Threats sections of OSAC assessments https://www.osac.gov/Pages/ContentReports.aspx?cid=3

- Industry-wide news and data

- OODALoop: site:https://www.oodaloop.com [COUNTRY]
- Akami (Security) State of the Internet Report https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp

- Internet World Stats - Country Internet and Telecom Reports

Below are definitions and resources for the research categories which can help build out a country or regional assessment useful for the auditor, the organization, and for the broader organizational security community.

- **Surveillance**
- *Surveillance Technology*
  - **Definition and Guiding Questions**: Telecommunications network monitoring or surveillance technology in use. To what extent are providers of access to digital technologies required to aid the government in monitoring the communications of their users?
  - **Useful Data Sources**: https://sii.transparencytoolkit.org , Google Searches of Privacy international: site:https://www.privacyinternational.org/ "[COUNTRY]" filetype:pdf, Google Searches of Citizen Lab: site:https://citizenlab.org/ [TERM] [COUNTRY], Information Security and Cyber Threats sections of OSAC assessments
- *Encryption Regulation*
  - **Definition and Guiding Questions**: Encryption and/or secure communications and anonymity is limited or banned via regulation. Are users prohibited from using encryption software to protect their communications? Are there laws restricting the use of encryption and other security tools, or requiring that the government be given access to encryption keys and algorithms?
  - **Useful Data Sources**: https://www.gp-digital.org/national-encryption-laws-and-policies/, http://www.cryptolaw.org https://github.com/digitalfreedom, http://www.nationaldefensemagazine.org/archive/2013/August/pages/UseCautionWhenTravelingWithEncryptio http://www.infolawgroup.com/ , https://mlat.info/ , http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx
- *Identity Tracking*
  - **Definition and Guiding Questions**: There are regulations requiring some form of identification tracking on telecommunication technology or online platforms, such as for purchase of a SIM card. Are users able to post comments online or purchase mobile phones anonymously or does the government require that they use their real names or register with the government? Are website owners, bloggers, or users in general required to register with the government?
  - **Useful Data Sources**: https://www.gp-digital.org/national-encryption-laws-and-policies/, http://www.cryptolaw.org https://github.com/digitalfreedom, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx
- *Requests for User Information*
  - **Definition and Guiding Questions**: The government requests user data from internet intermediaries like ISP's, social media, and online services.
  - **Useful Data Sources**: Recent transparency reports from top and/or locally relevant service providers; see the following for listings: https://www.accessnow.org/transparency-reporting-index/ , http://thememoryhole2.org/blog/transparency-reports , http://jameslosey.com/post/114045240881/who-publishes-transparency-reports-a-list-of-the
- **Targeted Attacks**
- *Targeting Ability*
  - **Definition and Guiding Questions**: Host nation has in-house or commercially sourced capability to leverage the information from social media monitoring, arrests, or existing targeted attacks in conducting additional attacks such as phishing, pharming, or spear-phishing.
  - **Useful Data Sources**: Google Searches of Citizen Lab: site: https://citizenlab.org/ [TERM] [COUNTRY], https://targetedthreats.net/media/2-Extended%20Analysis-Full.pdf#page=23 , http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Country_Profiles.aspx , http://www.kroll.com/en-us/intelligence-center/reports/global-fraud-report,Symantechttps://www.symantec.com/security-center/threat-report , https://www.symantec.com/security_response/publications/monthlythreatreport.jsp , https://www.symantec.com/connect/blogs
- *Technical Sophistication*
  - **Definition and Guiding Questions**: Host nation has in-house or commercially sourced capability to maintain persistent access to targets over time and across platforms.
  - **Useful Data Sources**: https://sii.transparencytoolkit.org/ , APT Groups and Operations sheet (includes targets): https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=

, Google Searches of Citizen Lab: site:https://citizenlab.org/ [TERM] [COUNTRY],

- **Censorship and Connectivity**
- *Connectivity and Network Ownership*
  - **Definition and Guiding Questions**: Extent to which telecommunications networks and internet service providers are state owned or operated.
  - **Useful Data Sources**: https://freedomhouse.org/report-types/freedom-net , http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx , ASNs: https://ipinfo.io/countries , DYN Research Reports site:http://research.dyn.com [COUNTRY], Akami State of the Internet Report https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/index.jsp , ITU Statistics http://www.itu.int/en/ITU-D/Statistics/Pages/default.aspx , Internet World Stats http://www.internetworldstats.com/
- *Internet Shutdowns*
  - **Definition and Guiding Questions**: The host nation is willing and able to obstruct access to the global Internet or mobile networks either in a specific region or nationwide
  - **Useful Data Sources**: https://www.accessnow.org/keepiton
- *Targeted Censorship*
  - **Definition and Guiding Questions**: Host nation is willing and able to use targeted censorship approaches (including DDoS) against specific websites. To what extent does the state employ legal, administrative, or other means to force deletion of particular content, including requiring private access providers to do so? To what extent does the state or other actors block or filter specific internet and other ICT content, particularly on political and social issues e.g. distributed denial of service attacks (DDoS) attacks, content removal requests, and legal take-downs
  - **Useful Resources:** https://explorer.ooni.torproject.org/world/ , https://www.herdict.org/explore/indepth , https://www.qurium.org/alerts/ , https://equalit.ie/category/deflect-labs/ , DYN Research Reports site:http://research.dyn.com [COUNTRY], Internet Monitor https://cyber.law.harvard.edu/research/internetmonitor
- *Blocking Communications Apps and Platforms*
  - **Definition and Guiding Questions**: Entire platforms temporarily or permanently blocked to prevent communication and information sharing.
  - **Useful Data Sources**: https://explorer.ooni.torproject.org/world/, Herdict, GreatFire (for China)
- *Blocking Circumvention*
  - **Definition and Guiding Questions**: Host nation is willing and able to disable the use of circumvention or secure communications technology.
  - **Useful Data Sources**: https://explorer.ooni.torproject.org/world/
- **Seizure and Theft**
- *Device Confiscation*
  - **Definition and Guiding Questions**: Likelihood of confiscation of user devices when interacting with security forces. E.g. When crossing borders, at internal checkpoints, or during detainment or arrest. See themes for "targeted individuals"
  - **Useful Data Sources**: See physical-security risk register and for information around border crossings.
- *Targeted Raids*
  - **Definition and Guiding Questions**: Likelihood of office raid and seizure of equipment by host nation. See project information for modifiers around "unwelcome themes," “environmental factors,” and “office being built / existing” as well as physical security risk register for risk of sanctioned office raids.
  - **Useful Data Sources**:
- *Robbery/Theft*
  - **Definition and Guiding Questions**: Likelihood of (non-host nation) theft of user or office devices
  - **Useful Data Sources**: OSAC reports https://www.osac.gov/Pages/ContentReports.aspx?cid=2 , Pinkerton Risk Index https://www.pinkerton.com/risk-index/ ,

CAPACITY ASSESSMENT

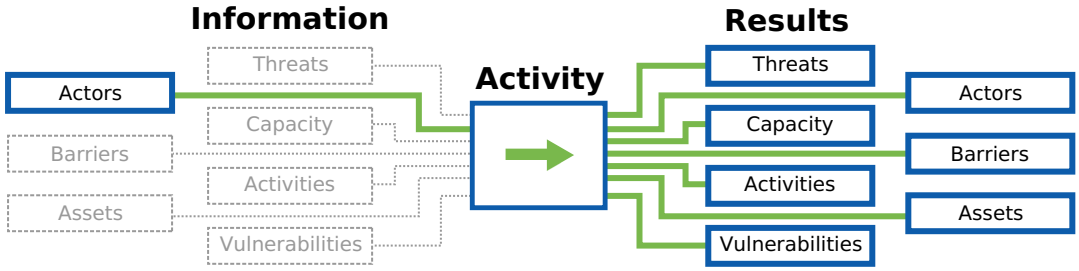
SUMMARY

In this component the auditor engages with staff through interviews and conversations 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 allows 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. This information also provides a starting place for understanding the organization's current use and understanding of technology, digital security, and current threat landscape, as well as revealing elements of an organization's workflow, infrastructure and even vulnerabilities that you might otherwise have overlooked.

THE FLOW OF INFORMATION



Audit Preparation Information Flow

GUIDING QUESTIONS

- What is the organization's ability to adopt new technologies or practices?
- What resources does the organization have available to them?
- What is the environment that the organization works within like? What barriers, threat actors, and other aspects influence their work?
- Are there any specific considerations for the audit that would require modifying the overall approach, tools, preparation steps, or timeline?

APPROACHES

- Conduct pre-audit interviews with key managerial and technical staff to identify organizational areas of strength and weakness (expertise, finance, staff time, etc.).
- Have informal conversations with staff during the course of the audit to further gather capacity and historical "stories" of technology adoption.
- Generate easy to follow capacity self-assessment checklist, which can be continuously used and modified by the organisation over time.

OUTPUTS

- Organization's ability to:
  - Adopt new technology
  - Learn from others
- Organization's resources (financial, time, buy-in, expertise...) available for technological adoption
- The availability and quality of communications and electronic infrastructure.
- Threats posed to the digital and physical security of the organization and its staff, and past security issues encountered by the organization and its partners.

- Priority security concerns.
- 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.

OPERATIONAL SECURITY

PREPARATION

- Review or create a set of interview questions to keep you on track
- Have a secure note-taking process ready

RESOURCES

- *Questionnaire:* Context Analysis Questionnaire - pg. 76 - Workbook on Security (Front Line Defenders)
- *Guide:* Assessing Context, Priorities and Learning Styles (Integrated Security)

Background Interview Approaches

- *Project:* Tech Scape (the engine room)
- *Guide:* Individual Depth Interviews: Design Research for media development (Internews)
- *Guide:* Develop an Interview approach - pg. 58 - HCD Toolkit (IDEO)
- *Guide:* Interview Guide - pg. 57 - Development Impact & You (IDEO.org)
- *Guide:* Conducting key informant Interviews - 1996, Number 2 (USAD Center for Development Information and Evaluation)
- *Questionnaire:* Context Analysis Questionnaire - pg. 76 - Workbook on Security (Front Line Defenders)
- *Guide:* Assessing Context, Priorities and Learning Styles (Integrated Security)

ACTIVITIES

INTERVIEWS

Summary

The auditor conducts interviews with various staff members to gather information on the organizations risks and capacity.

Q&A sessions are unabashedly *white box* aspects of a security assessment, and you will occasionally hear push-back along the lines of, "You wouldn't have found that thing if we hadn't told you about this other thing." Compelling *black box* findings certainly do have an advantage when it comes to persuasiveness, but obtaining them can be quite time-consuming, so relying exclusively on vulnerabilities that you can identify without "help" is generally a mistake in this resource-constrained sector.

Overview

- Set up secure channels for communication
- Interview managerial staff
- Interview technical staff
- Use the Categories (at the end of the sample interview questions) to help scope which questions to ask
- Use the Capacity Assessment Cheat-Sheet to track topics you have covered

Materials Needed

Considerations

- If the auditor or organization believes that there is a good chance of surveillance on the channel you are communicating over, do the rest of the interview on a secured channel or in person where possible, though some information-gathering is critical to do before planning the audit. Inability to do so contributes towards a no-go situation.

Walkthrough

See the Appendix for a sample set of interview questions

CAPACITY ASSESSMENT CHECKLIST

Summary

A monolithic, one-time interview with key staff is not always possible or advisable, but interacting with a variety of staff exposes valuable information about every aspect of the audit, from vulnerabilities to capacity to hidden barriers. This serves as a "cheat sheet" of some topics to explore both during the planning and preparation phase and throughout the audit process.

Walkthrough

"Homework"

- Basic contact and organizational information: name, org, org's stated mission
- Contextual research

Organizational

- Size of staff
- Key roles in org for tech and management
- Structure: Management and Technical?
- (Program size, activities, information)
- (Change management)
- Languages used in office

Contextual / Background / Threat information

- What (if any) threats have occured to the organization and its partners? (digital, physical)
- Surveillance?
- What other threats are you concerned about? What has happened to other organizations in the space?
- Org responses to these threats - trainings, technical responses, organization process/change successes?
- Specific programs or other work outside of publicly stated mission that are high-risk
- Program use of technology (SMS surveys, blogs, facebook pages, other websites, media recording and broadcast

...?)

Technical:

- Primary website:
- Additional websites:
- Website technologies (content management, hosting provider)
- Technology in use:
- Desktop software (OS, Office)
- Desktop security tools (anti-virus, anti-malware, firewalls, vpns, disk encryption...)
- Servers (email, shared file system, networking tools, backups)
- Email, email hosts
- Other communication tools - skype, facebook, chat, mobile...
- Other less formal tools - external emails, dropbox...
- Internal network - wired, wireless, type of wireless network, ISP

Preparation Support

- Infrastructure
- How is the office connected to the Internet?
- Power outages or other challenges?
- Office setup and size
- Shared office space, shared floor or building?
- Physical security of the office?

RECONNAISSANCE

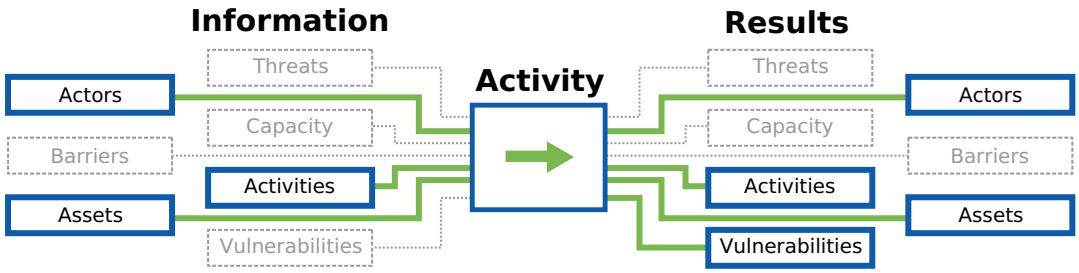
SUMMARY

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") This 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.

PURPOSE

While much of SAFETAG focuses on digital security challenges within and around the office, unintended information available from "open sources" can pose real threats and deserve significant attention. This also builds the Auditor's understanding of the organization's digital presence and will guide specific vulnerabilities to investigate once on site.

THE FLOW OF INFORMATION



Reconnaissance Information Flow

GUIDING QUESTIONS

- Depending on the organization's security needs, does it "leak" any sensitive information online (location, staff identities, program locations?)
- Can you identify partners or beneficiaries through the organizations sites?
- What is the pattern for staff e-mail addresses?
- Have any of the the organization's servers, users, or e-mail accounts been compromised in the past?

APPROACHES

- **Manual OSINT:** Identify availability of partner, beneficiary, and current project information online using advanced Google searching and website-scraping. [36]
- **Recon-NG:** Use recon-ng to do automated web-based open source reconnaissance. [37]
- **Social Network OSINT:** Identify availability of staff partner, beneficiary, and current project information by searching social networks for information leaked about the organization.

OUTPUTS

- 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.

OPERATIONAL SECURITY

- While this does not focus on identifying of vulnerabilities, it may nonetheless expose certain threats, particularly with

regard to publicly-accessible information that is presumed to be confidential, such as the identity of sensitive staff, the existence of sensitive partner- and funder-relationships, or the organization's history of participation in sensitive events or travel to sensitive locations.

PREPARATION

RESOURCES

Open Source Intelligence (General)

- *Standard:* Intelligence Gathering (The Penetration Testing Execution Standard)
- *Guide:* "Passive Reconnaissance" (Security Sift)
- *Tool:* "NameChk account search" (NameChk)
- *List:* "Open Source Intelligence Links" (Intel Techniques)
- *List:* "OSINT Tools - Recommendations List Free OSINT Tools." (subliminalhacking.net)
- *Guide:* "OWASP Testing Guide v4 - Information Gathering" (OWASP)

Organizational Information Gathering

- *Database:* "find the email address formats in use at thousands of companies." (Email Format)

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)

Pastebin Searching

- *Article:* "Using Pastebin Sites for Pen Testing Reconnaissance" (Lenny Zeltser)
- *Custom Search* "This custom search page indexes 80 Paste Sites:" (Intel Techniques)
- *Article* "Pastebin: How a popular code-sharing site became the ultimate hacker hangout" (Matt Brian)
- *Advanced Search* "Github Advanced Search" (Github)

Recon-ng

- *Site:* "Recon-ng: Website" (Bitbu * *Guide:* [The Recon-ng Frameworkcket)
- *Type:* "Recon-ng: Usage Guide" (Bitbucket)

- *Demonstration:* "Look Ma, No Exploits! – The Recon-ng Framework - Tim "LaNMaSteR53" Tomes" (Derbycon 2013)
- *Guide:* toolsmith guide to Recon-ng
- *Video:* Tektip ep26 - Information gathering with Recon-ng Video Tutorial
- *Guide:* The Recon-ng Framework : Automated Information Gathering
- *Guide:* The Recon-ng Framework : Updated modules
- *Blog:* Professionally Evil Toolkit - Recon-ng

ACTIVITIES

MANUAL RECONNAISSANCE

Summary

This exercise suggests some targeted online search tools and tricks to gather information leakages from organizations. While many advocacy, activism, and media/journalism focused organizations are very public as part of their operations, the searches suggested here aim to explore data that could be used to better attack or socially engineer an organization.

Overview

- Use advanced search tools of major search engines to discover partners, projects, and other valuable information about the organization.
- Social Media / Account Discovery
- Search pastebin and github style sites for breach and website/software development records
- Use reverse image searching and exif tools on photos of interest
- Use to add additional data in to, and to research further discoveries from, the automated recon work

Materials Needed

Considerations

- Use VPNs or Tor to conduct your searching. Tor may be blocked by some services.
- Some searches may reveal personal information. Be empathetic and responsible with this, even though it is "public" information.

Walkthrough

These custom and more manual approaches work excellently in combination with automated tools such as recon-ng or the commercial Maltego. Working with both these tricks and the automated tools, feeding information learned from one back to the other, is a powerful way to unearth large amounts of information about an organization.

Much of the tools and further guidance is well covered in the references for the Reconnaissance method, a small selection of starting points is mapped out below.

Take care, however, to not waste time on this; using image information tools on every photo on an organization's website, or researching every linked social media account may not provide further valuable information - step back and judge the value of digging deeper - are you finding adversaries? Are you finding information that the organization may not want

online? Are there other methods which might be more appropriate to apply?

Search Engines

Google dorking tricks:

- limit to the target webiste using site: and look for potentially accidentally uploaded file types (e.g. xlsx, you can reference this full list of searchable filetypes)
- inurl:
- search for link: to discover partners and projects (add "project of" and similar), removing known, un-interesting and irrelevant sites with -site:
- Browse Exploit-db for interesting and advanced combinations to consider, e.g. inurl:/wp-en/wpbackitup_backups

Social Media / Account Discovery

- Use tools such as KnowEm, namechk, or namechecklist to find similar or organizationally-linked usernames across other social media accounts.

Additional Tools

- GlassDoor can provide insight (mostly for larger organizations) on whether there might be disgruntled former (or current) employees.

Pastebin Searching

- Search pastebin for keywords about the organization (usually their website address) -- this custom google search by IntelTechniques searches across over 100 pastebin-like sites, including github, at once.

Working with Images

- Use tools like tineye and Google Reverse Image search to find images (especially user icons from twitter, etc.) on other sites, and test interesting ones for additional image in the EXIF data using online tools like Exif Viewer or commandline tools like exiftool.

Recommendation

AUTOMATED RECONNAISANCE

Summary

This component allows the auditor to quickly 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.

Overview

- Passive Reconnaissance
  - Identify availability of staff, partner, beneficiary, and current project information online. [38]
  - Search "paste-bin" sites for leaked internal information or existing exploitation of their infrastructure.
  - Create API keys for Recon-ng services to be used. [39]
  - Use recon-ng to do automated web-based open source reconnaissance. [40]

Materials Needed

Considerations

- Use VPNs to do automated searching. The automated process can be misconstrued by various services as malicious and cause your local network to get blocked, filtered, or surveilled. Tor is often blocked by the tools you will be using.

Walkthrough

Both Recon-ng and Foca are open source reconnaissance tools with many available plugins. Foca is, out-of-the-box, more aimed at extracting metadata from documents and images, whereas Recon is slightly more focused on finding digging into domains, subdomains, contacts, and the more network-level information. Both tools are best used in addition to critical thinking and manual exploration, and require "seed" inputs to get started and careful curation to remove false leads.

Recon-ng

Installing Recon-ng

- Install recon-ng from the git source: git clone https://LaNMaSteR53@bitbucket.org/LaNMaSteR53/recon-ng.git
- cd recon-ng
- Install pip (sudo apt-get install python-pip) and dependencies: pip install -r REQUIREMENTS
- Launch Recon-ng: ./recon-ng

For full instructions, see the Recon-ng Getting Started Instructions

Using Recon-ng

- Read the short Recon-ng Usage Guide

NOTE: This guide is based upon the data flow documentation from the Recon-ng website

- Interface Basics

By pressing tab twice you can use auto-completion.

```
[recon-ng][default] >
add       exit      load      record    search    show      use
back      help      pdb       reload    set       spool     workspaces
del       keys      query     resource  shell     unset
```

This works even in commands.

```
[recon-ng][default] > show
banner        credentials   hosts         locations     options       schema
companies     dashboard     keys          modules       ports         vulnerabilities
contacts      domains       leaks         netblocks     pushpins      workspaces
```

Using recon modules

The recon modules are named in a very specific fashion to help the user understand the flow of data inside the tool. Modules use the syntax <methodology step>/<input table>-<output table>/<module>. The inputs are the first part of each module, and the outputs are the second part. The module name itself is the tool used to process the data. So, recon/domains-hosts/brute-hosts takes domain names (websitename.org) as an input, and outputs hostnames (extranet.websitename.org, etc.). If you provide the name of the specific module, recon-ng can figure it out (though tab completion doesn't help) -- for example, use breachalarm works just as well as use recon/contacts-creds/breachalarm

You can also search modules by their inputs or outputs. search domains- displays all modules that take domain names as their input, and search -contacts displays all modules that outputs contact information.

Preparing

Set verboseness on during the guide so that you can see everything that happens. (recommended to begin with)

```
[recon-ng][default] > set VERBOSE True
```

- Add API Keys

You can use auto completion to see all the possible keys you can add.

```
[recon-ng][websitename] > keys add
bing_api          facebook_secret    google_cse        jigsaw_username    pwnedlist_iv      twitter_api
builtwith_api     facebook_username  ipinfodb_api      linkedin_api       pwnedlist_secret  twitter_secret
facebook_api      flickr_api         jigsaw_api        linkedin_secret    shodan_api        virustotal_api
facebook_password google_api         jigsaw_password   pwnedlist_api      sonar_api
```

Choose and add a key.

```
[recon-ng][default] > keys add bing_api TYPE_THE_KEY_VALUE_HERE
[*] Key 'bing_api' added.
```

You can list keys by using the command keys list Reference the Creating API Keys Section below for quick links to setting up popular APIs.

First steps

NOTE: This walkthrough is using sample data. Results will vary widely depending on the organization you are working with.

- Create a workspace for your recon.

```
[recon-ng][default] > workspaces add websitename
[recon-ng][websitename] >
```

- Note that you can also switch workspaces during the recon.

```
[recon-ng][websitename] > workspaces select default
[recon-ng][default] >
[recon-ng][default] > workspaces select websitename
[recon-ng][websitename] >
```

- Add known seed information (domains, netblocks, company names, locations, etc.)

Display possible seed information by using auto-completion.

```
[recon-ng][default] > add
companies      credentials    hosts          locations      ports          vulnerabilities
```

```
contacts        domains         leaks           netblocks       pushpins
```

We will only use the organization's name, one domain, two netblocks (that we got by searching for other domains and ping-ing them), and two e-mails of the company we are looking for so we will add those.

First, add the company name.

```
[recon-ng][websitename] > add companies
company (TEXT): Websitename
description (TEXT):
```

Next, add the domain.

```
[recon-ng][default] > add domains websitename.org
[recon-ng][websitename] > show domains

 +---------------------------------+
 | rowid |     domain    | module |
 +---------------------------------+
 | 1     | websitename.org | base   |
 +---------------------------------+

[*] 1 rows returned
```

Next, add my contacts. we don't know much. But, we will add what we know.

```
[recon-ng][websitename] > add contacts
first_name (TEXT): Bob
middle_name (TEXT):
last_name (TEXT): Smith
email (TEXT): bsmith@websitename.org
title (TEXT):
region (TEXT):
country (TEXT): USA
[recon-ng][websitename] > add contacts
first_name (TEXT): Carl
middle_name (TEXT):
last_name (TEXT): Johnson
email (TEXT): cjohnson@websitename.org
title (TEXT):
region (TEXT):
country (TEXT): USA
[recon-ng][websitename] >
```

Finally we will add the ip address of their website.

```
[recon-ng][websitename] > add netblocks
netblock (TEXT): 174.154.167.69
[recon-ng][websitename] > add netblocks
netblock (TEXT): 96.127.170.121
```

Here it is in the database.

```
[recon-ng][websitename][shodan_net] > show netblocks

 +---------------------------------+
 | rowid |    netblock    | module |
 +---------------------------------+
 | 2     | 174.154.167.69 | base   |
 | 3     | 96.127.170.121 | base   |
```

```
+----------------------------------+
```

Reconnaisance phase (netblocks example)

- Run modules that leverage known netblocks. This exposes other domains and hosts from which domains can be harvested.

First, search for any modules that use netblocks as an input.

```
recon-ng][websitename] > search netblocks-
[*] Searching for 'netblocks-'...

 Recon
 -----
   recon/netblocks-hosts/reverse_resolve
   recon/netblocks-hosts/shodan_net
   recon/netblocks-ports/census_2012
```

In the case of `recon/netblocks-hosts/shodan_net` we can see that the "shodan_net" module is a reconnaissance module that takes in netblocks and produces hosts.

Lets try it out...

```
[recon-ng][websitename] > use recon/netblocks-hosts/shodan_net
[recon-ng][websitename][shodan_net] >
```

An empty command line can be daunting. If you are ever stuck on what current commands you can use the help command to see the current commands.

```
[recon-ng][websitename][shodan_net] > help

Commands (type [help|?] <topic>):

add           Adds records to the database
back          Exits the current context
del           Deletes records from the database
exit          Exits the framework
help          Displays this menu
keys          Manages framework API keys
load          Loads selected module
pdb           Starts a Python Debugger session
query         Queries the database
record        Records commands to a resource file
resource      Executes commands from a resource file
run           Runs the module
search        Searches available modules
set           Sets module options
shell         Executes shell commands
show          Shows various framework items
spool         Spools output to a file
unset         Unsets module options
use           Loads selected module
```

Use the `show info` command to learn about the module and see what options are available.

```
[recon-ng][websitename][shodan_net] > show info

    Name: Shodan Network Enumerator
    Path: modules/recon/netblocks-hosts/shodan_net.py
  Author: Mike Siegel and Tim Tomes (@LaNMaSteR53)
```

```
Description:
  Harvests hosts from the Shodanhq.com API by using the 'net' search operator. Updates the 'hosts'
  table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  LIMIT   1              yes       limit number of api requests per input source (0 = unlimited)
  SOURCE  default        yes       source of input (see 'show info' for details)

Source Options:
  default        SELECT DISTINCT netblock FROM netblocks WHERE netblock IS NOT NULL ORDER BY netblock
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][websitename][shodan_net] >
```

It pulls directly from the netblocks source that we set up. Now, use `run` to run the module .

```
[recon-ng][websitename] > use recon/netblocks-hosts/shodan_net
[recon-ng][websitename][shodan_net] > run

174.154.167.69
[*] Searching Shodan API for: net:174.154.167.69
[*] 174.154.167.69 (vps.websitename.org) - 7706
[*] 174.154.167.69 (vps.websitename.org) - 110
[*] 174.154.167.69 (vps.websitename.org) - 57
[*] 174.154.167.69 (vps.websitename.org) - 22
[*] 174.154.167.69 (vps.websitename.org) - 147
[*] 174.154.167.69 (vps.websitename.org) - 997
[*] 174.154.167.69 (vps.websitename.org) - 70
[*] 174.154.167.69 (vps.websitename.org) - 25

96.127.170.121
[*] Searching Shodan API for: net:96.127.170.121
[*] 96.127.170.121 (vps.websitename.org) - 7706
[*] 96.127.170.121 (vps.websitename.org) - 22
[*] 96.127.170.121 (vps.websitename.org) - 465
[*] 96.127.170.121 (vps.websitename.org) - 997
[*] 96.127.170.121 (vps.websitename.org) - 25
[*] 96.127.170.121 (vps.websitename.org) - 995
[*] 96.127.170.121 (vps.websitename.org) - 57
[*] 96.127.170.121 (vps.websitename.org) - 147
[*] 96.127.170.121 (vps.websitename.org) - 110
[*] 96.127.170.121 (vps.leillc.net) - 7070

SUMMARY
[*] 17 total (2 new) items found.
```

Since it promised me hosts, we will see what hosts it uncovered.

```
[recon-ng][websitename][shodan_net] > show hosts

  +-----------------------------------------------------------------------------------------------+
  | rowid |       host       |   ip_address   | region | country | latitude | longitude |   module   |
  +-----------------------------------------------------------------------------------------------+
  | 1     | vps.websitename.org | 174.154.167.69 |        |         |          |           | shodan_net |
  | 2     | vps.websitename.org | 96.127.170.121 |        |         |          |           | shodan_net |
  | 3     | vps.leillc.net    | 96.127.170.121 |        |         |          |           | shodan_net |
```

```
+----------------------------------------------------------------------------------------------+

[*] 3 rows returned
```

It seems the website leillc.net is obviously not associated with the company I am doing recon on. Since this module has finished, we will leave it using the back command.

```
[recon-ng][websitename][shodan_net] > back
[recon-ng][websitename] >
```

Now we will use the other two netblock- modules. We will show one more and then skip the second.

First we find all the possible modules using tab completion.

```
[recon-ng][websitename] > use recon/netblocks-
recon/netblocks-hosts/reverse_resolve  recon/netblocks-hosts/shodan_net       recon/netblocks-ports/census_2012
[recon-ng][websitename] > use recon/netblocks-
```

We are going to use reverse-resolve.

```
[recon-ng][websitename][census_2012] > use recon/netblocks-hosts/reverse_resolve
```

But, when we run it we get an error!

```
[recon-ng][websitename][reverse_resolve] > run
174.154.167.69
[!] Need more than 1 value to unpack.
```

OPTIONAL: To figure out what was going on, go back and then set DEBUG True to see the underlying error. The debug error message lets us know that we need to use full netmask syntax for netblocks. We will now add new netblocks in the correct format and then delete the old ones.

First we will add them correctly.

```
[recon-ng][websitename][reverse_resolve] > add netblocks
netblock (TEXT): 177.154.167.69/72
[recon-ng][websitename][reverse_resolve] > add netblocks
netblock (TEXT): 96.127.170.121/72
```

Now we have double of the same netblocks

```
[recon-ng][websitename][reverse_resolve] > show netblocks

+-------------------------------------------+
| rowid |     netblock     |     module     |
+-------------------------------------------+
| 2     | 174.154.167.69    | base           |
| 4     | 177.154.167.69/72 | reverse_resolve |
| 3     | 96.127.170.121    | base           |
| 5     | 96.127.170.121/72 | reverse_resolve |
+-------------------------------------------+

[*] 4 rows returned
```

Now that we know their rowid numbers, I can delete them.

```
[recon-ng][websitename][reverse_resolve] > del netblocks
rowid(s) (INT): 2
[recon-ng][websitename][reverse_resolve] > del netblocks
rowid(s) (INT): 3
```

And, re-running the module now works.

```
[recon-ng][websitename][reverse_resolve] > run

[*] 177.154.167.69 => dsl-177-154-167-69-dyn.prod-infinitum.com.mx
[*] 96.127.170.121 => vps.websitename.org

SUMMARY

[*] 2 total (1 new) items found.
```

Now, exploring these hosts we realize quickly that most the new hosts on other domains are not associated with the company. Hence, we will remove them.

```
[recon-ng][websitename] > show hosts

 +-------------------------------------------------------------------------------------------------------------------------------+
 | rowid |                    host                    |   ip_address   | region | country | latitude | longitude |      module     |
 +-------------------------------------------------------------------------------------------------------------------------------+
 | 4     | dsl-177-154-167-69-dyn.prod-infinitum.com.mx | 177.154.167.69 |        |         |          |           | reverse_resolve |
 | 1     | vps.websitename.org                          | 174.154.167.69 |        |         |          |           | shodan_net      |
 | 2     | vps.websitename.org                          | 96.127.170.121 |        |         |          |           | shodan_net      |
 | 7     | vps.pineapplebob.net                         | 96.127.170.121 |        |         |          |           | shodan_net      |
 +-------------------------------------------------------------------------------------------------------------------------------+

[*] 4 rows returned
[recon-ng][websitename] > del hosts
rowid(s) (INT): 4
[recon-ng][websitename] > del hosts
rowid(s) (INT): 7
```

We skip the last module `recon/netblocks-ports/census_2012` since you already get the idea.

- Add new domains gleaned from the results if they have not automatically been added.

Sadly, none of the new domains were actually useful.

- Run modules that conduct DNS brute forcing of TLDs and SLDs against current domains.

Let's find new domains using brute forcing. First we should look for what is available.

```
[recon-ng][websitename] > search domains-domains
[*] Searching for 'domains-domains'...

 Recon
 -----
   recon/domains-domains/brute_suffix
[recon-ng][websitename] > use recon/domains-domains/brute_suffix

[recon-ng][websitename][brute_suffix] > run

-------------
WEBSITENAME.ORG
-------------
[*] websitename.ac => No record found.
[*] websitename.academy => No record found.
[*] websitename.ad => No record found.
[*] websitename.ae => No record found.
[*] websitename.aero => No record found.
[*] websitename.af => (SOA) websitename.af - Host found!
[*] websitename.ag => No record found.
```

```
[*] websitename.ai => No record found.
[*] websitename.al => No record found.
[*] websitename.am => (SOA) websitename.am - Host found!
[*] websitename.an => No record found.
[*] websitename.ao => No record found.
[*] websitename.aq => (SOA) websitename.aq - Host found!
[*] websitename.ar => No record found.
[*] websitename.arpa => No record found.
[*] websitename.as => No record found.
[*] websitename.asia => No record found.
[*] websitename.at => No record found.
[*] websitename.au => No record found.
[*] websitename.aw => (SOA) websitename.aw - Host found!
[*] websitename.ax => No record found.
[*] websitename.az => No record found.
[*] websitename.ba => No record found.
[*] websitename.bb => No record found.
[*] websitename.bd => No record found.
[*] websitename.be => No record found.
[*] websitename.berlin =>  (SOA) websitename.berlin - Host found!
...
```

This returned quite a few domains. We have removed the middle section

```
[recon-ng][websitename][brute_suffix] > show domains

 +-----------------------------------------+
 | rowid |       domain      |    module    |
 +-----------------------------------------+
 | 2     | websitename.af      | brute_suffix |
 | 7     | websitename.am      | brute_suffix |
 | 4     | websitename.asia    | brute_suffix |
 | 5     | websitename.aq      | brute_suffix |
 | 7     | websitename.bg      | brute_suffix |
           ....
           ....
           ....
 | 25    | websitename.net     | brute_suffix |
 | 1     | websitename.org     | base         |
 | 17    | websitename.uz      | brute_suffix |
 +-----------------------------------------+
```

- Have list of domains validated by the client.
- Remove out-of-scope domains with the "del" command or generate a query which only selects the scoped domains as input.

Many out of scope domains had to be removed, but luckily you can specify ranges when you delete.

```
[recon-ng][websitename][brute_suffix] > del domains
rowid(s) (INT): 72-44
```

- Run modules that conduct DNS brute forcing of hosts against all domains.

There are a lot of these, so we will only run one since there is little to nothing new to learn here.

```
[recon-ng][websitename][brute_suffix] > use recon/domains-hosts/baidu_site
[recon-ng][websitename][baidu_site] > run

------------
WEBSITENAME.EU
------------
```

```
[*] URL: http://www.baidu.com/s?pn=0&wd=site%7Awebsitename.eu
[*] www.websitename.eu
[*] Sleeping to avoid lockout...

------------
WEBSITENAME.FR
------------
[*] URL: http://www.baidu.com/s?pn=0&wd=site%7Awebsitename.fr

-------------
WEBSITENAME.ORG
-------------
[*] URL: http://www.baidu.com/s?pn=0&wd=site%7Awebsitename.org
[*] www.websitename.org
[*] things.websitename.org
[*] Sleeping to avoid lockout...

-----------------
WEBSITENAME.ORG.UK
-----------------
[*] URL: http://www.baidu.com/s?pn=0&wd=site%7Awebsitename.org.uk

------------
WEBSITENAME.COM
------------
[*] URL: http://www.baidu.com/s?pn=0&wd=site%7Awebsitename.com
[*] www.websitename.com
[*] Sleeping to avoid lockout...

-------
SUMMARY
-------
[*] 5 total (2 new) items found.

[recon-ng][websitename][baidu_site] > use recon/domains-hosts/brute_hosts
[recon-ng][websitename][brute_hosts] > run

-------------
WEBSITENAME.ORG
-------------
[*] No Wildcard DNS entry found.
[*] 0.websitename.org => No record found.
[*] 01.websitename.org => No record found.
[*] 02.websitename.org => No record found.
[*] 03.websitename.org => No record found.
[*] 1.websitename.org => No record found.
[*] 10.websitename.org => No record found.
[*] 11.websitename.org => No record found.
[*] 12.websitename.org => No record found.
[*] 13.websitename.org => No record found.
[*] 14.websitename.org => No record found.
[*] 15.websitename.org => No record found.
[*] 16.websitename.org => No record found.
[*] 17.websitename.org => No record found.
[*] 18.websitename.org => No record found.
[*] 19.websitename.org => No record found.
[*] 2.websitename.org => No record found.
[*] 20.websitename.org => No record found.
[*] 3.websitename.org => No record found.
[*] 3com.websitename.org => No record found.
[*] 4.websitename.org => No record found.
```

```
[*] 5.websitename.org => No record found.
[*] 6.websitename.org => No record found.
...
...
[*] autodiscover.websitename.org => (CNAME) autodiscover.websitename-mail.org - Host found!
[*] autodiscover.websitename.org => (A) autodiscover.websitename.org - Host found!
[*] autorun.websitename.org => No record found.
[*] av.websitename.org => No record found.
...
...

[recon-ng][websitename] > show hosts

 +-----------------------------------------------------------------------------------------------------------+
 | rowid |              host              |   ip_address   | region | country | latitude | longitude |    module   |
 +-----------------------------------------------------------------------------------------------------------+
 | 8     | autodiscover.websitename-mail.org |              |        |         |          |           | brute_hosts |
 | 9     | autodiscover.websitename.org      |              |        |         |          |           | brute_hosts |
 | 32    | autodiscover.websitename.com      |              |        |         |          |           | brute_hosts |
 | 10    | conference.websitename.org        |              |        |         |          |           | brute_hosts |
 | 12    | beta.websitename.org              |              |        |         |          |           | brute_hosts |
 | 5     | demo.websitename.org              |              |        |         |          |           | baidu_site  |
 | 14    | email.websitename.org             |              |        |         |          |           | brute_hosts |
 | 15    | intranet.websitename.org          |              |        |         |          |           | brute_hosts |
 | 16    | ftp.websitename.org               |              |        |         |          |           | brute_hosts |
 | 37    | ftp.websitename.com               |              |        |         |          |           | brute_hosts |
 | 13    | ftp2.websitename.org              |              |        |         |          |           | brute_hosts |
 | 11    | websitename.github.com            |              |        |         |          |           | brute_hosts |
 | 24    | websitename.org                   |              |        |         |          |           | brute_hosts |
 | 75    | websitename.com                   |              |        |         |          |           | brute_hosts |
 | 18    | localhost.websitename.org         |              |        |         |          |           | brute_hosts |
 | 19    | mail.websitename.org              |              |        |         |          |           | brute_hosts |
 | 36    | mail.websitename.com              |              |        |         |          |           | brute_hosts |
 | 20    | ns1.websitename.org               |              |        |         |          |           | brute_hosts |
 | 27    | temp.websitename.org              |              |        |         |          |           | brute_hosts |
 | 25    | test.websitename.org              |              |        |         |          |           | brute_hosts |
 | 1     | vps.websitename.org               | 174.174.177.77 |      |         |          |           | shodan_net  |
 | 2     | vps.websitename.org               | 77.127.170.121 |      |         |          |           | shodan_net  |
 | 27    | webmail.websitename.com           |              |        |         |          |           | brute_hosts |
 | 4     | www.websitename.org               |              |        |         |          |           | baidu_site  |
 | 7     | www.websitename.com               |              |        |         |          |           | baidu_site  |
 +-----------------------------------------------------------------------------------------------------------+

[*] 77 rows returned
```

- Run host gathering modules.

NOTE: Many host gathering modules use other hosts as a starting place. It is important to sanitize the hosts database between modules to make sure that you do start enumerating based upon incorrectly added hosts.

- Resolve IP addresses.
- Run vhost enumeration modules.
- Run port scan data harvesting modules.
- Use JOIN queries for data analysis.

```
[recon-ng][websitename][census_2012] > query select hosts.ip_address, hosts.host, ports.host, ports.port from hosts join ports using (ip_address)

 +-------------------------------------------------------------------+
 |   ip_address   |          host          |       host       | port |
 +-------------------------------------------------------------------+
 | 174.174.177.77 | vps.websitename.org       | vps.websitename.org | 110  |
 | 174.174.177.77 | vps.websitename.org       | vps.websitename.org | 147  |
```

```
| 174.174.177.77 | vps.websitename.org       | vps.websitename.org | 22   |
| 174.174.177.77 | vps.websitename.org       | vps.websitename.org | 27   |
| 174.174.177.77 | vps.websitename.org       | vps.websitename.org | 7707 |
| 174.174.177.77 | vps.websitename.org       | vps.websitename.org | 77   |
| 174.174.177.77 | vps.websitename.org       | vps.websitename.org | 70   |
| 174.174.177.77 | vps.websitename.org       | vps.websitename.org | 777  |
| 77.127.170.121 | vps.websitename.org       | vps.websitename.org | 110  |
| 77.127.170.121 | vps.websitename.org       | vps.websitename.org | 147  |
| 77.127.170.121 | vps.websitename.org       | vps.websitename.org | 22   |
| 77.127.170.121 | vps.websitename.org       | vps.websitename.org | 27   |
| 77.127.170.121 | vps.websitename.org       | vps.websitename.org | 7707 |
| 77.127.170.121 | vps.websitename.org       | vps.websitename.org | 477  |
| 77.127.170.121 | vps.websitename.org       | vps.websitename.org | 77   |
| 77.127.170.121 | vps.websitename.org       | vps.websitename.org | 777  |
| 77.127.170.121 | vps.websitename.org       | vps.websitename.org | 777  |
| 174.174.177.77 | www.websitename.org       | vps.websitename.org | 110  |
| 174.174.177.77 | www.websitename.org       | vps.websitename.org | 147  |
| 174.174.177.77 | www.websitename.org       | vps.websitename.org | 22   |
| 174.174.177.77 | www.websitename.org       | vps.websitename.org | 27   |
| 174.174.177.77 | www.websitename.org       | vps.websitename.org | 7707 |
| 174.174.177.77 | www.websitename.org       | vps.websitename.org | 77   |
| 174.174.177.77 | www.websitename.org       | vps.websitename.org | 70   |
| 174.174.177.77 | www.websitename.org       | vps.websitename.org | 777  |
| 77.127.170.121 | things.websitename.org | vps.websitename.org | 110  |
| 77.127.170.121 | things.websitename.org | vps.websitename.org | 147  |
| 77.127.170.121 | things.websitename.org | vps.websitename.org | 22   |
| 77.127.170.121 | things.websitename.org | vps.websitename.org | 27   |
| 77.127.170.121 | things.websitename.org | vps.websitename.org | 7707 |
| 77.127.170.121 | things.websitename.org | vps.websitename.org | 477  |
| 77.127.170.121 | things.websitename.org | vps.websitename.org | 77   |
| 77.127.170.121 | things.websitename.org | vps.websitename.org | 777  |
| 77.127.170.121 | things.websitename.org | vps.websitename.org | 777  |
| 174.174.177.77 | websitename.org           | vps.websitename.org | 110  |
| 174.174.177.77 | websitename.org           | vps.websitename.org | 147  |
| 174.174.177.77 | websitename.org           | vps.websitename.org | 22   |
| 174.174.177.77 | websitename.org           | vps.websitename.org | 27   |
| 174.174.177.77 | websitename.org           | vps.websitename.org | 7707 |
| 174.174.177.77 | websitename.org           | vps.websitename.org | 77   |
| 174.174.177.77 | websitename.org           | vps.websitename.org | 70   |
| 174.174.177.77 | websitename.org           | vps.websitename.org | 777  |
| 174.174.177.77 | test.websitename.org      | vps.websitename.org | 110  |
| 174.174.177.77 | test.websitename.org      | vps.websitename.org | 147  |
| 174.174.177.77 | test.websitename.org      | vps.websitename.org | 22   |
| 174.174.177.77 | test.websitename.org      | vps.websitename.org | 27   |
| 174.174.177.77 | test.websitename.org      | vps.websitename.org | 7707 |
| 174.174.177.77 | test.websitename.org      | vps.websitename.org | 77   |
| 174.174.177.77 | test.websitename.org      | vps.websitename.org | 70   |
| 174.174.177.77 | test.websitename.org      | vps.websitename.org | 777  |
+----------------------------------------------------------------------+
```

Reconnaisance: Next Steps

- Run vulnerability harvesting modules.
- Run contact harvesting modules.
- Mangle contacts into email addresses.
- Run modules that convert email addresses into full contacts.
- Run credential harvesting modules.

Reporting

- Export data for analysis.

```
[recon-ng][websitename] > use reporting/csv
[recon-ng][websitename][csv] >
[recon-ng][websitename][csv] > set TABLE Domains
TABLE => Domains
[recon-ng][websitename][csv] > set FILENAME /home/computer/.recon-ng/workspaces/websitename/Domains.csv
FILENAME => /home/computer/.recon-ng/workspaces/websitename/Domains.csv
[recon-ng][websitename][csv] > run
[*] 5 records added to '/home/computer/.recon-ng/workspaces/websitename/Domains.csv'.
```

Creating API Keys

- Bing API Key (bing_api) -
  - Sign up for the free subscription to the Bing Search API here: https://datamarket.azure.com/dataset/bing/search
  - The API key will be available under the "Account Keys" page.
- BuiltWith API Key (builtwith_api) -
  - Sign up for a free account here: https://api.builtwith.com/
  - Sign in to the application.
  - The API key will be available in the upper right hand portion of the screen.
- Google API Key (google_api) -
  - Create an API Project here: https://console.developers.google.com/project/
  - The API key will be available in the project management console
    - Click on the "APIs & auth" Menu
    - Click on the "Credentials" sub-menu
    - Click the "Create new Key" button under "Public API Access"
    - Click "Server Key"
    - Type your current ip-address into the text box.
    - Make sure you delete it after use.
- Google Custom Search Engine (CSE) ID (google_cse) -
  - Create a CSE here: https://www.google.com/cse/create/fromkwsetname
  - Type in a name
  - Click the "Proceed" button
  - Click "Setup" in the side bar.
  - Change the "Sites to search" drop-down from "Search only included sites" to "Search the entire web bit emphasize included sites"
  - Read here for guidance on configuring the CSE to search the entire web. Otherwise, the CSE will be restricted to only searching domains specified within the CSE management console. This will drastically effect the results of any module which leverages the CSE.
  - The CSE ID will be available in the CSE management console.
  - Click "Setup" in the side bar.
  - Click the "Search engine ID" button in the "Details" section.
- IPInfoDB API Key (ipinfodb_api) -
  - REQUIRES A PERMANENT IP ADDRESS LIKE A SERVER
  - REQUIRES A CUSTOM DOMAIN EMAIL (it rejects "free" accounts like gmail)
  - Create a free account here: http://www.ipinfodb.com/register.php
  - Log in to the application here.
  - The API key will be available on the "Account" tab.
- Shodan API Key (shodan_api) -
  - Create an account or sign in to Shodan using one of the many options available here: https://developer.shodan.io/
  - On the right side of the screen under "API Key" Click "Click here to create an API key."
  - The API key will be replace that text.
  - An upgraded account is required to access advanced search features.
- Twitter App API key (twitter_api) and (twitter_secret) -
  - Create an application here: https://apps.twitter.com/
  - The Consumer key will be available on the application management page.
  - The Consumer secret (twitter_secret) will be available on the application management page for the application created above.
- VirusTotal API Key (virustotal_api)

    - Create a free account by clicking the "Join our community" button here: https://www.virustotal.com/en/documentation/private-api/#
    - Log in to the application and select "My API key" from the user menu.
    - The API key will be visible towards the top of the page.

- Facebook API Key (facebook_api) - TBD

- Facebook Secret (facebook_secret) - TBD

- Flickr API Key (flickr_api) - TBD

- API's we won't be using
    - Jigsaw API Key: Costs $1,500/year
    - PwnedList: Costs Money
- LinkedIn API Key (linkedin_api) -
    - Log in to the developer portal with an existing LinkedIn account
    - Add a new application.
    - Click on the application name.
    - Add http://127.0.0.1:11777 to the list of "OAuth 2.0 Redirect URLs".
    - The API key will be available underneath the "OAuth Keys" heading.

- As of November 4th, 2017, the People Search API (required for all LinkedIn related modules) has been added to the Vetted API Access program. As a result, a Vetted API Access request must be submitted and approved for the application in order for the associated API key to function properly with the LinkedIn modules.

- LinkedIn Secret (linkedin_secret) - The Secret key will be available underneath the "OAuth Keys" heading for the application created above.

Foca Analyzer

FOCA Quick Guide

Requirements: - FOCA executable - Windows Environment (Virtualized) - .NET Framework

Installing FOCA analyzer - Download from FOCA website - Install .NET Framework - Extract FOCA zip file into a folder - To launch, go to `foca pro` then`bin` and select FOCA application

Features & Functionality

FOCA scanner has tons of great features from web searches and DNS searches as examples. To know more of functionalities, visit FOCA's website

Creating Your first Project:

To create a project in FOCA, click `Project` on the tab menu, and select `New Project`

There are few items to fill in FOCA: - **Project name:** Name of your project - **Domain website:** the Website of your target - **Alternative domains:** for sub-domains, and other domains that your target own - **Folder where to save documents:** Select any folder or create a folder for your FOCA results - **Project date:** Date of your project (automatically filled up) - **Project notes:** Any notes that you have for this particular project

After completing the forms, select the button `Create`

Scan and Search:

After saving your project, it will bring you to the main window. On the upper right hand corner of your screen, you will see the two settings:

- **Search Engines:** search engines you wanted to use (*Google, Bing, Exalead*)
- **Extensions:** Extension refers to file extensions (*doc, docx, xls, xlsx etc*) By selecting an extension, it will be included in the scan/search.

Click the Search All buttong below the Extension options to start scan.

Note: FOCA will give you a warning regarding the IP address of the target and it's netrange owner. This will be added to the alternative domain.

Analyzing Public Documents:

The results of FOCA depends on the files/documents uploaded to the website that are "publicly available". There are situations, where an organization may not have any publicly available documents. If that is the case, move next to the Maltego assessment activity.

However, if your scan generates files/documents scanned, you can may analyzing and extract metadata from the identified files/documents.

Downloading Files:

After when the search/scan has completed, right-click on any file, (NOTE: you can start downloading files one-by-one, or all at once by using SHIFT+SELECT. you can only extract metadata of files that are already downloaded). If the target website contains a lot of files and documents available, you may want to download all the files all at once.

Extracting Metadata:

After selecting a file/s that is/are downloaded, you may right-click and select Download Metadata You may start analyzing the files one-by-one of all at once. To do this, first, download all documents. Then, right-click, select Extract all Metadata. After Extracting your metadatas you can now right-click again, and select: analzye metadata. (There's a green button that will appear once a file has been downloaded and analyzed. It will show download progress bars for each individual files and the time it takes time to download)

Analyzing Reports and Findings

After downloading documents and extracting metadata, you may view the results on the left side pane of your FOCA. On the left pane, you will see the following options: - Network - Domains - Roles - Vulnerabilities - Metadata

Under Metadata you will have two sub-menus, Documents and Metadata Summary. The Documents, option displays scraped metadata per document/file. However, on Metadata Summary option, you will have the following options: - User - Folders - Printers - Software - Emails - Operating Systems - Passwords - Servers

These information can then be added to your records and be used for other attack surface such as social engineering attacks.

Along with your other results, from different tools and recon activity, you may include all of these information to your documentation tool. Kali Linux comes with a documentation tool called Keepnote.

Recommendation

Summary

Using online tools as a starting point in assessing the auditee web application is a good way to expand online reconnaisance as well as start your vulnerability assessment. You can build a profile and a good understanding of the web application by identifying what comprises the web application and technologies behind. From there you can start your next move by putting together different strategies on conducting your vulnerability assessment.

For example, after discovering accessable web directories, you can then start looking for forgotten or abandoned files and applications that might contain sensitive information like (Passwords) or an outdated and vulnerable applications. Content management systems, while powerful, require ongoing maintenance and updates to stay secure. Quite often these (or specific plugins) fall out of date and become increasingly vulnerable to automated as well as targeted attacks.

Online tools offer ways of performing "passive" scans, in which your identity is hidden from the target organization, in cases where there are IDS/IPS, firewalls deployed. These should be used in conjuction with other outputs from reconnaisance to determine platforms and hosts which are out of scope.

Overview

- Determine the version of any content management system used by the organization
- Search for potential security vulnerabilities for that version.

Materials Needed

Considerations

Walkthrough

Before unleashing more advanced and powerful tools like OpenVAS, a few quick steps can help better guide your work. As a general note, surfing using a browser with at least NoScript enabled may help not only protect you, but may also help to reveal malware or adware infecting the websites.

Record core details about the website - determine the hosting provider, platform, Content Management Systems, and other baseline data. BuiltWith is a great tool. There are a few alternatives, including an open source tool, SiteLab. *Note that BuiltWith is a tool bundled in recon-ng, but the output it provides is not currently stored in its data structures.* These tools may also reveal plugins, javascript libraries, and DDoS protection systems like CloudFlare.

Tools

- BuiltWith
- Online Pentesting Tools
- Hacker Target

CMS Version Detection

For CMS systems, out of date components can mean well-known and easy to exploit by malicious actors.

Drupal For Drupal, try visiting /CHANGELOG.txt , which, if not manually removed, will reveal the most recent version of Drupal installed on the server. Other telltale signs depend on the specific Drupal release; http://corporate.adulmec.ro/blog/2010/drupal-detection-test-site-running-drupal maintains a detection tool.

```
Drupal 6.27, 2012-12-19
----------------------
- Fixed security issues (multiple vulnerabilities), see SA-CORE-2012-004.
Drupal 6.26, 2012-05-02
----------------------
- Fixed a small number of bugs.
- Made code documentation improvements.
```

Joomla For Joomla, default templates provide strong hints towards versions based on copyright dates. Specific versions can often be discovered using this guide: https://www.gavick.com/magazine/how-to-check-the-version-of-joomla.html

WordPress Wordpress sites tend to advertise their version number in the header of each webpage, such as

```
<meta name="generator" content="WordPress 3.3.1" />
```

There is a web-based tool with browser add-ons available here: http://www.whitefirdesign.com/tools/wordpress-version-check.html

---

Recommendation

Most popular CMS platforms provide emailed alerts and semi-automated ways to update their software. Make sure someone responsible for the website is either receiving these emails or checking regularly for available updates. Security updates should be applied immediately. It is a best practice however to have a “test” site where you can first deploy any CMS update before attempting it on a production site.

For custom CMS systems, it is strongly advisable to migrate to a more standard, open source system.

An increasingly good practice is for organizations to take advantage of the "free" tiers of DDoS mitigation services, of which CloudFlare is probably the best known. A challenge of these free services can be that they have definite limits to their protection. With CloudFlare, organizations can request to be a part of their Project Galileo program to support at-risk sites even beyond their normal scope of support.

A community-based, open source alternative is Deflect, which is completely free for eligible sites.

Some of these services will be revealed by BuiltWith, but checking the HTTP Response Headers (in Chromium/Chrome, available under the Inspect Element tool, or by using Firebug in Firefox. See Deflect's wiki for more information.

Guide for NGOs about DDoS: Digital First Aid Kit

DNS ENUMERATION

Summary

DNS Stands for Domain Name Service. In a nutshell, what it does is translate hosts/computer's name into it's IP addresses. It provides a way to know the IP address of any given machine on the internet, with the corresponding URL, or domain. You can consider it as telephone directory of the Internet.

DNS enumeration is one of your initial steps in your overall vulnerability assessment and audit. It is one stage where it will allow you to discover more potential targets. Upon completion of this assessment stage, you may find issues such as leaked information caused by default settings and server misconfigurations. Along with these, you can also have a broader scope of targets, such as internal server IP addresses, company netblocks and domain/subdomain names.

DNS Enumeration can be accomplished with different number of tools along with different approaches. This guide will discuss some of the approaches and the tools required to perform each of the activities. You can perform DNS enumeration passively or actively, depending on your operational security needs.

Passive, or "indirect" approach refers to the enumeration process that doesn't send any traffic or packets from your machine, directly to your target. This can be done using 3rd tools such as online tools and cloud based scanners.

Active, or "direct" approach refers to sending DNS queries and enumeration tests directly to the target. Consider that traffic is send over the target which may leave traces or traffic logs coming from your source IP. Active techniques include Zone Transfer, Reverse Lookup, Domain and Host Brute-Forcing, Standard Record Enumeration (wildcard, SOA, MX, A, TXT etc), Cache snooping, and Zone Walking

Overview

- Using a variety of passive and active techniques, uncover as many domains/subdomains linked to the target organization as possible.
- Use these to advance other aspects of your work to discover additional credentials and potential vulnerable or outdated services.

Materials Needed

- System or VM running Kali Linux.
- Internet Connection (and possibly a VPN or tor setup)
- Target domain(s)
- Secure notetaking tool

Considerations

- These techniques can reveal your interest in the target organization to anyone in your network path, so consider using a VPN or tor to conduct searches.
- When performing "active enumeration" it is always good to ask to whitelisting your IPs whenever you perform assessments. This rules out the idea of attackers having able to avoid shunning. Whitelisting your IPs also removes false positive reports and inaccurate results
- It is important that we verify that we have the correct target domain(s) before proceeding with any of the scans/audits/assessments exercises within SAFETAG Framework. The last thing we wouldn't want to happen is to scan and enumerate target which is out of scope!)

Walkthrough

The flexibility of having multiple options in performing a DNS enumeration activity is the key for a successful enumeration. As a practice, comparing results can help in assuring that the information we gather is accurate. Your investigation may be blocked by CloudFlare, a popular DDoS protection service. "CloudFlair" provides some options in this case.

DNS Enumerations Tools:

Tools	Description	Type	Technique
	Gathers public information about IP numbers, domain names, host names,		

Tools	Description	Type	Technique
Robtex	Autonomous systems, routes etc, then indexes the data in a big database and provide free access to that data	Online	Passive
DNSdumpster	Free domain research tool that can discover hosts related to a domain, results with banners for HTTP, FTP, SSH & Telnet	Online	Passive
CentralOps-Domain Dossier	Investigates domains and IP addresses. Gathers registrant information, DNS records, Network and Domain Whois Records, services scans and traceroutes	Online	Passive
DNSSEC Analyzer	Checks for DNSSEC keys managment and configurations records	Online	Passive
Recon-ng	Automated web reconnaissance framework written in Python. Complete with independent modules, database interaction, built-in convenience functions, interactive help and command completion.	Script	Active
IntoDNS	IntoDNS checks the health and configuration of your DNS and provides report on MX records too. Provides suggestions to fix and improve findings	Online	Passive
YougetSignal	Helps you find other sites being hosted on a particular IP address, verifying if the target is using a shared hosting service	Online	Passive
DNSRecon	A Python script written by Carlos Perez for conducting DNS reconnaissance. It can enumerate general DNS records, perform zone transfers, perform reverse lookups, and brute-force subdomains among other functions. It will even perform Google scanning, automating the process we discussed in the Using Google to find subdomains section.	Script	Active
DNSenum	multithreaded perl script to enumerate DNS information of a domain and to discover non-contiguous ip blocks.	Script	Online

Specific instructions for selected tools/techniques follows:

Passive: Third Party and Online Tools

Using 3rd party and online tools can help an auditor/tester in avoiding his/her machine to generate logs on the target's end. In cases where the target, or partner organization who requests for an audit/assessment has some security devices in place (IDS/IPS, Firewall etc.) Generating logs from your machine/network may result sometimes in our traffic getting blocked due to "automatic blocking" features in these security devices/appliances.

Passive tools include:

- Robtex
- DNSDumpster
- CentralOps Domain Dossier
- DNSSEC analyzer
- IntoDNS
- YougetSignal Reverse IP Domain Check

Active: DNSrecon

DNSrecon (available in Kali 2017 Release) is a powerful DNS enumeration script that can help and auditor in gathering information during the recon stage. This tool checks all NS records for Zone transfers, enumerate general DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF and TXT). Performs SRV record enumeration and TLD (Top Level Domain) Expansion to name some.

This exercise will help you in performing some of the DNS enumeration methods using DNSrecon and generate information which you can add to your database to be used for other avenues of testing.

Perform basic DNS enumeration on target:

```
root@kali:~# dnsrecon -d <target domain>
```

Perform DNS Zone Transfer enumeration:

```
root@kali:~# dnsrecon -d <target.domain> -a
root@kali:~# dnsrecon -d <target.domain> -t axfr
```

Perform Reverse Lookup:

```
root@kali:~# dnrecon -r <start-IP-to-end-IP>
```

Domain Brute-Force:

```
root@kali:~# dnsrecon -d <target.domain> -D <namelist> -t brt
```

Cache Snooping:

```
root@kali:~# dnsrecon -t snoop -n Sever -D <Dictionary>
```

Zone Walking:

```
root@kali:~# dnsrecon -d <target.domain> -t zonewalk
```

Active: DNSenum

DNSenum, just like DNSrecon, is a tool designed to analyze DNS information of a specific DNS target. From zone transfer, hostname and subdomain dictionary brute force, reverse lookup service record and standard record query and top level domain name expansion, results are almost identical for both assessment tools.

You can use DNSenum from the Kali terminal and MSF Console platform as an auxilliary.

To access DNSenum, simply type the command `dnsenum`. (You can add `-h` for help options.)

```
root@kali:~# dnsenum
```

The table below will help you get started with your DNS enumeration using `dnsenum` tool.

DNS Command	Description
dnsenum -h	Display Help options
dnsenum domain.com	Performs basic DNS enumeration
dnsenum --enum domain.com	Performs fast enumeration (equivalent to --threads 5 -s 15 -w)
dnsenum -f list.txt -r <domain.com>	Performing hostname and subdomain directory bruteforce using the list.txt file
dnsenum -f list.txt -s 5 -p 5 domain.com	Enumerate using subdomain list, (list.txt) scrap 5 subdomains (-s), with 5 Google result pages (-p)
dnsenum -f list.txt -o result.xml internews.org	Enumerate target with subdomain list (list.exe), generates output in XML format -o

Active: Simple Zone Transfer

Anonymous individuals online can request the full list of the hostnames on the organizations domain. Responding to zone requests from anyone on the Internet is comparable to providing an inventory of office locations, pending projects and service providers to anyone who asks. As such, it is not inherently dangerous, but it does require that the organization not rely on the assumption that unpublicized URLs are in fact secret.

An overly permissive domain name service (DNS) provider allows an attacker to enumerate online services that the organization might think are “hidden” because they have not been (intentionally) published. A zone transfer returns all of the hostnames at a particular domain, or “zone.” So, a request for sample.org may return www.sample.org, webmail.sample.org and ftp.sample.org, along with other less obviously guessable targets, such as wordpress-testing.sample.org.

While any user should be able to use a name server to look up a hostname and convert it to the corresponding IP address, most well-administered name servers allow full “zone transfer” requests only from a specific list of authorized locations (often themselves subsidiary name servers).

Determine the authoritative name server(s) for the organization’s primary domain:

```
$ host -t ns sample.org
sample.org name server ns1.something.net.
sample.org name server ns2.something.net.
```

Attempt a zone transfer on that domain, using that name server:

```
$ host -l sample.org ns1.something.net
Using domain server:
Name: ns1.something.net
Address: 256.0.0.1#53
Aliases:

www.sample.org has address 256.0.0.2
mail.sample.org has address 256.0.0.3
webmail.sample.org has address 256.0.0.4
ftp.sample.org has address 256.0.0.5
foo.sample.org has address 256.0.0.6
bar.sample.org has address 256.0.0.7
```

Active: MX Records

MX, or Mail Exchange, records are required to be public for any domain you wish to receive email through. These records can still reveal sensitive information about an organization's hosting set-up and office software in use through further scanning (see Vulnerability Scanning). MX Records can reveal vulnerable mail servers or information about other services hosted internally. Unless other assessments reveals specific vulnerabilities in e-mail services used, there is no specific action to take. If an orgnization is self-hosting email, it may be advisable to suggest outsourcing that if funds permit. While self-hosted email provides more control and potentially security, managing the security of the server is a complex job. Other mail services can provide some level of protection by being a first-pass check for spam and viruses, and (slightly) reducing the visibility of an organizational mail server.

```
root@bt:~# host -t mx sample.org
sample.org mail is handled by 21 mail.sample.org
```

Determine the IP address of the mail server:

```
root@bt:~# host mail.sample.org
mail.sample.org has address 256.0.0.3
```

Recommendation

DNS is inherently public information, but we can still do a lot of steps to secure any parts of it which are revealing more private information. Fortinet provides a set of good recommendations:

https://blog.fortinet.com/2016/03/10/10-simple-ways-to-mitigate-dns-based-ddos-attacks

If a zone transfer was successful, (most providers automatically limit anonymous zone transfers), you will need to work with their support team to prevent this, or switch to a different DNS provider. If your organization maintains its own DNS servers, the administrator of those servers should check the zone transfer policies to prevent anonymous transfers.

NETWORK ACCESS

SUMMARY

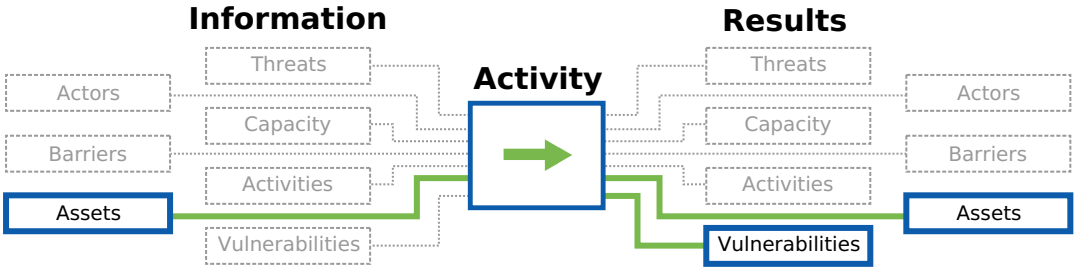
This component allows the auditor to test the strength of defenses the host has in place to protect their local area network. This component consists of gaining access to the local area network through a wireless access point and unsecured physical channels (such as an ethernet jack).

PURPOSE

By walking organizations through the vulnerabilities of wireless networks, you have the opportunity to discuss password strength, and the power that having "offline" access to a password means in terms of brute forcing it, as well as the importance of defense in depth even within their trusted work network - reducing the services computers and servers are sharing, setting up local firewalls on computers, and requiring authentication to access files.

Even a few minutes of network "sniffing" by an adversary can enable them to work offline to reveal the network password. Knowing this password would let someone then access the entire internal network, files shared internally, and even change network settings to enable remote access. While in an ideal setup, this would give no further access to sensitive documents, it is not uncommon to find shared file folders, or to gain access to the firewall or network routers (often set to the default password, because they're only accessible from inside the network...).

THE FLOW OF INFORMATION



Information Flow

GUIDING QUESTIONS

- Does the organization use strong encryption (WPA2) to secure its wifi?
- How secure is the password for the wifi network?
- How are guests provided Internet access?

APPROACH

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

Note: If you didn't manage to break through the password, it's not worth the precious audit time to brute force it - simply ask for the password and move on. If it's a WPA network, you can work on cracking the password after hours, if only to demonstrate the amount of time their current password would "protect" them for against a dedicated attacker.

OUTPUTS

- Un-authorized access to the Wireless access point (WAP)
- List of unused ethernet jacks with network connectivity.

OPERATIONAL SECURITY

Note: 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.

Once you have access to the network, you need to first document how you managed that and share it with the hosts. This is a great moment to discuss passwords in many cases.

- Confirm that all devices you are accessing/scanning belong to the organization.
- Clarify timing and seek permission with staff - some activities can tax the network or cause disruptions.

PREPARATION

Baseline Skills

- Knowledge of wireless networking and the aircrack suite of tools

RESOURCES

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)
- *Documentation:* "Wireless Network Review" (amanhardikar.com)
- *References:* "Router Hacking"
- *Guide:* "Common/default passwords" (Penetration Execution Standard)
- *List:* "Default Password List" (defaultpassword.com)

- *List:* "Default Password List" (CIRT.net)
- *List:* "Default Password List - 2007" (Phenoelit)

ACTIVITIES

WPA PASSWORD CRACKING

Summary

The organization's wireless Local Area Network (WLAN) protects the network and its users with WPA encryption. This is an important security measure, and a WPA-protected wireless network is much safer than an unencrypted "open" network or a WEP-protected network. (WEP is fundamentally flawed, and extremely simple attacks have been widely known for over a decade.) However, the ease with an attacker could guess the WPA key, or "WiFi password," is a serious issue, particularly considering its importance as an essential perimeter control. An attacker who gains access to the wireless LAN immediately bypasses many protections that network administrators, and other users of the office network, often take for granted. Put another way, anyone able to guess the WPA key is immediately "inside the firewall."

Using a laptop and a wireless card with a standard, internal antenna (or using a customized smartphone or other small device), an attacker could easily position themselves close enough to the office to carry out the first phase of this attack, which would only take a few minutes. The second phase, which is supposed to be the difficult part, could take even less time. From the privacy of their own home or office, the attacker could use a minimally customized password dictionary to guess the WPA key .

Overview

Materials Needed

- For the (most common) WPA password-based attacks, an already-prepared dictionary of words to use to attack the password will be required. See the Appendix on Audit Preparation for guidance on dictionary preparation.

Considerations

Walkthrough

An attacker can crack the office's WPA key in approximately with a short and minimally customized password dictionary based on open information about the organization and basic word collections.

Step 1: The attacker customizes their WiFi password dictionary, adding phrases related to the subject: organization name, street address, phone number, email domain, wireless network name, etc. Common password fragments are included, as well: qwerty, 12345, asdf and all four-digit dates back to the year 2001, for example, among others. The attacker may then add hundreds or thousands of words (in English and/or other relevant languages).

See the Dictionary Creation example under Preparation for details on password dictionary buidling.

Step 2: The attacker would then begin recording all (encrypted) wireless traffic associated with the organization's access point:

```
$ sudo airodump-ng -c 1 --bssid 1A:2B:3C:4D:5E:6F -w sampleorg_airodump mon0
```

```
CH  1 ][ Elapsed: 12 mins ][ 2012-01-23 12:34 ][ fixed channel mon0: -1
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
1A:2B:3C:4D:5E:6F  -70 100    12345    43210    6   1  12e. WPA2 CCMP   PSK sampleorg
BSSID              STATION            PWR   Rate    Lost  Packets  Probes
1A:2B:3C:4D:5E:6F  01:23:45:67:89:01    0    0e- 0e   186    12345
1A:2B:3C:4D:5E:6F  AB:CD:EF:AB:CD:EF    0    1e- 1      0     1234
1A:2B:3C:4D:5E:6F  AA:BB:CC:DD:EE:FF  -76    0e- 1      0     1122
1A:2B:3C:4D:5E:6F  A1:B2:C3:D4:E5:F6  -80    0e- 1      0     4321
```

wifite is also useful for this step, and claims to automatically de-auth (step 3).

Step 3: Next, the auditor forces a wireless client, possibly chosen at random, to disconnect and reconnect (an operation that is nearly always invisible to the user).

In the example below, AB:CD:EF:AB:CD:EF is the MAC address of a laptop that was briefly disconnected in this way.

```
$ aireplay-ng -0 1 -a 1A:2B:3C:4D:5E:6F -c AB:CD:EF:AB:CD:EF mon0

15:54:48  Waiting for beacon frame (BSSID: 1A:2B:3C:4D:5E:6F) on channel -1
15:54:49  Sending 64 directed DeAuth. STMAC: [AB:CD:EF:AB:CD:EF] [ 5| 3 ACKs]
```

The goal of this step is to capture the cryptographic handshake that occurs when the targeted client reconnects. Try using different clients if the first one doesn't work, or try (physically) moving around.

This handshake does not contain the WPA key itself, but once the the complete handshake process has been seen, the auditor (or a potential attacker) can leave the vicinity and run various password cracking tools to try and discover the password. While a complete password cracking tutorial is out of scope for SAFETAG documentation, below are three strategies:

Step 4: The auditor attempts to discover the WPA password.

A good wordlist with a few tweaks tends to break an unforunate number of passwords. Using a collection of all english words, all words from the language of the organization being audited, plus a combination of all these words, plus relevant keywords, addresses, and years tends to crack most wifi passwords.

```
  $ aircrack-ng -w pwdpairs.txt -b 1A:2B:3C:4D:5E:6F sampleorg_airodump*.cap
```

For WPA captures, John can either feed in to an aircrack process or attack a capture directly. For captures, you first have to convert the .cap file (from wireshark, wifite, airodump, etc.) to a format that John likes. The Jumbo version we use has conversion tools for this available:

```
$wpapcap2john wpa.cap > crackme
$./john -w:password.lst -fo=wpapsk-cuda crackme
```

Results

Successful password cracking via piping these into aircrack-ng:

```
Opening sampleorg_airodump-01.cap
Reading packets, please wait...
                          Aircrack-ng 1.1
                [00:00:05] 9123 keys tested (1876.54 k/s)
                     KEY FOUND! [ sample2012 ]

    Master Key     : 2A 7C B1 92 C4 61 A9 F6 7F 98 6B C1 AB 53 7A 0F
                     3C AF D7 9A 0C BD F0 4B A2 44 EE 5B 13 94 12 12
```

```
Transient Key  : A9 C8 AD 47 F9 71 2A C6 55 F8 F0 73 FB 9A E6 1D
                 23 D9 31 25 5D B1 CF EA 99 2C B3 D7 E5 7F 91 2D
                 56 25 D5 9A 1F AD C5 02 E3 2C C9 ED 74 55 BA 94
                 D6 F5 0A D1 3B FB 39 40 19 C9 BA 65 2E 49 3D 14

EAPOL HMAC     : F1 DF 09 C4 5A 96 0B AD 83 DD F9 07 4E FA 19 74
```

The fourth line of the above output provides some useful information about the effectiveness of a strong WPA key. That rate of approximately 2000 keys per second means that a full-on, brute-force attack against a similar-length key that was truly random (and therefore immune to dictionary-based attacks) would take about 70^9 or 20 trillion seconds, which is well over 600,000 years. Or, for those who favor length and simplicity over brevity and complexity, a key containing four words chosen from among the 10,000 most common English dictionary words would still take approximately 150,000 years to crack (using this method on an average laptop).

It is worth noting that an attacker with the resources and the expertise could increase this rate by a factor of a hundred. Using a computer with powerful graphical processing units (GPUs) or a cloud computing service like Amazon's EC2, it is possible to test 250,000 or more keys per second. A setup like this would still take several lifetimes to guess a strong password, however.

Regardless, the success of this attack against a wireless network would allow an attacker to bypass all perimeter controls, including the network firewall. Without access to the office LAN, a non-ISP, non-government attacker would have to position himself on the same network as an external staff member in order to exploit any flaws in the organization's email or file-sharing services. With access to the local network, however, that attacker could begin carrying out Local attacks quite quickly, and from a distance.

With regard to the distance from which an attacker could maintain such access, the office WiFi network appears to have a relatively strong signal, which extends to the street out front:

{photograph of location}

Figure 1: WiFi signal strength from a nearby location

{screenshot of WiFi strength}

Material that may be Useful:

- *Tutorial:* "How to Crack WPA/WPA2" (Aircrack-ng Wiki) "Aircrack-ng" (Aircrack-ng Wiki)
- *Documentation:* "Aireplay-ng" (Aircrack-ng Wiki)
- *Documentation:* "Airodump-ng" (Aircrack-ng Wiki)

Recommendation

WPS PIN CRACKING

Summary

WPS was built as an addition to WPA to make it easier to add devices without typing in secure passwords, but this ease of use means that a malicious actor can pose as a device and effectively reduce the potentially very difficult passwords WPA allows down to a simple numeric-only 8 character PIN. Further, the WPS system allows an attacker to work on this PIN in two parallel chunks, further reducing its security. This, like WEP, is a "live" attack - you have to stay connected to the network - but also like WEP, it is a guaranteed attack; your brute forcing of the WPS system will eventually (2-10 hours) allow you network access.

Walkthrough

- Find the BSSID of the target routerr
- Use Wash to find WPS Routers
- Start Reaver : estimated time: Between 2 and 10 hours

Material that may be Useful:

- *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)
- *Documentation:* "Airodump-ng" (Aircrack-ng Wiki)
- *Tutorial:* "Resetting WPS Lockouts" (Kali Linux Forums)

Recommendation

WPS Pin entry should be disabled on the wireless router, or only enabled temporarily to add new devices to the network.

WEP PASSWORD CRACKING

Summary

WEP provides no effective protection for a wifi network. Most wifi routers offer WPA encryption as an option, and if this is available it should be immediately implemented. Some older routers (and wifi devices) do not support WPA. It is highly recommended to upgrade immediately to hardware that supports WPA and to eliminate all WEP network access.

Walkthrough

The auditor can be guaranteed to access a WEP network with sufficient time by cracking the WEP key.

- Start the wireless interface in monitor mode on the specific AP channel
- Use aireplay-ng to do a fake authentication with the access point
- Start airodump-ng on AP channel with a bssid filter to collect the new unique IVs
- Start aireplay-ng in ARP request replay mode to inject packets
- Run aircrack-ng to crack key using the IVs collected

Material that may be Useful:

For educational purposes, if no WEP network is available, you can use this pre-built airodump-ng capture file and skip the airodump-ng and aireplay-ng packet injection steps.

- *Tutorial:* "Simple WEP Crack" (Aircrack-ng Wiki)
- *Tutorial:* "Simple Wep Cracking with a flowchart" (Aircrack-ng Wiki)
- *Documentation:* "Aircrack-ng" (Aircrack-ng Wiki)
- *Documentation:* "Aireplay-ng" (Aircrack-ng Wiki)
- *Documentation:* "Airodump-ng" (Aircrack-ng Wiki)

Recommendation

ACCESSING A MAC-FILTERED NETWORK

Summary

Open and MAC-address-filtered wireless access points are not only open to anyone within range to join and listen in to, but also do not provide protection to those on the network itself, even if they do not "broadcast" their name. These may seem like great ways to prevent unauthorized users from accessing your network without resorting to passwords, but they are trivial to overcome.

Overview

Materials Needed

Considerations

Walkthrough

The auditor can easily gain access to an open or MAC address filtered access point.

- MAC-Address Spoofing
  - Start the wireless interface in monitor mode
  - Identify MAC addresses that are on the whitelist

airodump-ng

* Change our MAC address to one that's on the whitelist

ifconfig mon0 down
macchanger -m [MAC ADDRESS IDENTIFIED] mon0
ifconfig mon0 up

Material that may be Useful:

- *Tutorial:* "Bypassing MAC Filters on WiFi Networks" (techorganic.com)
- *Documentation:* "Airodump-ng" (Aircrack-ng Wiki)

Recommendation

Transitioning to WPA networks with strong passwords, even for guest networks, is recommended.

NETWORK MAPPING

SUMMARY

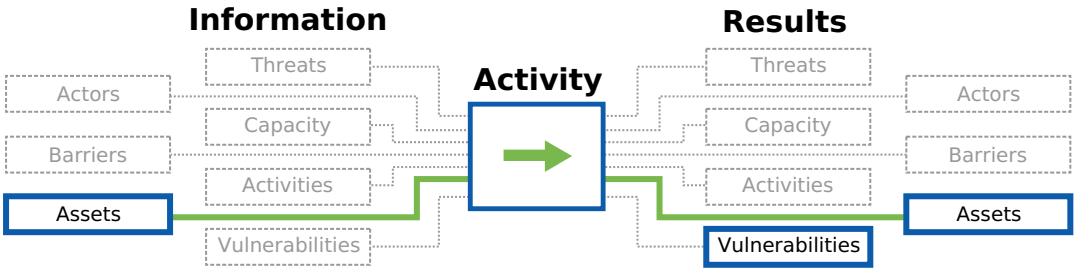
This component allows the auditor to identify the devices on a host's network, the services that are being used by those devices, and any protections in place.

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 and vulnerability research.

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.

THE FLOW OF INFORMATION



Network Mapping Information Flow

GUIDING QUESTIONS

- What operating systems, and services being hosted or used by an organization? Are any hosts running unusual, custom, or outdated operating systems and services?
- Are there unexpected/unusual devices or services on the network?
- What is the topology of the network? What are the routers and modems managing it?
- What services (e.g. dropbox, web-mail, etc.) are running on the network that have not been mentioned by the organizational staff?
- What network assets does an attacker have access to once they have gained access to the internal network?

APPROACHES

- **Network Mapping:** Map hosts, services, and network hardware by scanning network devices.
- **Monitor Open Wireless Traffic:** Monitor wireless traffic for handshakes, beacons, and MAC addresses.
- **Wireless Range Mapping:** Map the range of the organizations wireless network outside of office space.

OUTPUTS

- 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. [41]

OPERATIONAL SECURITY

- Clarify timing and seek permission with staff - some activities can tax the network or cause disruptions.
- Confirm that all devices you are accessing/scanning belong to the organization.
- Delete all devices from your scan that do not belong to the organization.

- Study outputs for any obviously embarrassing personal information (especially traffic sniffing or personal devices connected to the network) before sharing.
- Treat captured network traffic with the utmost security and empathetic responsibility. They may contain very personal data, passwords, and more. These should not be shared except in specific, intentional samples with anyone, including the organization itself.

PREPARATION

Baseline Skills

- Skill with using nmap/zenmap and its scripting options
- Skill with Wireshark or other packet-capturing tool, as well as possibly more advanced traffic interception tools.

RESOURCES

- *Guide:* "10 Techniques for Blindly Mapping Internal Networks"
- *Resource List:* Wireless Access Guides & Resources (SAFETAG)
- *Resource List:* nmap Scanning Resources (SAFETAG)
- *Resource List:* System Vulnerability Scanning Resources (SAFETAG)

Network Mapping Methods

- *Guide:* "10 Techniques for Blindly Mapping Internal Networks"
- *Directory:* "Network Forensics Packages and Appliances" (Forensics Wiki)
- *Directory:* "Scripts and tools related to Wireshark" (Wireshark Wiki)

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)

ACTIVITIES

NETWORK SCANNING

Summary

Local networks often have a variety of devices connected to them - servers, user devices, staff cellphones, and more. Scanning the connected devices can reveal potential areas for further research (odd ports being open, out of date devices/services, forgotten servers/services...).

Selected scanning of external network devices (websites, webmail, extranet services) may also reveal vulnerabilities or other areas of concern.

Overview

- Scan the network for all connected devices
- Review device information and open services for potential vulnerabilities
- Using beacons and other data, map devices to users.
- Scan select external services (particularly self-hosted webmail/email servers and other extranet services) to detect possible unencrypted but sensitive connection possibilities
- Enumerate shared directories on the network and check for access controls

Materials Needed

Considerations

Walkthrough

Using a network scanning tool (**nmap**/**zenmap** work well), discover the devices connected to the organization's network, and explore further information such as services, service banners, and operating systems. More intense scans can be too time-consuming to run across the entire network, so target those to higher value systems. As always, be aware of the scans and additional scripts you choose, and focus your exploration (in nmap) on scripts categorized as "safe".

- Discover network-connected devices, including servers and workstations, but also smartphones, printers, security cameras, voip phones, and other devices.
- OS detection
- Open ports and banners (not all ports corectly map to their "expected" services, also provides service version information)
- additional scripts and more exhaustive port scanning as needed

Port/Service research

- Inspect all systems providing internal services to the host organization.
- Record the version and patch levels of software on the device. [42]
- Identify weak ports or services available under the current device's firewall configuration. [43]
    - Using the list of software versions and patches identify attacks and, if possible, identified malware that devices in the office are vulnerable to.
    - Identify and investigate any open ports that should not be open (e.g.: almost no ports should be open in personal computers, see below)

SMB Network tools

- smbtree

Shared Folders Enumeration

Unsigned NTLM authentication messages vulnerable to Man-in-the-Middle attack on SMB file servers

Unsigned NTLM authentication messages allow an attacker on the LAN to add, remove or copy files to and from the organization's file servers (and workstations with filesharing enabled).

How to decide if an open port is suspicious

If a port is open in a personal computer or mobile device, this should be immediately considered suspicious and investigated.

An open port in a server or IoT device should be investigated if it doesn't correspond to a known service. For example, if the open port is 80, 8080, or 443, it's supposed to be open for a web server, so you can try to browse it by pasting the IP address in your browser address bar. If it's for SSH (port 22), try to log into it through SSH.

In general, these are ports that might be open in a server:

Port	Service
21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP
139	SMB
143	IMAP
194	IRC
443	HTTPS
465	SMTP
530	CUPS
587	SMTP
667	IRC
993	IMAP
995	POP
1900	port authority
3306	MySQL
6881 to 6889	Torrent
6969	Torrent
8080	HTTP

To identify what a port might be used for, look at the complete list at IANA.org. Using nmap's banner scripts will also reveal what the service reports itself as (for example, you can run ssh, usually port 22, on port 443, usually https). Once you have identified what service that port might be used for, always check that that service is actually running in the machine and that the user or sysadmin is aware of it.

If the service isn't supposed to be running in the identified device, you can run a scan of the open ports to identify what service they are connected to.

- On Mac and Linux, launch `netstat -tulpn`
- On Windows, we recommend you install the official Microsoft Process Explorer (right-click a process to see the Properties - the port will be visible in the TCP/IP tab).
- On Windows, you can also use netstat from the command prompt as an administrator: the command would be `netstat -ab`

If that service isn't running in the machine, the port might have been opened by malware. In such case, the device where the suspicious port is open needs to be analyzed, see User Device Assessment

Recommendation

While office networks are often treated as "trusted" spaces, measures should be in place to reduce the potential harm of an attacker who gains access. In addition, devices that "travel" -- such as laptops and mobile phones -- should have adequate security settings (generally, firewalls) to protect them on other networks.

A policy should be in place for connecting personal devices to work networks, as well as work devices to non-work networks.

NETWORK TRAFFIC ANALYSIS

Summary

Any content that is sent out over the network without encryption is easy to intercept; this includes email, web passwords, and chat messages.

This attacker could be someone, such as a patron of the Internet cafe where a staff member is working, who just happens to be using the same local network to connect to the Internet. Or, she could work for an organization with privileged access to the relevant network, such as the Internet Service Provider (ISP) of either the sender or receiver and other network-backbone connections made along the way.

Overview

- Intercept network traffic
- Review it for security concerns
- Watch for unencrypted email (POP/SMTP/IMAP) connections, unencrypted website logins (for blogs, websites, and webmail in particular)

Materials Needed

- Wifi device and drivers supporting "promiscuous mode" (see http://www.aircrack-ng.org/doku.php?id=compatible_cards&DokuWiki=a36042531edb54f9b95a76ff61d77d14)

Considerations

- Treat captured network traffic with the utmost security and empathetic responsibility. They may contain very personal data, passwords, and more. These should not be shared except in specific, intentional samples with anyone, including the organization itself.

Walkthrough

Network Traffic Interception

Step 1: The attacker tricks the victim into routing all of their traffic through the attacker's machine. This involves making a simple request to the victim's IP address, which is not difficult to do. Computers are rarely configured to ignore such requests.

```
$ sudo sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'

$ sudo arpspoof -i wlan0 -t 192.168.1.99 192.168.1.1
```

Sample Output:

```
00:11:22:33:44:55 aa:bb:cc:dd:ee:ff 0806 42: arp reply 192.168.1.1 is-at 00:11:22:33:44:55
00:11:22:33:44:55 aa:bb:cc:dd:ee:ff 0806 42: arp reply 192.168.1.1 is-at 00:11:22:33:44:55
00:11:22:33:44:55 aa:bb:cc:dd:ee:ff 0806 42: arp reply 192.168.1.1 is-at 00:11:22:33:44:55
00:11:22:33:44:55 aa:bb:cc:dd:ee:ff 0806 42: arp reply 192.168.1.1 is-at 00:11:22:33:44:55
...
00:11:22:33:44:55 aa:bb:cc:dd:ee:ff 0806 42: arp reply 192.168.1.1 is-at 00:11:22:33:44:55
```

In the example above, only a single victim (192.168.1.99) is being targeted, but the attack works fine against multiple victims, or even against the entire network. In other words, the attacker does not need to know which IP address (on the office or Internet cafe LAN, for example) belongs to the target. Furthermore, the victim is extremely unlikely to notice any sign that this phase of the attack is taking place.

EtterCap provides a powerful frontend to managing this process with multiple potential targets. In EtterCap:

- Under the "Sniff" menu, select "Unified sniffing" (for most cases where you are using one interface to both intercept and forward traffic), and select the relevant interface (wlan0)
- Under the Hosts menu, select the systems on the network you will target, or leave blank to target all systems
- Under Mitm, select "arp spoofing" for this example
- Select "Start" under the Sniffing menu

Step 2: At this point, if the attacker is looking for unencrypted traffic, all the attacker needs to do is launch a packet-sniffer, such as Wireshark, and scan through the intercepted traffic for specific vulnerable information, such as email or website logins, as well as traffic revealing shadow infrastructure usage, such as Dropbox.

Wireshark can also be used to identify malicious traffic.

If you rarely use Wireshark, the output you will see will be a long list of packets, protocols and connections that might be hard to classify. To look into suspicious processes in a clearer way, you can use the "Protocol Hierarchy" option in the Statistics menu A good video to learn how to use this option for this purpose can be found here.

- If you want to practice with captures of malicious traffic, you can find them in the Wireshark wiki.

Recommendation

Only use services with "SSL" encryption ("HTTPS"), and consider adding HTTPS Everywhere to browsers. This does not itself guarantee protection from all attacks, but it is a good first-step in protecting information (such as passwords or email) in transit from your computer to the service provider.

REMOTE NETWORK AND USER DEVICE ASSESSMENT

Summary

This component allows the auditor to work remotely to identify the devices on a host's network, the services that are being used by those devices, and any protections in place, as well as to assess the security of the individual devices on the network.

Overview

There can be several approaches for this exercise, depending on the scenario.

Scenario 0

The organization has contacted the auditor through an intermediary who is familiar with tech and can follow SAFETAG instructions, or the organization has a tech person among their employees.

This scenario is comparable to a situation where the auditor is on site. In this case, the auditor will instruct the intermediary or the tech person in the organization to follow the instructions in the exercise on Network mapping and on User device assessment.

Scenario 1

The organization has someone among their employees who is ready to follow simple instructions, including opening a terminal and pasting commands we will provide them.

In this scenario, the auditor will send simple instructions to the auditee, so as to be able to access the organization's network through a reverse SSH tunnel and assess the LAN and single devices from there. To run the computer used within the organization's network to establish the tunnel, a UNIX system is needed. This will be a Linux live distribution or a Mac computer.

Scenario 2

In this scenario, no one at the organization is ready to apply complex instructions. Instead of relying on an individual, the auditor will rely on tunneling into a device located in the physical space of the auditee. This can be done in two ways:

1. Remote Desktop or remote VPN into targeted Network. Remote Desktop is tunneling into a targeted machine that lives on the same targeted LAN network where you wish to scan the network and do the device assessment; the auditor controls the machine remotely and uses it as the auditor machine.
2. VPN to a trusted VPN server. In this case, the auditee will connect one of their machines to a trusted VPN server, and the auditor will connect to the same VPN server, allowing both LANs at the auditee's and auditor's ends to connect.

Materials Needed

Scenario 1

- A machine accessible globally via ssh. It could be a machine or a virtual server
- A GNULinux machine on the auditor's side
- A machine running Linux or Mac with ssh on the auditee's end. If the audited organization only has Windows computers, they can use a live distribution, for example Ubuntu Live.
    - If you're using a live Linux distribution, you will probably need to guide the auditee into changing the BIOS settings for enabling the computer to boot from a USB stick.
- If we use sshuttle, `net-tools` needs to be installed on the auditee's side. This package is installed by default in Ubuntu.

Scenario 2

In the case of remote desktop:

- Clean PC connected to the local auditee LAN network
- Stable and fast Internet connection at both ends
- TeamViewer client installed on the local clean machine. (Windows remote desktop can also be used.)
- TeamViewer installed on the auditor's machine

In the case of using an in-the-middle trusted VPN server:

- A PC connected to the local auditee's LAN network
- Stable and fast Internet connection at both ends
- OpenVPN client installed on the local clean machine
- OpenVPN client installed on the auditor's machine
- A trusted OpenVPN Server

Applications to use: TightVNC TeamViewer Windows remote desktop

Considerations

Scenario 1

- Make sure that the auditee downloads the Linux image over TLS and guide them through the verification process (instructions for Ubuntu can be found here).
- When starting a live Linux distribution, make sure the auditee has a secure communication channel with you on a different device than the one that will be rebooted - for example through Signal on an Android phone, or on a different computer.
- Warn the auditee that they should not press "install" when the live Linux distribution has started, else their hard disk will be formatted and they will lose their data.
- Make sure that a secure communication channel is in place for sending the ssh commands to the auditee.
- The server used for the middle connection should be updated and secured, or updated and ephemeral.
- Make sure to remove/clean any persistent connections once you are done with auditing.

Walkthrough

Scenario 0

Instruct the intermediary or the tech person in the organization to follow the instructions in the exercise on Network mapping and on User device assessment.

Scenario 1

Legend

- S: Server - a machine accessible globally via ssh. It could be a machine or a virtual server
- A: Auditor's GNULinux machine
- C: A machine running GNULinux or Mac with ssh on the auditee's end

Instruct the auditee to initiate a connection to the server (S) and set up a reverse ssh server:

Let's assume we have a server named safetag-audit.org (S), and usernames for each auditee called auditee1, auditee2, etc.

- on the auditee's machine (C); the auditee will need to be instructed to run the following commands:

```
service sshd start
ssh -R 2200:localhost:22 auditee1@safetag-audit.org
```

(the auditor has to provide the auditee with a password for the password prompt that will appear when this command is entered.)

this will allow any connection to port 2200 on safetag-audit.org (S) to be sent to port 22 on the auditee's machine (C). The remote port is an arbitrary high number port (> 1023); a practice can be established to assign a number to each location and machine.

example:

the auditee on machine on site 0 could be instructed to run:

```
ssh -R 2200:localhost:22 auditee0@safetag-audit.org
```

this will allow the auditee to connect to port 2200 from within safetag-audit.org (S) and have traffic forwarded to port 22 on the auditee's machine (C).

the auditee on machine on site 1 will run:

```
ssh -R 2210:localhost:22 auditee1@safetag-audit.org
```

Important: make sure that the ports you use don't conflict with ports by other services or auditees, i.e. don't use a port number twice.

Once this session is open, the auditor can access the auditee's machine (C). At this point there are a few powerful options:

- simply ssh from S to C via the tunnel (port defined in the reverse tunnel on the server localhost interface);

example:

to connect to site 0:

```
ssh clientUser@localhost -p 2200
```

with site 1 in the previous example, the port would be 2210 (or whatever the auditee used in her command).

- Create a VPN-like connection to site:
    - create a forward tunnel from A to S that is "piped" into the reverse tunnel:

```
ssh -L 2200:localhost:2200 user@safetag-audit.org
```

now you have a tunnel from your localhost:2200 to safetag-audit.org:2200, which in turn has a tunnel from safetag-audit.org:2200 to the client machine on port 22.

- once you have that, you can use sshuttle (needs to be installed, it's in most Linux standard repositories) on the auditor's machine (A) to access additional resources in the auditee's network (as long as they are non-ICMP) directly from the Auditor's machine (A). Such resources might include web-based resources (router web interface for example) or remote desktop (to assess windows or mac clients) or accessing file shares on the auditee's network, etc...

to do this, you would need to use client credentials through the tunnel you just created, and provide the client subnet to route traffic correctly through that "VPN":

```
sshuttle -r user@localhost:2200 192.168.1.0/24
```

once this tunnel is created, you should be able to access any resource on the remote network by its IP and port (for example, through the browser for http(s))

An additional thing that one might want to do is making the connection from C to S passwordless and automatic (this can be accomplished with tools or scripts readily available on the internet).

WARNING: Make sure to remove/clean any persistent connections once you are done with auditing.

There should be no need for multiple reverse tunnels, as multiple forward tunnels can be set up from S to C if needed (eg. VNC or RDP); this requires multiple forward tunnels from A to S though.

Scenario 2

Legend:

- A: Auditee's local machine; a clean machine, connected to the Internet through the auditee's LAN network
- B: Auditor machine

Someone at the auditee's side will prepare machine A in coordination with the auditor, then install TeamViewer.

After that, and using a trusted communication method, TeamViewer ID and passcode will be sent to the Auditor.

The auditor will use the ID and passcode to connect to the machine and start using machine A as the auditing machine.

There are pros and cons for this:

Cons:

1. Internet speed: You will need a high speed Internet connection to achieve such task, as the remote access will be transferring the desktop of the targeted machine to you in order to do the tasks.
2. Connection interruption: While you are working remotely, you might face some connection interruptions during your session, and restarting the remote access will be a challenge because in most of the cases you will need someone at the other end to authorize you to tunnel into the machine.
3. Physical limitations: You are still physically far from the machine, which means you cannot connect a USB drive to boot from it or do any other tasks that require you to be near the device.
4. Installing Kali Linux might be hard: It might be hard for a non-technical person to prepare a Kali Linux machine

Pros:

1. Usability: TeamViewer is easy to install and use. Anyone with basic knowledge on how to install software can assist you with preparing the auditing machine.
2. Network speed: Technically, your auditing machine is the machine you are connected to, which is physically located in the targeted office and connected to the LAN network. This means that you will have full speed running your audit tasks.

Note: Some remote assistant software provides VPN solutions that turn Machine A into a VPN Server and allow Machine B to VPN into it. Tunneling into that VPN server will allow you to connect to the local LAN network, which will allow you to use Machine B to run the audit.

Using an in-the-middle trusted VPN server

Legend:

- A : Auditee's local machine; a clean machine, connected to the Internet through the auditee's LAN network
- B: Auditor's machine
- C: OpenVPN Server

Auditee's Network --------- (A) ---------- C ---------- (B) ---------- Auditor's Network

The auditor will put efforts preparing an OpenVPN server (C) and create 2 profiles (Keys and configurations) to allow machines A and B to connect to C.

Get a VPS from your favorite and trusted VPS provider and keep in mind the physical location of the server, then install OpenVPN Server by following the instructions contained in this guide on Ubuntu Server.

The default configuration of OpenVPN will not allow the clients (A-B) to see each other on the network. To allow that, you have to enable client-to-client directive and enable your both subnets (Auditee and Auditor) to see each others networks. To do so, follow these instruction.

After finishing the installation and testing it, the auditor will pass the .ovpn file to the person at the auditee's site through a trusted way, and provide instructions on how to install and connect to the server. After connecting A and B to C, the auditor will be able to start the network and device assessment at the other end.

Note: In case the VPN is censored in A or B's countries, or in both, you can follow these instructions on how to bypass the censorship by using pluggable transports.

Recommendation

ROUTER ATTACKS

Covered in full in Vulnerability Scanning and Analysis

- Find the router(s) (route works well for this)
- Test using default passwords
- Check for upgrades / un-patched vulnerabilities and backdoors
- Investigate potentially valuable data (logs, connected users)

WIRELESS RANGE MAPPING

Covered in full in Network Discovery

This component consists of wireless scanning and wireless signal mapping. It is useful for organizations with offices in shared spaces/buildings/apartment complexes or near locations where an adversary could easily "listen" to network traffic. In conjuction with Monitoring Open Wireless Traffic exercise, it can also identify devices using that network. It is useful to do this in parallel with Office Mapping to build a more comprehensive view of the information assets of the organization.

- Identify and verify the network(s) belonging to the organization
- Create a map or photos indicating the range of each relevant wireless access point.

MONITOR OPEN WIRELESS TRAFFIC

Covered in full in Network Discovery

Each wireless device maintains a "memory" of what networks it has successfully connected to. When it is connecting to a network, it sends out "probes" to all of the networks it has in this memory. It is important to note that this data gets broadcast widely, and can be collected without any network access, only proximity to the device.

These network probes can often contain names (especially from mobile phone tethers), organizational affiliations, device manufacturers, and a mixture of other potentially valuable data (home network names, recent airports/travel locations, cafés and conference networks). If there are many networks in the office's vicinity, this activity can also help identify the specific office network (if there is any doubt). In many cases, an organization may not want the name of their wireless network to be associated with to their organization, but it may be revealed by this additional meta-data.

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.

- Scan for wireless networks nearby, identify (and confirm) the office network(s).
- Monitor traffic of that network and capture potentially sensitive metadata (wireless security settings, beacons, and MAC addresses).
- Research likely device hardware using MAC addresses.
- Do the staff devices leak sensitive metadata?
- What can be determined about the organization based on broadcast wireless data?

ORGANIZATIONAL DEVICE USAGE

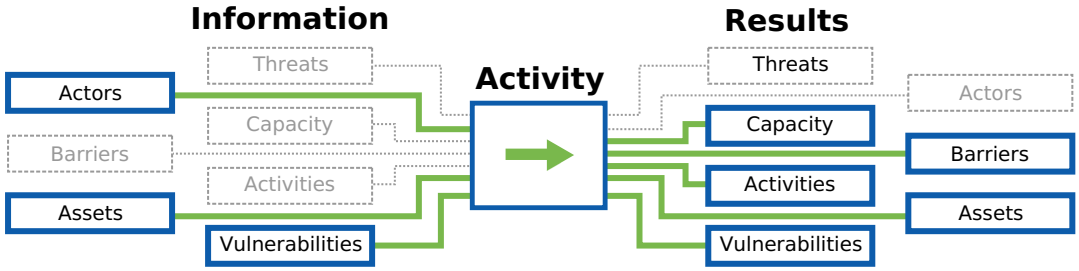
SUMMARY

This component allows the auditor to discover and assess the security of the devices on the network and/or used in the organization. This component consists of interviews, surveys, network mapping, 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 updates/upgrades and what core protections exist against unauthorized access is vital to designing a strategy to make the host more secure. Because the SAFETAG framework is focused on the security of data, it's also criticalial that the physicality of devices on which this data residences including the hard-wired networks through which its exchanged be not overlooked.

THE FLOW OF INFORMATION



User Device Assessment Information Flow

GUIDING QUESTIONS

- What work and personal devices do staff use to accomplish their work, store work related files, or engage in work communications?
- What organizational and external/personal services do staff use to accomplish their work, store work related files, or engage in work communications?
- How do staff communicate internal and external? What tools do they use?
- What are the existing in/formal security practices that the participants use to address risks.
- Who has physical access to what? Who has remote access to what?
- When are devices not monitored by trusted staff?
- How could adversaries gain access? (forced entry, theft, social engineering, seizure)
- Are there mitigation procedures if devices are lost or taken by adversaries? (e.g.: encrypted drives, offsite backups?)

APPROACHES

- **Physical Access to Devices:** Tour the office and look for logged in devices without users, servers, network jacks, written down passwords and document how difficult it would be for a visitor or after-hours break-in to access sensitive systems. Have staff take a physical security security
- **Conduct a Hands on Device Interview/Audit:** Inspect and record information on user devices (work & personal) for security concerns (existance of passwords, patch levels, user privileges, drive encryption, ports/services running, anti-virus capabilities)
- **Password User Survey:** Have staff take the password use survey for ALL devices used for work. [44,45]
- **A Day In the Life:** Have staff walk you through a usual "day in their life" showing you what devices they use, how they use them, and what data they have to interact with to conduct their work.

OUTPUTS

- List of all assets in the organization and whom they belong to.
- Notes on un/documented access controls measures for the office

- List of software running on staff devices and date of last update
- 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.)
- List of specific unsecured servers, workstations, external hard drives and any other digital resources
- Notes on existing security measures for all digital systems
- Written-down passwords

OPERATIONAL SECURITY

- Treat the information learned/collected with the utmost sensitivity and security. Physical notes should be destroyed immediately after use and digital notes should be kept in line with overall SAFETAG standards.

PREPARATION

Baseline Skills

- Basic systems administration experience for common operating systems

RESOURCES

- *Guidelines:* "Guidelines on Firewalls and Firewall Policy" (NIST 800-41)
- *Benchmarks:* "Security Configuration Benchmarks" (CIS Security Benchmarks)
- *Repository:* "National Checklist Program Repository - Prose security checklists" (National Vulnerability Database)
- *Security Guidance:* "Operating Systems Security Guidance" (NSA)
- *Windows Utility:* "HardenTools" (Security Without Borders)

Password Security

- *Guide:* "How to Teach Humans to Remember Really Complex Passwords" (Wired)
- *Guide:* "Security on Passwords and User Awareness" (HashTag Security)
- *Video:* "What's wrong with your pa$$w0rd?" (TED)
- *Article:* "Password Security: Why the horse battery staple is not correct" (Diogo Mónica)
- *Organization:* "Passwords Research" (The CyLab Usable Privacy and Security Laboratory (CUPS))
- *Guide:* "Hacker Lexicon: What Is Password Hashing?" (Wired)
- *Guide:* "7 Password Experts on How to Lock Down Your Online Security" (Wired)

Privilege Separation Across OS

- identify what privileges services are running as
- identify is the admin user is called admin or root
- Identify if users are logging in and installing software as admin.

Examining Firewalls Across OS

- *Checklist:* "Firewall Configuration Checklist." (NetSPI)

Identifying Software Versions

Device Encryption By OS

- Identifying if a device is using encryption by OS
- Encryption availablility by OS
- Encryption Guides

Anti-Virus Updates

Identifying Odd/One-Off Services

- *Guide:* "Physical Penetration Test" (About The Penetration Testing Execution Standard)
- *Checklist:* "Check list: Office Security" (Frontline Defenders)
- *Manual:* Planning, improving and checking security in offices and homes
- *Guide:* "Physical Security Assessment - pg. 122" (OSTTM)
- *Guide:* "Workbook on Security: Practical Steps for Human Rights Defender at Risk" (Frontline Defenders)
- *Guide:* "Protect your Information from Physical Threats" (Frontline Defenders)
- *Policy Template:* Information Security Policy Templates (SANS)

ACTIVITIES

DEVICE AND BEHAVIOUR ASSESSMENT

Summary

The auditor checks staff devices for updated systems and software, anti-virus and other security capabilities, and identifies software running on computers and its current version. The auditor checks for known vulnerabilities to any out of date software.

This is used to develop a report component exposing how un-updated software can lead to large vulnerabilities.

Overview

- Identify what privilege level services are running under -- Are users using accounts with admin privelges, or are they using another user and have to type in a password to get admin rights? [46]
- Check for existence and status of anti-virus (and anti-malware tools) on the device. [47]
- Record the version and patch levels of software on the device. [48]
- Identify what level of encryption is being used and is available for data storage on the device. [49]
- Using the list of software versions and patches identify attacks and, if possible, identified malware that devices in the office are vulnerable to.

Materials Needed

- A notepad may be useful

Considerations

- Communicate with the staff members the level of confidentiality you are treating discussions around their device and technology usage with - i.e. explain what incident response triggers you have agreed upon with the organization, and that anything not triggering that is to be only reported in aggregate.

Walkthrough

The auditor inspects a subset of key and/or representative user devices (work & personal). The auditor should focus on the work devices to limit scope creep, but if the office has many personal devices accessing organizational accounts/data, the auditor should share what "red flags" they are looking for and work in tandem with device owners and/or IT staff. For a small office, it may be possible to check every machine. For larger offices, the auditor should use a subset to get a feel for the overall security stance of user devices.

As you work with staff members, also interview them about the other devices they use such as phones and tablets, and how they connect to work services - email/webmail, chat Apps, intra/extranet tools, Constituent Relationship Management (CRM) tools like CiviCRM or Salesforce, financial tracking tools, and website management tools.

Below is a checklist to assist in checking across different platforms/versions for common security needs.

OSX

- OS Security Updates

- Firewall
  - See http://support.apple.com/en-us/HT1810 for cross-version guidance
  - (GUI) Choose System Preferences from the Apple menu, Security (10.5 and before) or Security & Privacy (10.6 and later), then the Firewall tab.
- Anti-Virus Version
  -
- User privilege
  -
- Drive Encryption
- CLI. sudo fdesetup status
- (GUI) Choose System Preferences from the Apple menu, Security (10.5 and before) or Security & Privacy (10.6 and later), then the FileVault tab.
- (VeraCrypt)
- Services Running
- (Command line) sudo launchctl list
- (Command line) ps -ef

- (GUI) The "Activity Monitor" application is located in /Applications/Utilities provides a similar interface to "top"

Windows

If Windows is not your primary OS, you can download sample Virtual Machines (with time limitations) from Microsoft through their project to improve IE support via https://www.modern.ie/en-us/virtualization-tools#downloads (see also http://www.makeuseof.com/tag/download-windows-xp-for-free-and-legally-straight-from-microsoft-si/ and https://modernievirt.blob.core.windows.net/vhd/virtualmachine_instructions_2014-01-21.pdf)

Windows 10

- OS Security Updates
- Start --Settings --Update & Security --Windows Update
- Firewall
- Start, type Firewall (select Windows Firewall)
- Privacy
- Start --Settings -- Privacy
- Anti-Virus Version
-
- Privacy
- (GUI) Start --Settings -- Privacy
- User privilege
- Start, type 'User Account', select "Change User Account Control settings"
- Drive Encryption
- (Bitlocker), https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-device-encryption-overview-windows-10
- Services Running
- Start, type "Task Manager"

Windows 8

- OS Security Updates
- Firewall
- (GUI) Start (or Down Arrow Icon, PC Settings) -- Control Panel -- Windows Firewall
- CLI. Netsh Advfirewall show allprofiles
- (more detail: http://windows.microsoft.com/en-us/windows-8/windows-firewall-from-start-to-finish)
- Anti-Virus Version
-
- User privilege
-
- Drive Encryption
-
- https://diskcryptor.net/wiki/Main_Page
- Services Running
- Right-Click on bottom taskbar, select "Task Manager"

Installed updates

Control Panel Programs and features installed updates CLI: http://www.techsupportalert.com/en/quick-and-easy-way-list-all-windows-updates-installed-your-system.htm

Windows 7

In Windows 7, (GUI) Control Panel -- All Control Panel Items -- Action Center (Security tab) provides a quick run-down of most security features installed and their update status. It does not show drive encryption or specific versions.

- OS Security Updates
-
- Firewall
- (GUI) Control Panel -- All Control Panel Items -- Windows Firewall
- CLI. Netsh Advfirewall show allprofiles
- Anti-Virus Version
-
- User privilege
- (GUI) Control Panel -- All Control Panel Items -- User Accounts and checking also the User Account Control settings.
- Drive Encryption
- (GUI) Control Panel -- All Control Panel Items -- BitLocker Drive Encryption
- (VeraCrypt) , https://diskcryptor.net/wiki/Main_Page
- Services Running
- CLI. tasklist
- (GUI) Right-click on task bar, select "Start Task Manager"

- (Advanced) Use TechNet/SysInternal's Process Explorer: http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

Windows XP

If user is still operating on windows XP, recommendation is to upgrade to later windows. Windows XP is no longer supported and is not receiving security updates: https://www.microsoft.com/windows/en-us/xp/end-of-xp-support.aspx

If there is an organizationally critical system relying on Windows XP, removing it from the network and carefully managing data exchange with it may provide a bridge solution until a replacement process can be funded and rolled out.

Linux

- Firewall
- CLI. sudo iptables -L -n
- CLI. (Ubuntu, and only if installed) sudo ufw status
- (GUI) (Ubuntu, and only if installed) gufw
- Anti-Virus Version
- CLI. deb: dpkg-query -l | grep virus rpm: yum list installed | grep virus
- See also: https://en.wikipedia.org/wiki/Linux_malware#Anti-virus_applications
- User privilege
- CLI. groups
- Drive Encryption
-
- (VeraCrypt)
- Services Running
- CLI. ps -ef
- CLI. top

Recommendation

If Unsupported Operating System - Upgrade to Recent Version

Popular operating systems like Windows XP are, sadly, no longer receiving security updates. Upgrade to the latest version keeping in mind the system requirements of the version selected

While "pirated" operating systems and software are extremely common (especially for Windows) they often leave much to be desired in terms of security. If the OS or Software is not receiving regular updates from the software creator, it is extremely vulnerable to thousands of potential attacks. Switch to licensed software or recommended Free Open Source Software

If Pirated Software - Move to Licensed Software Systems

While "pirated" operating systems and software are extremely common (especially for Windows) they often leave much to be desired in terms of security. If the OS or Software is not receiving regular updates from the software creator, it is extremely vulnerable to thousands of potential attacks. Switch to licensed software or recommended Free Open Source Software

If Outdated - Update Operating Systems and Other Software

Operating Systems and Softwares of all varieties - Windows, Mac, Linux, and others, are constantly being updated. These updates often fix bugs, but they also protect the system from newly discovered vulnerabilities. It can seem difficult to keep updating constantly, but this is very important to protect even non-sensitive systems.

If Vulnerable Software - Update Vulnerable Software

Many critical software components, such as Java or Adobe Flash, have many vulnerabilities and need to be aggressively updated. If there are not needed for work by the users, uninstall them

If No Anti-Virus and Anti-Malware Scanner - Install Anti-Virus and Anti-Maware Scanner

An Anti-virus and Anti-malware offer some minimal protection to the system and therefore is important to have them installed.

If Outdated Anti-Virus - Update Anti-Virus

Most AV tools automatically update, but this can sometimes get out of sync, or if the AV was a pre-installed trial system, it will stop updating after its trial period. An out of date anti-virus is worthless. Therefore ensure that continuous udpdating of AV is done.

If Unencrypted Drive - Encrypt Hard Drives

When possible, build-in drive encryption (Filevault on OSX, BitLockeron Windows, and LUKS on Linux) tend to offer the most seamless, user-friendly experiences. VeraCrypt offers free cross-platform drive encryption and cna also create encrypted drives which can be shared across platforms.

If Inactive firewall - Activate both personal and server firewall (If present)

Again, where present, use built-in firewalls and configure them for both office and public network options. Testing to ensure systems can still perform expected office natworking (file sharing, printing, etc.) is essential unless alternatives are created.

PASSWORD SECURITY SURVEY

Summary

Weak and "shared" passwords are prevalent - even after hundreds of well-publicized global password breaches, "password" and "12345" remain the most popular passwords. Weak wifi passwords are specifically a challenge, as wifi signals often are accessible outside of an office's physical limits, but provide full access to the private network.

Overview

- Using the password survey, determine the organization's baseline for password security
- If relevant, test the wireless network's password strength

Materials Needed

- For the (most common) WPA password-based attacks, an already-prepared dictionary of words to use to attack the password will be required. See the Appendix on Audit Preparation for guidance on dictionary preparation.
- A Password Survey (see Appendix) for an alternate way to gather password practices
- The Level Up Activity, Password Reverse Race provides a staff activity.

Considerations

Walkthrough

This exercise supports the auditor in building an effective dictionary that is customized to an organization.

This dictionary can then be used in a variety of ways:

- By using the examples referenced in the Network Access section, the auditor can attack weak wifi passwords, which present a non-personal and non-disruptive way to demonstrate password security problems. Weak wifi passwords are specifically a challenge, as wifi signals often are accessible outside of an office's physical limits, but provide full access to the private network.
- An Auditor can show or discuss their preferred customization strategy and the tools (like JtR) that automatically "mutate" passwords with numbers, capitals, and so on, to demnonstrate the power of a computer to quickly get around common "tricks"
- An Auditor can also use a password "survey" to get an understanding of password practices within the organization.

This skillset, plus demonstration against non-invasive accounts, provides an opening for a discussion with staff on password security. See Level Up for further activities and exercises around passwords.

- Download basic word lists
- Research dictionary needs
- Create custom word list
- Build core list(s)
- Attack a password hash using increasingly more time-consuming methods

This component provides resources and recommendations on cracking passwords - both the creation of dictionaries and rules to modify those dictionaries, as well as some basic implementation as well. This is a dangerous (and in many cases, illegal) skill to use, and should be more of a guide to auditors on what password security myths do not work against modern password cracking software, and to use only with permission and only in very specific situations as a demonstration of the power of even a common laptop against weak passwords.

Primarily for use in the Network Access component, building a password dictionary, understanding the ways to automatically mutate it, and running it against passwords is a useful skill to have, and to use to explain why simple passwords are insecure. This Ars Technica article provides a good insight into the path to tackle iterative password cracking using a variety of tools to meet different goals.

These instructions use a small set of password cracking tools, but many are possible. If there are tools you are more familiar or comfortable with using, these by no means are required. The only constraints are to be respectful and responsible, as well as keeping focused on the overall goals and not getting bogged down.

A good wordlist with a few tweaks tends to break most passwords. Using a collection of all English words, all words from the language of the organization being audited, plus a combination of all these words, plus relevant keywords, addresses, and years tends to crack most wifi passwords in a reasonable timeframe.

An approach which begins with quick, but often fruitful, attacks to more and more complex (and time consuming) attacks is the most rewarding. However, after an hour or two of password hacking, the in-office time on other activities is more valuable, so admit defeat and move on. See the Recommendations section for talking points around the levels of password cracking that exist in the world. You can work on passwords offline/overnight/post-audit for report completeness.

Here is a suggested path to take with suggested tools to help. You might try the first few steps in both the targeted keyword approach and the dictionary approach before moving on to the more complex mutations towards the end of each path.

- Targeted Keywords
- Begin with a simple combination of organizationally relevant keywords (using hashcat's combinator attack, combining your org keyword list with itself)
- Add in numbers/years (simple scripting, hashcat, JtR)
- Add in other mutators like 1337 replacements, capitalization tricks (John)

- Language dictionary attack (simple scripting, hashcat)
- Run a series of dictionary word attacks:
  - A simple language dictionary attack
  - Add in numbers/years (simple scripting, hashcat, JtR)
  - Add in the org keywords (a full combination creates a massive list, recommend starting with 1:1)
  - Try other combinations of the dictionary, keywords, years
  - Add in other mutators like 1337 replacements, capitalization tricks (John)
- Brute forcing (do not bother with this on-site)
- John's incremental modes, limited by types
- Crunch's raw brute-force attack (very, very time intensive - a complete waste of time without GPUs)

Dictionary Research and Creation

Before you arrive on-site it is important to have your password cracking tools downloaded and relevant dictionaries ready to go, as your main demonstration and use of these tools is to gain access to the organization's network. The effectiveness of this demonstration is drastically reduced if you already have had to ask for the password to connect to the Internet and update your dictionaries, tools, or so on. Some of these files (especially larger password dictionaries) can be quite large, so downloading them in-country is not recommended.

Many password dictionary sites, such as SkullSecurity , maintain core dictionaries in multiple languages. If your target language is not available, some quick regular expression work can turn spell-check dictionaries (such as those used by LibreOffice into useful word lists. It is generally useful to always test with English in addition to the target language.

CloudCracker and OpenWall have, for a fee, well-tested password dictionaries.

Keyword generation

In addition, create a customized dictionary with words related to the subject as revealed in the Remote Assessment research: organization name, street address, phone number, email domain, wireless network name, etc. For the organization "ExampleOrg , which has its offices at 123 Central St., Federal District, Countryzstan , which does human rights and journalism work and was founded in 1992, some context-based dictionary additions would be:

exampleorg
example
exa
mple
org
123
central
federal
district
countryzstan
human
rights
journo
journalism
1992
92

Also add common password fragments: qwerty, 1234/5/6/7/8, and, based on field experience, four-digit dates back to the year 2001 (plus adding in the founding year of the organization). It's also useful to see what calendar system is in use at your organization's location as some cultures don't use Gregorian years . It's quite amazing how often a recent year will be part of a wifi password -- this presentation discusses many common patterns in passwords: https://www.owasp.org/images/a/af/2011-Supercharged-Slides-Redman-OWASP-Feb.pdf

Optional Further steps

Use CeWL, to spider the organization's web properties to generate additional phrases. This list will need review, as some of the generated content is not very useful, but may be useful if the site is not in a language the auditor reads fluently.

For passwords other than WPA, specific policies or patterns may help to focus your password dictionary further. PACK, or Password Analysis and Cracking Toolkit is a collection of utilities developed to aid in analysis of password lists in order to enhance password cracking through pattern detection of masks, rules, character-sets and other password characteristics. The toolkit generates valid input files for Hashcat family of password crackers." PACK is most useful for large sets of passwords, where it can detect patterns in already-broken passwords to help build new rules. Both password cracking tools listed here are powerful, and have slightly different abilities. The auditor should choose the one they prefer and/or the one which has the features they desire for this job.

Combinator Attack with scripting and Hashcat

One quick way to build a more complex password list is to simply double the list up (a "combinator" attack), so that it includes an entry for each pair of these strings:

You can do a 1-way version of this list simply, such as:

```
$ for foo in `cat pwdlist.txt`; do for bar in `cat pwdlist.txt`; do printf $foo$bar'\n'; done; done > pwdpairs.txt
$ cat pwdlist.txt >> pwdpairs.txt
```

Hashcat can do this in a live attack under its "combinator" mode, and hashcat-utils (hiding in /usr/share/hashcat-utils/combinator.bin) provides this as a standalone tool. This provides a true combination of the list, so it exponentially increases the list size - use with caution, or use with one larger dictionary and one smaller dictionary.

For example, use these combination approach on your custom dictionary (combining it with itself, creating combinations from the above list such as example92, journorights, exampleorgrights).

```
$  /usr/share/hashcat-utils/combinator.bin dict.txt dict.txt
```

Hashcat is extremely powerful when you have desktop computer systems to use, but has a few wordlist manipulation tools that are useful regardless.

More References: (http://hashcat.net/wiki/doku.php?id=cracking_wpawpa2 , http://www.darkmoreops.com/2014/08/18/cracking-wpa2-wpa-with-hashcat-kali-linux/)

Word mutation with John the Ripper (JtR)

JtR is a powerful tool you can use in combination of existing wordlists, but it also can add in common substitutions (people using zero for the letter "o"). JtR can be used to generate a static list of passwords for other programs, or it can be used directly against a password database. JtR is a bit weak combining words within a wordlist, so you should apply your customizations and any folding before moving on to JtR.

You can add custom "rules" to aid in these substitutions - a base set is included with JtR, but a much more powerful set is added by [KoreLogic] (http://contest-2010.korelogic.com/rules.html). KoreLogic also provides a custom character set "chr file" that takes password frequency data from large collections of real-world passwords to speed up JtR's brute force mode . This PDF presentation has a good walkthrough of how John and Kore's rules work

Additional guides: * (http://linuxconfig.org/password-cracking-with-john-the-ripper-on-linux)

The bleeding-edge jumbo version combines both the built-in rules and an optimized version of the KoreLogic rules. This list of KoreLogic Rules provides nice descriptions of what the KoreLogic rules do. In bleeding-jumbo, you can remove "KoreLogicRules". BackReference provides a great example of rules usage.

Some particularly useful ones individual rulesets are: * AppendYears (appends years, from 1900 to 2019) and AppendCurrentYearSpecial (appends 2000-2019 with punctuation) * AddJustNumbers (adds 1-4 digits to the end of everything) * l33t (leet-speek combinations)

There are some build-in combinations of rulesets - for example, just --rules runs john's internal collection of default rules, and --rules:KoreLogic runs a collection of the KoreLogic rules in a thoughtful order, and --rules:all is useful if you hate life.

e.g. :

```
$ john -w:dictionary.txt --rules:AppendYears --stdout
```

Building custom rules

PROTIP Create a dictionary with just "blah" and run various rules against it to understand how each ruleset or combination works. Note specifically that each rule multiplies the size of the dictionary by the number of permutations it introduces. Running the KoreLogic ruleset combination against a **one word** dictionary creates a list of 6,327,540 permutations on just that word.

Brute force, using John and crunch

JtR's "incremental" mode is essentially an optimized brute force attack, so will take a very long time for anything but the shortest passwords, or passwords where you can limit the search space to a character set: "As of version 1.8.0, pre-defined incremental modes are "ASCII" (all 95 printable ASCII characters), "LM_ASCII" (for use on LM hashes), "Alnum" (all 62 alphanumeric characters), "Alpha" (all 52 letters), "LowerNum" (lowercase letters plus digits, for 36 total), "UpperNum" (uppercase letters plus digits, for 36 total), "LowerSpace" (lowercase letters plus space, for 27 total), "Lower" (lowercase letters), "Upper" (uppercase letters), and "Digits" (digits only). The supplied .chr files include data for lengths up to 13 for all of these modes except for "LM_ASCII" (where password portions input to the LM hash halves are assumed to be truncated at length 7) and "Digits" (where the supplied .chr file and pre-defined incremental mode work for lengths up to 20). Some of the many .chr files needed by these pre-defined incremental modes might not be bundled with every version of John the Ripper, being available as a separate download." (http://www.openwall.com/john/doc/MODES.shtml)

As a last resort, you can try a direct brute force attack overnight or post-audit to fill in details on key strength. Crunch is a very simple but thorough approach. Given enough time it will break a password, but it's not particularly fast, even at simple passwords. You can reduce the scope of this attack (and speed it up) if you have a reason to believe the password is all lower-case, all-numeric, or so on. WPA passwords are a minimum of 8 characters, a maximum of 16, and some wifi routers will accept punctuation, but in practice these are usually just !@#$. — so:

```
$ /path/to/crunch 8 16 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890$!@#$. | aircrack-ng -a 2 path/to/capture.pcap -b 00:11:22
```

This says to try every possible alpha-numeric combination from 8 to 16 characters. This will take a very, very, very long time.

Material that may be Useful:

Sample Practice For practice on any of these methods, you can use the wpa-Induction.pcap file from Wireshark.

https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

http://zed0.co.uk/crossword/

http://www.instantcheckmate.com/crimewire/is-your-password-really-protecting-you/#lightbox/0/

Note that password cracking systems are rated on the number of password guesses they make per second. Stock laptop computers without high-end graphics cards or any other optimizations can guess 2500 passwords/second. More powerful desktop computers can test over a hundred million each second, and with graphics cards (GPUs) that rises to billions of

passwords per second. (https://en.wikipedia.org/wiki/Password_cracking).

This website has a good explanation about how improving the complexity of a password affects how easy it is to break: http://www.lockdown.co.uk/?pg=combi, but is using very out of date numbers - consider a basic laptop able to produce "Class E" attacks, and a desktop, "Class F"

http://rumkin.com/tools/password/passchk.php

http://cyber-defense.sans.org/blog/downloads/ has a calculator buried in the zip file "scripts.zip"

http://www.dailymail.co.uk/sciencetech/article-2331984/Think-strong-password-Hackers-crack-16-character-passwords-hour.html

https://www.grc.com/haystack.htm

https://www.owasp.org/images/a/af/2011-Supercharged-Slides-Redman-OWASP-Feb.pdf

http://www.nytimes.com/2014/11/19/magazine/the-secret-life-of-passwords.html?_r=1

Recommendation

Materials that may be useful

Password Survey

How many passwords do you have to remember for accounts and devices used to do your work?

- [ ] No
- [ ] Yes

If you tried to login to your computer account right now, how many attempts do you think it would take?

- [ ] No
- [ ] Yes

To how many people have you given your current password?

- [ ] No
- [ ] Yes

Have you ever forgotten your current password?

- [ ] No
- [ ] Yes

If yes, how did you recover it?

Have you ever forgotten old work passwords?

- [ ] No
- [ ] Yes

If yes, how did you recover it?

When you created your current password, which of the following did you do?

- [ ] I reused an old password
- [ ] I modified an old password
- [ ] I reused a password I was already using for a different account
- [ ] I created an entirely new password
- [ ] Other:

Did you use any of the following strategies to create your current password (choose all that apply) ?

- [ ] Password based on the first letter of each word in a phrase
- [ ] Based on the name of someone or something
- [ ] Based on a word or name with numbers / symbols added to beginning or end
- [ ] Based on a word or name with numbers and symbols substituting for some of the letters (e.g. '@' instead of 'a')
- [ ] Based on a word or name with letters missing
- [ ] Based on a word in a language other than English
- [ ] Based on a phone number
- [ ] Based on an address
- [ ] Based on a birthday

How long is your current password (total number of characters)?

- [ ] I prefer not to answer.

What symbols (characters other than letters and numbers) are in your password?

- [ ] I prefer not to answer.

How many lower-case letters are in your current password?

- [ ] I prefer not to answer.

How many upper-case letters are in your current password?

- [ ] I prefer not to answer.

In which positions in your password are the numbers?

- [ ] I prefer not to answer.
- [ ] First
- [ ] Second
- [ ] Second from last
- [ ] Last
- [ ] No Numbers
- [ ] I prefer not to answer.

In which positions in your password are the symbols?

- [ ] I prefer not to answer.
- [ ] First
- [ ] Second
- [ ] Second from last
- [ ] Last
- [ ] No Numbers
- [ ] I prefer not to answer.

Have you written down your current password?

- [ ] No
- [ ] Yes, on paper

- [ ] Yes, electronically (stored in computer, phone, etc.)
- [ ] Other

If you wrote down your current password how is it protected (choose all that apply) ?

- [ ] I do not protect it
- [ ] I stored it in an encrypted file
- [ ] I hid it
- [ ] I stored it on a computer or device protected with another password
- [ ] I locked up the paper
- [ ] I always keep the password with me
- [ ] I wrote down a reminder instead of the actual password
- [ ] Other

Do you have a set of passwords you reuse in different places?

- [ ] No
- [ ] Yes

Do you have a password that you use for different accounts with a slight modification for each account?

- [ ] No
- [ ] Yes

A DAY IN THE LIFE

Covered in full in User Device Assessment:

- Integrated with other activities/interactions, interview staff on their usage of technology and remote services

NETWORK MAPPING

Covered in full in Network Mapping

- Scan the network for all connected devices
- Review device information and open services for potential vulnerabilities
- Using beacons and other data, map devices to users.
- Scan select external services (particularly self-hosted webmail/email servers and other extranet services) to detect possible unencrypted but sensitive connection possibilities
- Enumerate shared directories on the network and check for access controls

PHYSICAL SECURITY GUIDED TOUR

Covered in full in Physical Assessment:

Have your point of contact walk you around the office (often as part of introductions on the first day) - mentally note physical security concerns. Document how difficult it would be for a visitor or after-hours break-in to access sensitive systems. Identify physical assets with sensitive content, such as:

- Networking equipment and servers
- User devices (workstations/laptops, smarthpones, USB drives)
- Sensitive information or external storage drives lying on desks
- Accounts/passwords written on post-its, white-boards, etc.
- Unattended, logged in computers
- Unlocked cabinets, computer rooms, or wiring closets
- Network ports that are not in use, especially ones not in plain sight

This can be done remotely via secure videoconference over a smartphone or tablet that can moved around the office easily.

Combining this activity with Office Mapping helps to reduce the awkwardness of taking notes while walking around the office, and if being done remotely, the two separate activities can be used to cross-verify the accuracy of each.

USER DEVICE ASSESSMENT

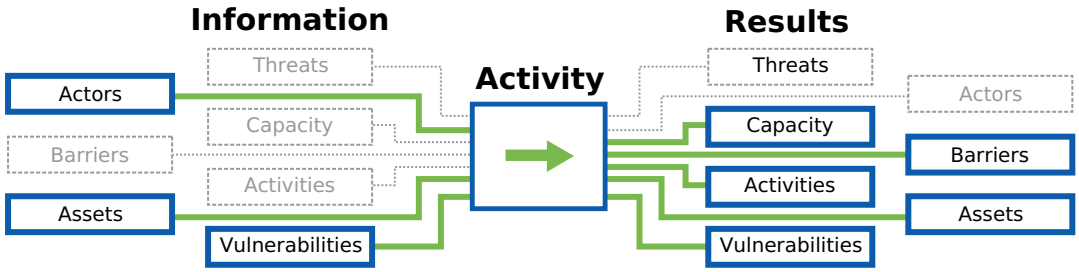
SUMMARY

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.

THE FLOW OF INFORMATION



User Device Assessment Information Flow

GUIDING QUESTIONS

- What work and personal devices do staff use to accomplish their work, store work related files, or engage in work communications?
- What organizational and external/personal services do staff use to accomplish their work, store work related files, or engage in work communications?
- What are the organizational processes that staff take part in and the tools and communication channels that are used in those process'?
- What are the existing in/formal security practices that the participants use to address risks.

APPROACHES

- **Conduct a Hands on Device Interview/Audit:** Inspect and record information on user devices (work & personal) for security concerns (patch levels, user privileges, drive encryption, ports/services running, anti-virus capabilities)
- **Password User Survey:** Have staff take the password use survey for ALL devices used for work. [50,51]
- **A Day In the Life:** Have staff walk you through a usual "day in their life" showing you what devices they use, how they use them, and what data they have to interact with to conduct their work.

OUTPUTS

- 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.)

OPERATIONAL SECURITY

- Treat device assessment data as well as any additional service information learned with the utmost security

PREPARATION

Baseline Skills

- Basic systems administration experience for common operating systems

RESOURCES

- *Guidelines:* "Guidelines on Firewalls and Firewall Policy" (NIST 800-41)
- *Benchmarks:* "Security Configuration Benchmarks" (CIS Security Benchmarks)
- *Repository:* "National Checklist Program Repository - Prose security checklists" (National Vulnerability Database)
- *Security Guidance:* "Operating Systems Security Guidance" (NSA)
- *Windows Utility:* "HardenTools" (Security Without Borders)

Password Security

- *Guide:* "How to Teach Humans to Remember Really Complex Passwords" (Wired)
- *Guide:* "Security on Passwords and User Awareness" (HashTag Security)
- *Video:* "What's wrong with your pa$$w0rd?" (TED)
- *Article:* "Password Security: Why the horse battery staple is not correct" (Diogo Mónica)
- *Organization:* "Passwords Research" (The CyLab Usable Privacy and Security Laboratory (CUPS))
- *Guide:* "Hacker Lexicon: What Is Password Hashing?" (Wired)
- *Guide:* "7 Password Experts on How to Lock Down Your Online Security" (Wired)

Privilege Separation Across OS

- identify what privileges services are running as
- identify is the admin user is called admin or root
- Identify if users are logging in and installing software as admin.

Examining Firewalls Across OS

- *Checklist:* "Firewall Configuration Checklist." (NetSPI)

Identifying Software Versions

Device Encryption By OS

- Identifying if a device is using encryption by OS
- Encryption availablility by OS
- Encryption Guides

Anti-Virus Updates

Identifying Odd/One-Off Services

ACTIVITIES

DEVICE AND BEHAVIOUR ASSESSMENT

Summary

The auditor checks staff devices for updated systems and software, anti-virus and other security capabilities, and identifies software running on computers and its current version. The auditor checks for known vulnerabilities to any out of date software.

This is used to develop a report component exposing how un-updated software can lead to large vulnerabilities.

Overview

- Identify what privilege level services are running under -- Are users using accounts with admin privelges, or are they using another user and have to type in a password to get admin rights? [52]
- Check for existence and status of anti-virus (and anti-malware tools) on the device. [53]
- Record the version and patch levels of software on the device. [54]
- Identify what level of encryption is being used and is available for data storage on the device. [55]
- Using the list of software versions and patches identify attacks and, if possible, identified malware that devices in the office are vulnerable to.

Materials Needed

- A notepad may be useful

Considerations

- Communicate with the staff members the level of confidentiality you are treating discussions around their device and technology usage with - i.e. explain what incident response triggers you have agreed upon with the organization, and that anything not triggering that is to be only reported in aggregate.

Walkthrough

The auditor inspects a subset of key and/or representative user devices (work & personal). The auditor should focus on the work devices to limit scope creep, but if the office has many personal devices accessing organizational accounts/data, the auditor should share what "red flags" they are looking for and work in tandem with device owners and/or IT staff. For a small office, it may be possible to check every machine. For larger offices, the auditor should use a subset to get a feel for the overall security stance of user devices.

As you work with staff members, also interview them about the other devices they use such as phones and tablets, and how they connect to work services - email/webmail, chat Apps, intra/extranet tools, Constituent Relationship Management (CRM) tools like CiviCRM or Salesforce, financial tracking tools, and website management tools.

Below is a checklist to assist in checking across different platforms/versions for common security needs.

OSX

- OS Security Updates

- Firewall
  - See http://support.apple.com/en-us/HT1810 for cross-version guidance
  - (GUI) Choose System Preferences from the Apple menu, Security (10.5 and before) or Security & Privacy (10.6 and later), then the Firewall tab.
- Anti-Virus Version
  -
- User privilege
  -
- Drive Encryption
- CLI. sudo fdesetup status
- (GUI) Choose System Preferences from the Apple menu, Security (10.5 and before) or Security & Privacy (10.6 and later), then the FileVault tab.
- (VeraCrypt)
- Services Running
- (Command line) sudo launchctl list
- (Command line) ps -ef

- (GUI) The "Activity Monitor" application is located in /Applications/Utilities provides a similar interface to "top"

Windows

If Windows is not your primary OS, you can download sample Virtual Machines (with time limitations) from Microsoft through their project to improve IE support via https://www.modern.ie/en-us/virtualization-tools#downloads (see also http://www.makeuseof.com/tag/download-windows-xp-for-free-and-legally-straight-from-microsoft-si/ and https://modernievirt.blob.core.windows.net/vhd/virtualmachine_instructions_2014-01-21.pdf)

Windows 10

- OS Security Updates
- Start --Settings --Update & Security --Windows Update
- Firewall
- Start, type Firewall (select Windows Firewall)
- Privacy
- Start --Settings -- Privacy
- Anti-Virus Version
-
- Privacy
- (GUI) Start --Settings -- Privacy
- User privilege
- Start, type 'User Account', select "Change User Account Control settings"
- Drive Encryption
- (Bitlocker), https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-device-encryption-overview-windows-10
- Services Running
- Start, type "Task Manager"

Windows 8

- OS Security Updates
- Firewall
- (GUI) Start (or Down Arrow Icon, PC Settings) -- Control Panel -- Windows Firewall
- CLI. Netsh Advfirewall show allprofiles
- (more detail: http://windows.microsoft.com/en-us/windows-8/windows-firewall-from-start-to-finish)
- Anti-Virus Version
-
- User privilege

-
- Drive Encryption
-
- https://diskcryptor.net/wiki/Main_Page
- Services Running
- Right-Click on bottom taskbar, select "Task Manager"

Installed updates

Control Panel Programs and features installed updates CLI: http://www.techsupportalert.com/en/quick-and-easy-way-list-all-windows-updates-installed-your-system.htm

Windows 7

In Windows 7, (GUI) Control Panel -- All Control Panel Items -- Action Center (Security tab) provides a quick run-down of most security features installed and their update status. It does not show drive encryption or specific versions.

- OS Security Updates
-
- Firewall
- (GUI) Control Panel -- All Control Panel Items -- Windows Firewall
- CLI. Netsh Advfirewall show allprofiles
- Anti-Virus Version
-
- User privilege
- (GUI) Control Panel -- All Control Panel Items -- User Accounts and checking also the User Account Control settings.
- Drive Encryption
- (GUI) Control Panel -- All Control Panel Items -- BitLocker Drive Encryption
- (VeraCrypt) , https://diskcryptor.net/wiki/Main_Page
- Services Running
- CLI. tasklist
- (GUI) Right-click on task bar, select "Start Task Manager"
- (Advanced) Use TechNet/SysInternal's Process Explorer: http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

Windows XP

If user is still operating on windows XP, recommendation is to upgrade to later windows. Windows XP is no longer supported and is not receiving security updates: https://www.microsoft.com/windows/en-us/xp/end-of-xp-support.aspx

If there is an organizationally critical system relying on Windows XP, removing it from the network and carefully managing data exchange with it may provide a bridge solution until a replacement process can be funded and rolled out.

Linux

- Firewall
- CLI. sudo iptables -L -n
- CLI. (Ubuntu, and only if installed) sudo ufw status
- (GUI) (Ubuntu, and only if installed) gufw
- Anti-Virus Version
- CLI. deb: dpkg-query -l | grep virus rpm: yum list installed | grep virus
- See also: https://en.wikipedia.org/wiki/Linux_malware#Anti-virus_applications
- User privilege
- CLI. groups
- Drive Encryption
-
- (VeraCrypt)

- Services Running
- CLI. ps -ef
- CLI. top

Recommendation

If Unsupported Operating System - Upgrade to Recent Version

Popular operating systems like Windows XP are, sadly, no longer receiving security updates. Upgrade to the latest version keeping in mind the system requirements of the version selected

While "pirated" operating systems and software are extremely common (especially for Windows) they often leave much to be desired in terms of security. If the OS or Software is not receiving regular updates from the software creator, it is extremely vulnerable to thousands of potential attacks. Switch to licensed software or recommended Free Open Source Software

If Pirated Software - Move to Licensed Software Systems

While "pirated" operating systems and software are extremely common (especially for Windows) they often leave much to be desired in terms of security. If the OS or Software is not receiving regular updates from the software creator, it is extremely vulnerable to thousands of potential attacks. Switch to licensed software or recommended Free Open Source Software

If Outdated - Update Operating Systems and Other Software

Operating Systems and Softwares of all varieties - Windows, Mac, Linux, and others, are constantly being updated. These updates often fix bugs, but they also protect the system from newly discovered vulnerabilities. It can seem difficult to keep updating constantly, but this is very important to protect even non-sensitive systems.

If Vulnerable Software - Update Vulnerable Software

Many critical software components, such as Java or Adobe Flash, have many vulnerabilities and need to be aggressively updated. If there are not needed for work by the users, uninstall them

If No Anti-Virus and Anti-Malware Scanner - Install Anti-Virus and Anti-Maware Scanner

An Anti-virus and Anti-malware offer some minimal protection to the system and therefore is important to have them installed.

If Outdated Anti-Virus - Update Anti-Virus

Most AV tools automatically update, but this can sometimes get out of sync, or if the AV was a pre-installed trial system, it will stop updating after its trial period. An out of date anti-virus is worthless. Therefore ensure that continuous udpdating of AV is done.

If Unencrypted Drive - Encrypt Hard Drives

When possible, build-in drive encryption (Filevault on OSX, BitLockeron Windows, and LUKS on Linux) tend to offer the most seamless, user-friendly experiences. VeraCrypt offers free cross-platform drive encryption and cna also create encrypted drives which can be shared across platforms.

If Inactive firewall - Activate both personal and server firewall (If present)

Again, where present, use built-in firewalls and configure them for both office and public network options. Testing to ensure systems can still perform expected office natworking (file sharing, printing, etc.) is essential unless alternatives are created.

A DAY IN THE LIFE

Summary

The auditor checks staff devices for updated systems and software, anti-virus and other security capabilities, and identifies software runing on computers and its current version. The auditor checks for known vulnerabilities to any out of date software.

This is used to develop a report component exposing how un-updated software can lead to large vulnerabilities.

Overview

- Integrated with other activities/interactions, interview staff on their usage of technology and remote services

Materials Needed

Considerations

- Communicate with the staff members the level of confidentiality you are treating discussions around their device and technology usage with - i.e. explain what incident response triggers you have agreed upon with the organization, and that anything not triggering that is to be only reported in aggregate.

Walkthrough

As you work with staff members (this pairs well with the device checklist activity), also interview them about the other devices they use, and how they connect to work services - email/webmail, intra/extranet tools, Constituent Relationship Management (CRM) tools like CiviCRM or Salesforce, financial tracking tools, and website management tools.

Phone Usage

- Work Email
- Work Calls
- Chat Apps with partners/work related

User Software and Tools

- Email software
- Calendars
- Shared Files inside the office
- Other shared file systems
- Chat
- Voice calls
- Program tracking software
- Financial

- Progress
- Databases
- intranet
- extranet / other sites?

Remote Services

- Dropbox
- Work Email
- Websites and blogs
- Social media
- Online CRM or mass-mailing tools (SalesForce, CiviCRM, MailChimp...)

Recommendation

Only use services with "SSL" encryption ("HTTPS"), and consider adding HTTPS Everywhere to browsers. This does not itself guarantee protection from all attacks, but it is a good first-step in protecting information (such as passwords or email) in transit from your computer to the service provider.

FIREWIRE ACCESS TO ENCRYPTED/LOCKED COMPUTERS

Summary

Firewire ports and expansion slots can be abused to obtain data that are thought to be encrypted

Any attacker who obtains a running (including sleeping and hibernating!) Windows, Mac, or even Linux laptop with a Firewire port, an ExpressCard expansion slot, or a Thunderbolt port will be able to read, record or modify any sensitive information on the device, even if the screen is “locked” and the information is stored on an encrypted volume or in an encrypted folder. This applies to threats involving loss, theft and confiscation, but also to “checkpoint” scenarios in which the attacker may only have access for a few minutes.

This attack requires physical control of a machine that is not powered off. Full details of the scope of the attack are available at http://www.breaknenter.org/projects/inception/ .

Overview

Materials Needed

- A system with a firewire port, a thunderbolt port, or a PCMCIA slot and a firewire card. See http://www.breaknenter.org/projects/inception/#Requirements

Considerations

Walkthrough

Firewire ports and expansion slots can be abused to obtain data that are thought to be encrypted

The threat describe in this section is more complex than it needs to be. In fact, unencrypted data are vulnerable to any number of simple attacks, the two most straightforward being: 1) rebooting the computer from a USB stick CD-ROM or DVD containing an alternate operating system, then copying all of the data; or 2) removing the hard drive, inserting it into a different machine, then copying all of the data. These techniques, which work on nearly any computer, even if a strong login password has been set, are effective and widely used, but they require extended physical access to the device. A slightly different attack is described below, one that only requires physical access for a few minutes. It, too, works regardless of login/screen-lock passwords, though only devices with Firewire ports or expansion slots (ExpressCard, CardBus, PCMCIA, etc.) are vulnerable.

The steps required to defend against all of these threats is the same: encrypt your data using a tool like Microsoft's BitLocker, Apple's FileVaule or the open-source Truecrypt application. The Firewire attack highlighted here is particularly illustrative, however, because it serves as a reminder that merely setting up an encrypted volume is not enough. In much the same way that a lock does little to protect your home if the door to which it is attached remains open, data encryption is rarely effective while you are logged into your computer. Even if the screen is locked (which would foil the "reboot" and "hard drive removal" attacks described briefly above), an attacker may still find a way to access your sensitive data, while the computer is up and running, because the decryption key is present in the computer's memory. (This is how large-scale encryption actually works. Information remains encrypted at all times, on the storage device where it lives, but you are able to access it while you are logged in, or while your encrypted volume is "open," because your computer decrypts and encrypts it on the fly.) Walkthrough

Step 1: First, the attacker would connect her computer to the victim's using a Firewire cable. Either or both machines could be using a true Firewire port or a Firewire expansion card. When a Firewire ExpressCard expansion card is inserted, Windows automatically installs and configures the necessary drivers, even if nobody is logged into the laptop.

Step 2: Once connected, the attacker simply runs the Inception tool, selects the operating system of the target machine and waits a minute or two for the attack to complete (depending on the amount of RAM present):

```
$ incept

 _|  _|    _|   _|_|_| _|_|_|_| _|_|_|   _|_|_| _|   _|_|   _|    _|
 _|  _|_|   _| _|     _|     _|   _|   _|   _| _|   _| _|_|   _|
 _|  _|  _| _| _|     _|_|_|   _|_|_|    _|   _| _|   _| _| _| _|
 _|  _|   _|_| _|     _|     _|       _|   _| _|   _| _|   _|_|
 _|  _|    _|   _|_|_| _|_|_|_| _|       _|   _|   _|_|   _|    _|

v.0.2.0 (C) Carsten Maartmann-Moe 2012
Download: http://breaknenter.org/projects/inception | Twitter: @breaknenter

[*] FireWire devices on the bus (names may appear blank):
------------------------------------------------------------------------------
[1] Vendor (ID): MICROSOFT CORP. (0x50f2) | Product (ID):  (0x0)
------------------------------------------------------------------------------
[*] Only one device present, device auto-selected as target
[*] Selected device: MICROSOFT CORP.
[*] Available targets:
------------------------------------------------------------------------------
[1] Windows 8: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[2] Windows 7: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[3] Windows Vista: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[4] Windows XP: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[5] Mac OS X: DirectoryService/OpenDirectory unlock/privilege escalation
[6] Ubuntu: libpam unlock/privilege escalation
------------------------------------------------------------------------------
[!] Please select target (or enter 'q' to quit): 2
[*] Selected target: Windows 7: msv1_0.dll MsvpPasswordValidate unlock/privilege escalation
[*] Initializing bus and enabling SBP-2, please wait  1 seconds or press Ctrl+C
[*] DMA shields should be down by now. Attacking...
[*] Searching, 1328 MiB so far
[*] Signature found at 0x8b50c321 (in page # 570636)
[*] Write-back verified; patching successful
```

[*] BRRRRRRRAAAAAWWWWRWRRRMRMRMMRMRMMMM!!!

In the case of the laptops tested, Inception took approximately two minutes to reach the final, somewhat self-congratulatory line shown above. At that point, we were able to login using any password. (Entering "asdf" worked just fine, and gave us full access to all data on the computer.) Inception works by temporarily replacing authentication code using the Firewire's protocol's direct memory access (DMA). After a reboot, everything is restored to its original state.

Once again, it is worth noting that successful mitigation of this issue requires a combination of technology (data encryption) and some level of behavior change (shutting down laptops at the end of the day, when traveling and at any time when confiscation, theft, loss or tampering are particularly likely.)

Material that may be Useful:

Recommendation

PASSWORD SECURITY SURVEY

Summary

Weak and "shared" passwords are prevalent - even after hundreds of well-publicized global password breaches, "password" and "12345" remain the most popular passwords. Weak wifi passwords are specifically a challenge, as wifi signals often are accessible outside of an office's physical limits, but provide full access to the private network.

Overview

- Using the password survey, determine the organization's baseline for password security
- If relevant, test the wireless network's password strength

Materials Needed

- For the (most common) WPA password-based attacks, an already-prepared dictionary of words to use to attack the password will be required. See the Appendix on Audit Preparation for guidance on dictionary preparation.
- A Password Survey (see Appendix) for an alternate way to gather password practices
- The Level Up Activity, Password Reverse Race provides a staff activity.

Considerations

Walkthrough

This exercise supports the auditor in building an effective dictionary that is customized to an organization.

This dictionary can then be used in a variety of ways:

- By using the examples referenced in the Network Access section, the auditor can attack weak wifi passwords, which present a non-personal and non-disruptive way to demonstrate password security problems. Weak wifi passwords are specifically a challenge, as wifi signals often are accessible outside of an office's physical limits, but provide full access to the private network.
- An Auditor can show or discuss their preferred customization strategy and the tools (like JtR) that automatically

"mutate" passwords with numbers, capitals, and so on, to demnonstrate the power of a computer to quickly get around common "tricks"
- An Auditor can also use a password "survey" to get an understanding of password practices within the organization.

This skillset, plus demonstration against non-invasive accounts, provides an opening for a discussion with staff on password security. See Level Up for further activities and exercises around passwords.

- Download basic word lists
- Research dictionary needs
- Create custom word list
- Build core list(s)
- Attack a password hash using increasingly more time-consuming methods

This component provides resources and recommendations on cracking passwords - both the creation of dictionaries and rules to modify those dictionaries, as well as some basic implementation as well. This is a dangerous (and in many cases, illegal) skill to use, and should be more of a guide to auditors on what password security myths do not work against modern password cracking software, and to use only with permission and only in very specific situations as a demonstration of the power of even a common laptop against weak passwords.

Primarily for use in the Network Access component, building a password dictionary, understanding the ways to automatically mutate it, and running it against passwords is a useful skill to have, and to use to explain why simple passwords are insecure. This Ars Technica article provides a good insight into the path to tackle iterative password cracking using a variety of tools to meet different goals.

These instructions use a small set of password cracking tools, but many are possible. If there are tools you are more familiar or comfortable with using, these by no means are required. The only constraints are to be respectful and responsible, as well as keeping focused on the overall goals and not getting bogged down.

A good wordlist with a few tweaks tends to break most passwords. Using a collection of all English words, all words from the language of the organization being audited, plus a combination of all these words, plus relevant keywords, addresses, and years tends to crack most wifi passwords in a reasonable timeframe.

An approach which begins with quick, but often fruitful, attacks to more and more complex (and time consuming) attacks is the most rewarding. However, after an hour or two of password hacking, the in-office time on other activities is more valuable, so admit defeat and move on. See the Recommendations section for talking points around the levels of password cracking that exist in the world. You can work on passwords offline/overnight/post-audit for report completeness.

Here is a suggested path to take with suggested tools to help. You might try the first few steps in both the targeted keyword approach and the dictionary approach before moving on to the more complex mutations towards the end of each path.

- Targeted Keywords
- Begin with a simple combination of organizationally relevant keywords (using hashcat's combinator attack, combining your org keyword list with itself)
- Add in numbers/years (simple scripting, hashcat, JtR)
- Add in other mutators like 1337 replacements, capitalization tricks (John)
- Language dictionary attack (simple scripting, hashcat)
- Run a series of dictionary word attacks:
    - A simple language dictionary attack
    - Add in numbers/years (simple scripting, hashcat, JtR)
    - Add in the org keywords (a full combination creates a massive list, recommend starting with 1:1)
    - Try other combinations of the dictionary, keywords, years
    - Add in other mutators like 1337 replacements, capitalization tricks (John)
- Brute forcing (do not bother with this on-site)
- John's incremental modes, limited by types
- Crunch's raw brute-force attack (very, very time intensive - a complete waste of time without GPUs)

Dictionary Research and Creation

Before you arrive on-site it is important to have your password cracking tools downloaded and relevant dictionaries ready to go, as your main demonstration and use of these tools is to gain access to the organization's network. The effectiveness of this demonstration is drastically reduced if you already have had to ask for the password to connect to the Internet and update your dictionaries, tools, or so on. Some of these files (especially larger password dictionaries) can be quite large, so downloading them in-country is not recommended.

Many password dictionary sites, such as SkullSecurity , maintain core dictionaries in multiple languages. If your target language is not available, some quick regular expression work can turn spell-check dictionaries (such as those used by LibreOffice into useful word lists. It is generally useful to always test with English in addition to the target language.

CloudCracker and OpenWall have, for a fee, well-tested password dictionaries.

Keyword generation

In addition, create a customized dictionary with words related to the subject as revealed in the Remote Assessment research: organization name, street address, phone number, email domain, wireless network name, etc. For the organization "ExampleOrg , which has its offices at 123 Central St., Federal District, Countryzstan , which does human rights and journalism work and was founded in 1992, some context-based dictionary additions would be:

exampleorg
example
exa
mple
org
123
central
federal
district
countryzstan
human
rights
journo
journalism
1992
92

Also add common password fragments: qwerty, 1234/5/6/7/8, and, based on field experience, four-digit dates back to the year 2001 (plus adding in the founding year of the organization). It's also useful to see what calendar system is in use at your organization's location as some cultures don't use Gregorian years . It's quite amazing how often a recent year will be part of a wifi password -- this presentation discusses many common patterns in passwords: https://www.owasp.org/images/a/af/2011-Supercharged-Slides-Redman-OWASP-Feb.pdf

Optional Further steps

Use CeWL, to spider the organization's web properties to generate additional phrases. This list will need review, as some of the generated content is not very useful, but may be useful if the site is not in a language the auditor reads fluently.

For passwords other than WPA, specific policies or patterns may help to focus your password dictionary further. PACK, or Password Analysis and Cracking Toolkit is a collection of utilities developed to aid in analysis of password lists in order to enhance password cracking through pattern detection of masks, rules, character-sets and other password characteristics. The toolkit generates valid input files for Hashcat family of password crackers." PACK is most useful for large sets of passwords, where it can detect patterns in already-broken passwords to help build new rules. Both password cracking tools listed here are powerful, and have slightly different abilities. The auditor should choose the one they prefer and/or the one which has the features they desire for this job.

Combinator Attack with scripting and Hashcat

One quick way to build a more complex password list is to simply double the list up (a "combinator" attack), so that it includes an entry for each pair of these strings:

You can do a 1-way version of this list simply, such as:

```
$ for foo in `cat pwdlist.txt`; do for bar in `cat pwdlist.txt`; do printf $foo$bar"\n"; done; done > pwdpairs.txt
$ cat pwdlist.txt >> pwdpairs.txt
```

Hashcat can do this in a live attack under its "combinator" mode, and hashcat-utils (hiding in /usr/share/hashcat-utils/combinator.bin) provides this as a standalone tool. This provides a true combination of the list, so it exponentially increases the list size - use with caution, or use with one larger dictionary and one smaller dictionary.

For example, use these combination approach on your custom dictionary (combining it with itself, creating combinations from the above list such as example92, journorights, exampleorgrights).

```
$  /usr/share/hashcat-utils/combinator.bin dict.txt dict.txt
```

Hashcat is extremely powerful when you have desktop computer systems to use, but has a few wordlist manipulation tools that are useful regardless.

More References: (http://hashcat.net/wiki/doku.php?id=cracking_wpawpa2 , http://www.darkmoreops.com/2014/08/18/cracking-wpa2-wpa-with-hashcat-kali-linux/)

Word mutation with John the Ripper (JtR)

JtR is a powerful tool you can use in combination of existing wordlists, but it also can add in common substitutions (people using zero for the letter "o"). JtR can be used to generate a static list of passwords for other programs, or it can be used directly against a password database. JtR is a bit weak combining words within a wordlist, so you should apply your customizations and any folding before moving on to JtR.

You can add custom "rules" to aid in these substitutions - a base set is included with JtR, but a much more powerful set is added by [KoreLogic] (http://contest-2010.korelogic.com/rules.html). KoreLogic also provides a custom character set "chr file" that takes password frequency data from large collections of real-world passwords to speed up JtR's brute force mode . This PDF presentation has a good walkthrough of how John and Kore's rules work

Additional guides: * (http://linuxconfig.org/password-cracking-with-john-the-ripper-on-linux)

The bleeding-edge jumbo version combines both the built-in rules and an optimized version of the KoreLogic rules. This list of KoreLogic Rules provides nice descriptions of what the KoreLogic rules do. In bleeding-jumbo, you can remove "KoreLogicRules". BackReference provides a great example of rules usage.

Some particularly useful ones individual rulesets are: * AppendYears (appends years, from 1900 to 2019) and AppendCurrentYearSpecial (appends 2000-2019 with punctuation) * AddJustNumbers (adds 1-4 digits to the end of everything) * l33t (leet-speek combinations)

There are some build-in combinations of rulesets - for example, just --rules runs john's internal collection of default rules, and --rules:KoreLogic runs a collection of the KoreLogic rules in a thoughtful order, and --rules:all is useful if you hate life.

e.g. :

```
$ john -w:dictionary.txt --rules:AppendYears --stdout
```

Building custom rules

PROTIP Create a dictionary with just "blah" and run various rules against it to understand how each ruleset or combination works. Note specifically that each rule multiplies the size of the dictionary by the number of permutations it introduces. Running the KoreLogic ruleset combination against a **one word** dictionary creates a list of 6,327,540 permutations on just that word.

Brute force, using John and crunch

JtR's "incremental" mode is essentially an optimized brute force attack, so will take a very long time for anything but the shortest passwords, or passwords where you can limit the search space to a character set: "As of version 1.8.0, pre-defined incremental modes are "ASCII" (all 95 printable ASCII characters), "LM_ASCII" (for use on LM hashes), "Alnum" (all 62 alphanumeric characters), "Alpha" (all 52 letters), "LowerNum" (lowercase letters plus digits, for 36 total), "UpperNum" (uppercase letters plus digits, for 36 total), "LowerSpace" (lowercase letters plus space, for 27 total), "Lower" (lowercase letters), "Upper" (uppercase letters), and "Digits" (digits only). The supplied .chr files include data for lengths up to 13 for all of these modes except for "LM_ASCII" (where password portions input to the LM hash halves are assumed to be truncated at length 7) and "Digits" (where the supplied .chr file and pre-defined incremental mode work for lengths up to 20). Some of the many .chr files needed by these pre-defined incremental modes might not be bundled with every version of John the Ripper, being available as a separate download." (http://www.openwall.com/john/doc/MODES.shtml)

As a last resort, you can try a direct brute force attack overnight or post-audit to fill in details on key strength. Crunch is a very simple but thorough approach. Given enough time it will break a password, but it's not particularly fast, even at simple passwords. You can reduce the scope of this attack (and speed it up) if you have a reason to believe the password is all lower-case, all-numeric, or so on. WPA passwords are a minimum of 8 characters, a maximum of 16, and some wifi routers will accept punctuation, but in practice these are usually just !@#$. — so:

```
$ /path/to/crunch 8 16 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890$!@#$. | aircrack-ng -a 2 path/to/capture.pcap -b 00:11:22
```

This says to try every possible alpha-numeric combination from 8 to 16 characters. This will take a very, very, very long time.

Material that may be Useful:

Sample Practice For practice on any of these methods, you can use the wpa-Induction.pcap file from Wireshark.

https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

http://zed0.co.uk/crossword/

http://www.instantcheckmate.com/crimewire/is-your-password-really-protecting-you/#lightbox/0/

Note that password cracking systems are rated on the number of password guesses they make per second. Stock laptop computers without high-end graphics cards or any other optimizations can guess 2500 passwords/second. More powerful desktop computers can test over a hundred million each second, and with graphics cards (GPUs) that rises to billions of passwords per second. (https://en.wikipedia.org/wiki/Password_cracking).

This website has a good explanation about how improving the complexity of a password affects how easy it is to break: http://www.lockdown.co.uk/?pg=combi, but is using very out of date numbers - consider a basic laptop able to produce "Class E" attacks, and a desktop, "Class F"

http://rumkin.com/tools/password/passchk.php

http://cyber-defense.sans.org/blog/downloads/ has a calculator buried in the zip file "scripts.zip"

http://www.dailymail.co.uk/sciencetech/article-2331984/Think-strong-password-Hackers-crack-16-character-passwords-hour.html

https://www.grc.com/haystack.htm

https://www.owasp.org/images/a/af/2011-Supercharged-Slides-Redman-OWASP-Feb.pdf

http://www.nytimes.com/2014/11/19/magazine/the-secret-life-of-passwords.html?_r=1

Recommendation

Materials that may be useful

Password Survey

How many passwords do you have to remember for accounts and devices used to do your work?

- [ ] No
- [ ] Yes

If you tried to login to your computer account right now, how many attempts do you think it would take?

- [ ] No
- [ ] Yes

To how many people have you given your current password?

- [ ] No
- [ ] Yes

Have you ever forgotten your current password?

- [ ] No
- [ ] Yes

If yes, how did you recover it?

Have you ever forgotten old work passwords?

- [ ] No
- [ ] Yes

If yes, how did you recover it?

When you created your current password, which of the following did you do?

- [ ] I reused an old password
- [ ] I modified an old password
- [ ] I reused a password I was already using for a different account
- [ ] I created an entirely new password
- [ ] Other:

Did you use any of the following strategies to create your current password (choose all that apply) ?

- [ ] Password based on the first letter of each word in a phrase
- [ ] Based on the name of someone or something
- [ ] Based on a word or name with numbers / symbols added to beginning or end

- [ ] Based on a word or name with numbers and symbols substituting for some of the letters (e.g. '@' instead of 'a')
- [ ] Based on a word or name with letters missing
- [ ] Based on a word in a language other than English
- [ ] Based on a phone number
- [ ] Based on an address
- [ ] Based on a birthday

How long is your current password (total number of characters)?

- [ ] I prefer not to answer.

What symbols (characters other than letters and numbers) are in your password?

- [ ] I prefer not to answer.

How many lower-case letters are in your current password?

- [ ] I prefer not to answer.

How many upper-case letters are in your current password?

- [ ] I prefer not to answer.

In which positions in your password are the numbers?

- [ ] I prefer not to answer.
- [ ] First
- [ ] Second
- [ ] Second from last
- [ ] Last
- [ ] No Numbers
- [ ] I prefer not to answer.

In which positions in your password are the symbols?

- [ ] I prefer not to answer.
- [ ] First
- [ ] Second
- [ ] Second from last
- [ ] Last
- [ ] No Numbers
- [ ] I prefer not to answer.

Have you written down your current password?

- [ ] No
- [ ] Yes, on paper
- [ ] Yes, electronically (stored in computer, phone, etc.)
- [ ] Other

If you wrote down your current password how is it protected (choose all that apply) ?

- [ ] I do not protect it
- [ ] I stored it in an encrypted file
- [ ] I hid it
- [ ] I stored it on a computer or device protected with another password
- [ ] I locked up the paper
- [ ] I always keep the password with me
- [ ] I wrote down a reminder instead of the actual password
- [ ] Other

Do you have a set of passwords you reuse in different places?

- [ ] No
- [ ] Yes

Do you have a password that you use for different accounts with a slight modification for each account?

- [ ] No
- [ ] Yes

PHYSICAL SECURITY GUIDED TOUR

Covered in full in Operational Security Assessment:

Have your point of contact walk you around the office (often as part of introductions on the first day) - mentally note physical security concerns. Document how difficult it would be for a visitor or after-hours break-in to access sensitive systems. Identify physical assets with sensitive content, such as:

- Networking equipment and servers
- User devices (workstations/laptops, smarthpones, USB drives)
- Sensitive information or external storage drives lying on desks
- Accounts/passwords written on post-its, white-boards, etc.
- Unattended, logged in computers
- Unlocked cabinets, computer rooms, or wiring closets
- Network ports that are not in use, especially ones not in plain sight

This can be done remotely via secure videoconference over a smartphone or tablet that can moved around the office easily.

Combining this activity with Office Mapping helps to reduce the awkwardness of taking notes while walking around the office, and if being done remotely, the two separate activities can be used to cross-verify the accuracy of each.

VULNERABILITY SCANNING AND ANALYSIS

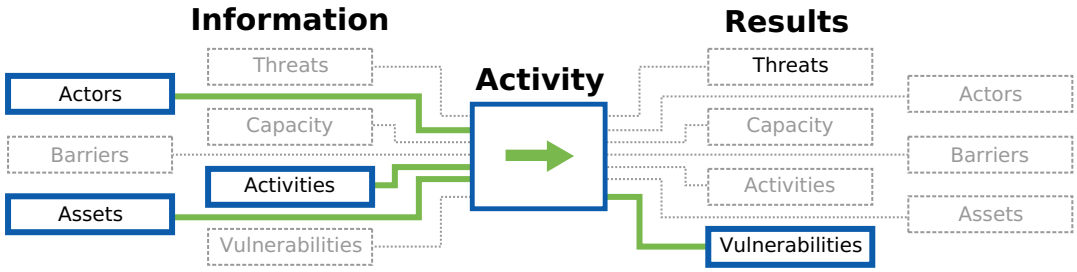
SUMMARY

This component has the auditor discover possible flaws the organization's devices, services, application designs, and networks by testing and comparing them against a variety of online and offline resources (vulnerability databases, vendor advisories, and auditor investigation) to identify known vulnerabilities. Basic vulnerability analysis should be occurring alongside the other activities so that evidence can be gathered from the network, however, deeper research into specific discovered exploits can happen after the on-site audit to fully take advantage of the short time the auditor has on site.

PURPOSE

It is not uncommon for a cash-strapped human rights NGO to run critical infrastructure themselves on available equipment. A better-resourced organization may host its critical services at a remote data center, or outsource its IT infrastructure to cloud providers, such as Google Apps, and/or to ad-hoc services (Dropbox, Yahoo! mail, Wordpress, etc.). Regardless, it is rare to have someone designated to update and patch systems as vulnerabilities are released, or to view the services from a security -- as opposed to availability -- standpoint.

THE FLOW OF INFORMATION



Vulnerability Analysis Information Flow

GUIDING QUESTIONS

- What level of proof do you need to identify to convey the importance (or importance) of a vulnerability to the organization?
- What would the organization and IT think is an appropriate amount of the IT staffs time that you can request to get the information you need?

APPROACHES

- **Vulnerability Scanning:** Run vulnerability scans against websites, externally facing servers, and key intranet servers.
- **Explore Vulnerability Databases:** Search vulnerability databases for potential risks to systems and software used on servers, user devices, and online services.
- **Examine Service Configuration Files:** Examine configuration files for vulnerabilities using "hardening", or "common mistake" guides found online.

OUTPUTS

- 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.

- Document Vulnerabilities (per vulnerability)
  - Write Up
  - Summary - A short (two to three sentence) basic overview of the vulnerability, including a discussion of potential impacts.

- Description - An in-depth (one to three paragraph) overview of the vulnerability.
- Approach - Step-by-step explanation of the methodology used that is tool agnostic.
- Proof - The cleaned up output from tests run to identify the vulnerability.

OPERATIONAL SECURITY

- Treat the data and analyses of this step with the utmost security.
- Use VPNs or Tor to search if scanning remotely.
- Seek explicit permission for vulnerability scanning - *NOTE:* The organization might not be in a position to give you meaningful “permission” to carry out an active remote assessment of "cloud services" used within the organization.
- In situations where the auditor is doing this work remotely it is important to only run "safe" tests that have no possibility of causing damage to the network.

PREPARATION

Baseline Skills

- **Vulnerability Scanning:** : General TCP/IP and networking knowledge; knowledge of ports, protocols, services, and vulnerabilities for a variety of operating systems; ability to use automated vulnerability scanning tools and interpret/analyze the results
- **Penetration Testing:** Extensive TCP/IP, networking, and OS knowledge; advanced knowledge of network and system vulnerabilities and exploits; knowledge of techniques to evade security detection

RESOURCES

- *Standard:* "Vulnerability Analysis - Research Phase" (Penetration Testing Execution Standard)
- *Framework:* "Vulnerability Assessment" (http://www.vulnerabilityassessment.co.uk)
- *Resource:* Vulnerability Databases (SAFETAG)
- *Security Advisories:* [56,57,58,59,60,61]

Vulnerability Databases

- *Standard* Vulnerability Analysis - Research Phase (Penetration Testing Execution Standard)
- *Framework* Vulnerability Assessment (http://www.vulnerabilityassessment.co.uk)
- *Database* "Open Sourced Vulnerability Database"
- *Database* "CVE Details"
- *Database* Search CVE and CCE Vulnerability Database
- *Database* "Threat Explorer"
- *Database* "The Exploit Database"
- *Database* "Security Focus Vulnerability Search"
- *Poster* Ultimate Pen Test 2013 (SANS Institute)
- *Security Advisories* [62,63,64,65,66,67]

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)
- *Article:* "14 Best Open Source Web Application Vulnerability Scanners" (InfoSec Institute)

System Vulnerability Scanning

- *Project Site:* "OpenVAS Project Site" (OpenVAS)
- *Manual:* "OpenVAS Compendium" (OpenVAS)
- *Guide:* "Creating OpenVAS "Only Safe Checks" Policy"
- *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)
- *Guide:* "VoIP Security Checklist" (ComputerWorld)
- *Overview:* "The Vulnerability of VoIP" (Symantec)
- *Research:* "Researchers find VoIP phones vulnerable to Simple Cyber attacks" (Security Intelligence)
- *Tool:* "Vsaudit (Eurialo)" (Eurialo) *Overview:* "Two attacks against VoIP" (Symantec)
- *Overview:* VOIP analysis Fundamentals(Wireshark)
- *Tool:* WireShark VOIP Capabilities

ACTIVITIES

VULNERABILITY SCANNING

Summary

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 activity uses active research and scanning to detect known vulnerabilities in external and key internal services. Usually penetration tests exploit possible vulnerabilities to confirm their existence. [68] But, the use of exploits puts the organization's systems at a level of increased risk [69] 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. [70]

Overview

- Identify services being hosted or used by an organization
- Research externally-facing organization services (websites, services hosted from the office, etc.)
- Research information about identified services (e.g current versions of those services.)
- Run vulnerability scans against websites hosted by the organization, externally facing servers run by the organization, and key intranet servers.

Materials Needed

- A Kali VM, bootable USB, or installed system with OWASP ZAP or OpenVAS installed, updated, and running

Considerations

- Be very careful about which automated scans you run to ensure that no aggressive or potentially damaging tests are included.
- OpenVAS saves its scan records in /var/lib/openvas/mgr/tasks.db - this file will contain sensitive data, ensure it is stored securely.
- OpenVAS and other vulnerability scanners can be highly aggressive in their tactics. Tools like Metasploit come with a library of active, functional exploits to "prove" that a system is actively vulnerable. As such, these can be tricky to use. Even OpenVAS on a safe-only scan can appear to a host as an active attack, blocking further access from your IP (this can cause some annoyance if you are, for example, scanning your host organization's website from their network). Some of these scans and techniques -- again, even the "safe" ones -- can also be a violation of local hacking laws. Get explicit permission, give warnings, and be careful.

Walkthrough

Vulnerability Scanning using OpenVAS

Setting up OpenVAS in Kali

```
openvas initial setup
openvas feed update
openvas check setup
openvas stop
openvas start
```

Visit https://127.0.0.1:9392/ in a web browser and log in.

Using OpenVAS

Once logged in to OpenVAS, the interface is disturbingly simple to use. For most use, using the Wizard to scan the target server works best. Things to verify before doing so:

- Check the Scan defaults for the Wizard - it should be set to run the built-in "Full and Fast" scan
- For that scan, verify (under Configuration->Scan Configs) that the "Scan Settings" list shows "safe_checks" as "yes"

Once you start a scan, change the display to "auto refresh" to give you more feedback on the scan process. Once the scan is completed, a report can be exported in PDF form.

Common problems * **Errors during openvas-start** OpenVAS is a rather ... delicate program. Most often, the openvas-start script will not wait long enough between launching openvassd and openvasmd, causing openvasmd to error out. Re-running openvasmd often works, though an entire stop/start cycle seems to be slightly more reliable. Often, openvasmd will

error out, but launch anyway. Checking the web interface at https://127.0.0.1:9392 to make sure that you can log in is the best way to check if it's actually successfully launched. * **Lost admin password** From a root command-line, you can reset the web interface's admin password:

```
openvasmd --create-user=admin
openvasmd --user=admin --new-password=admin
```

- **openvasmd will never launch** In many fresh install cases of OpenVAS7, the openVAS self-signed CA certificate is set to an invalid date, which also causes openvasmd to error out. The check-setup script will recommend rebuilding the database, but the /var/log/openvas/openvasmd.log may have errors discussing certificate errors. If this is the case, try:

```
rm /var/lib/openvas/CA/*
rm /var/lib/openvas/private/CA/*
openvas-mkcert
openvas-mkcert-client -n -i
openvas-check-setup
openvas-start
openvasmd --rebuild
openvas-stop
openvas-start
```

Recommendation

The auditor will need to do research and compare against the organization's capacity and risks to give specific recommendations based on the vulnerabilities discovered in the process. Some common recommendations include the following:

- Out of Date Content Manangement System

Most popular CMS platforms provide emailed alerts and semi-automated ways to update their software. Make sure someone responsible for the website is either receiving these emails or checking regularly for available updates. Security updates should be applied immediately. It is a best practice however to have a “test” site where you can first deploy any CMS update before attempting it on a production site.

For custom CMS systems, it is strongly advisable to migrate to a more standard, open source system.

An increasingly good practice is for organizations to take advantage of the "free" tiers of DDoS mitigation services, of which CloudFlare is probably the best known. A challenge of these free services can be that they have definite limits to their protection. With CloudFlare, organizations can request to be a part of their Project Galileo program to support at-risk sites even beyond their normal scope of support.

A community-based, open source alternative is Deflect, which is completely free for eligible sites.

Some of these services will be revealed by BuiltWith, but checking the HTTP Response Headers (in Chromium/Chrome, available under the Inspect Element tool, or by using Firebug in Firefox. See Deflect's wiki for more information.

Guide for NGOs about DDoS: Digital First Aid Kit

- Insecure Website Login HTTPS / SSL – this comes at a cost, both the SSL Certificate and often an upgrade to the hosting plan itself. However, without SSL, every password – including the one used for admin access to the website – goes across the Internet in the clear. This is immediately available to a state-level actor through the ISP, and can also be sniffed if accessed by a staff member on a shared wifi connection (at a coffeeshop or airport), and finally if the attacker has broken in to the office network (see the Local Access section). Enabling SSL (and making it the default for your site) also protects the users of your site.

If an organization updates their website via FTP, it is worth noting that FTP is similarly insecure. Many hosting providers provide SFTP or FTPS, (two different, but secure, FTP versions), or secure WebDAV to upload files. These should be used, turning “plain” FTP off altogether if possible.

When switching to SSL/Secure FTP after having used the plain versions, webmasters should also update all administrative passwords, and watch to make sure that no step along the way (hosting provider management/panel, file upload, CMS editing) goes over “clear” channels.

- Website Vulnerabilities

VULNERABILITY RESEARCH

Summary

Overview

After completing an automated vulnerability scan (network, system, webapp) and documenting findings, you can now move into vulnerability research.

Vulnerability research consists of:

- Reviewing your findings by researching on public vulnerability Databases about the vulnerability that you have found.
- Identify and enumerate risks involved for a certain vulnerability
- Formulate a mitigation plan or recommendations

Below is a list of some of the most common vulnerability databases:

- National Vulnerability Database
- Exploit Database
- Rapid 7 Vulnerability & Exploit Database
- SecurityFocus BugTraq Database
- WPScan Vulnerability Database
- PacketStorm
- CVEDetails
- KB CERT
- Skybox Security

Validation:

Each of your findings, onced reviewed and documented will be enough for your report. However, if you and the organization agreed to verify findings and vulnerability truly exist, you may refer to Penetration Testing resources within SAFETAG framework.

Materials Needed

Considerations

- Treat the data and analyses of this step with the utmost security.
- Use VPNs or Tor to search if conducting the search from a country that is highly competitive with the organization's country, or is known to surveil.

Walkthrough

Recommendation

WEBSITE FOOTPRINTING

See Website Footprinting in Recon for passive / lightweight investigation tools

WEB VULNERABILITY ASSESSMENT

Summary

Organizational websites are often a central part of their work, but resource constraints can leave them vulnerable to a wide variety of attacks, from simple DDoS (Distributed Denial of Service) attacks to being leveraged for online scams and malicious advertisin to targeted distruction and subversion. Insecure websites can even be used in "watering hole" attacks where malware is implanted into the site to intentionally target the website's audience.

This activity provides a SAFETAG auditor with a suite of processes and tools to investigate organization and project websites for potential vulnerabilities. There are multiple ways to do this, from passive to more active scanning. SAFETAG takes great care to take a primarily 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. Care should be taken to review operational security concerns, work closely with the organization, and pursue a minimal approach focused on the priorities of the organization. See also the Vulnerability Scanning activity for additional tools and approaches useful for investigating outside of the website itself the server level.

Overview

- Understand the current infrastructure the website is using on the level of the hosting provider, location, Operating system
- Identify the public IP address of the server you will be auditing as you will see in somecases, websites are using proxies or DDoS mitigation services that mask the real IP address of a server
- In the case of shared hosting, identify the hosting service and the current package
- Identify the web server, applications in use & plugins, themes, security protocols in place and users' session management
- Identify misconfigurations, sensitive information publicly available, metadata embedded within the web application
- Look for forgotten or insecure support applications like /phpmyadmin
- Run automated vulnerability scans against websites hosted by the organization to identify "low-hanging fruits" especially in the case of auditing an opensource and common content management system or other web applications
- Perform manual vulenrability asessment and testing to identify server misconfigurations, web sessions, tokens etc.

Materials Needed

Considerations

- Begin with passive techniques and consider if more detail is necessary (e.g. would simply upgrading the CMS solve multiple problems). Remember that the point is to create a clear, simple path towards security, not a comprehensive report on every possible vulnerability
- Seek explicit permission for vulnerability scanning - *NOTE:* The organization might not be in a position to give you meaningful “permission” to carry out an active remote assessment of "cloud services" used within the organization.
- Agree on the site(s) to scan and determine the intensity of the process
- Ensure documented permission and schedule an appropriate time with the site host.
- In situations where the auditor is doing this work remotely it is important to only run "safe" tests that have no possibility of causing damage to the website. Be very careful about which automated scans you run to ensure that no

aggressive or potentially damaging tests are included.
- Understand, discover and review the backup options the website has before starting the audit process.

Walkthrough

Performing web vulnerability assessment can be done in different ways, using different tools and having different results. Choosing any of these steps or guides must not confuse an auditor, but instead, provide a broader scope which should help them finding vulnerabilities as many as they can.

These vulnerabilities can range from: - Web Server/OS level vulnerabilities - Access control vulnerabilities - Application-specific vulnerabilities - Misconfiguration - SQL Injection - Cross-site Scripting - Directory Traversal - Failure to restrict URL Access - Insufficient Transport Layer Protection - LDAP Injections - Malicious Codes - Leaked information

Before pursuing any of these more active scans, review outputs from passive reconnsaisance, DNS history and current information, and (if relevant) CMS version checking. This guide covers a small subset of web vulnerability scanning tools, a more comprehensive list is available at https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools which may provide approaches better suited to specific situations.

OpenVAS, covered in the vulnerablity scanning activity, also includes Wapiti, which can help to detect many of the above common vulnerablitites.

Manual Testing with Burp (Active)

Introduction

According to Burp's official documentation, "Burp Suite is an integrated platform for performing security testing of web applications. It is **not a point-and-click** tool, but is designed to be used by hands-on testers to support the testing process. With a little bit of effort, anyone can start using the core features of Burp to test the security of their applications. Some of Burp's more advanced features will take further learning and experience to master." To know more about BurpSuite's other tools and features, visit BurpSuite's Tools and it's functions pages.

Requirements

Note: If you are using Kali Linux, you already have Burpsuite pre-installed. Otherwise if you do not have a Linux box, refer to the following requirements below:

- Windows/MAC OSX (Kali Linux Preferred)
- Java Runtime Environment
- Browser (Chrome, Firefox)
- BurpSuite

Launching Burp

Burp's Getting Started Documentation is quite detailed and useful, and strongly recommends launching Burp from the command line for better control. In specific, it recommends assigning the amount of memory you wish to dedicate to burp:

```
java -jar -Xmx1024m /path/to/burp.jar
```

where 1024 is the amount of memory (in Mb) that you want to assign to Burp, and /path/to/burp.jar is the location of the Burp JAR file on your computer.

The troubleshooting help can help if Burp doesn't appear shortly.

Setting up your environment

- Verifying Scope/Target:
  - Always check that you have the right URL/Domain before starting. Last thing we wanted to happen is to scan a different target that is out of our scope!

- Setting up your browser

- For Firefox:
  - Paste about:preferences#advanced this in your URL, and click Settings left of **Connection**
  - Click Manual proxy configuration and enter localhost under **HTTP Proxy**, with Port set to: 8080
  - Check Use this proxy server for all protocols
- For Chrome:
  - Paste chrome://settings/system then click **Open proxy Settings**
  - This will open the **Network Setting* windows in Kali. Click** Network proxy** and set *Method* to Manual
  - Set **HTTP Proxy** to 127.0.0.1 with **Port** valued at 8080
  - Configure the rest of settings with following values above (HTTPS, FTP Proxies, and Socks Host)
- Setting up Socks Proxy (Optional)
- In some cases, you will be required to scan from an approved testing environment or a specific network/IP range. In this case, you have to configure Socks Proxy for your assessment.
- Verify your IP. Take note of your current IP address. (WhatismyIP.com)
- To setup your Socks Proxy, we can do this by connecting via SSH to our server:
  - ssh –D 9292 –l username@server_name/ip
- Once authenticated, configure Burpsuite to route it's traffic to our outbound SSH tunnel.
  - From **Options** Tab, click **Connections** sub-tab and scroll down to Socks Proxy
  - In **Socks Proxy host**, type localhost. and under **Socks Proxy port**, type 9292
  - Then check **Use SOCKS proxy** button

- You can again check your IP address to verify if your configuration is correct.

Testing Burpsuite Configuration

NOTE: Scanning web applications without the owner's permission is potentially illegal. It is important that you test Burpsuite on your own web applications, or on a controlled environment. There are some publicly available websites that are insecure by default to be used for testing and learning purposes. Among these were:

- bWAPP - Buggy Web Application
- HackThis - Hacker's Playground
- HackThisSite - Community Driven hacking exercises
- HackMe - Community based, collaborative hacking exercises and vulnerable web apps
- CrackMeBank

(You can use these sites to get familiar with Burpsuite, and performing the following excerices in this guide.)

Intercepting Request

- To start intercepting traffic to and from your target domain/URL, in your configured browser, enter the the target domain, and hit enter.
- On your Burpsuite instance, under **Proxy** Tab, and sub-tab **Intercept**, make sure that the Intercept button is on.
- If it captures the request from your Firefox browser, it means that your configuration is correct.
- Click Forward and the request will be forwarded to the server/target and the next sub-tab **HTTP History** will now start to generate some contents, each time you open a link, or a page within the target domain.

Adding Target/Scope - Adding your target into scope is important so you won't miss, or even scan URLs that are not included in your list of targets. - To add the target to your scope, right-click the domain/website, then select **Add to Scope** - Burp will now tell you if you want ot stop sending out-of-scope items in your **HTTP history** tab and other Burp Tools - click **Yes**. - This will now appear in your **Target** tab, and under **Scope** sub-tab. - To add subdomains into your scope, you can use regex: .*\.test\.com$

Managing Burp Projects - Managing burpsuites project will depend on the version you are using. Some features may not be available for free version of burp, but are only available for Pro Version. See burp's documentation for managing projects here - Selecting project type: - Temporary project - Quick tasks, no need to save data - New project on Disk - Creates new project and stores it on disk on a "Burp project file" - Open existing project - Opens recent existing project from a "Burp project file". Scanners & spiders are paused.

- Selecting Configuration
  - Burp Defaults - BurpSuite's default options
  - Use options Saved within project - Only available when reopening an existing project. It uses the options saved from the previous project
  - Load from a configuration file - Opens a project using the options contained on a Burp Configuration File

NOTE: According to BurpSuite documentation, *"If you open an existing project that was created by a different installation of Burp, then Burp will prompt you to decide whether to take full ownership of the project.*

This decision is needed because Burp stores within the project file an identifier that is used to retrieve any ongoing Burp Collaborator interactions that are associated with the project. If two instances of Burp share the same identifier in ongoing work, then some Collaborator-based issues may be missed or incorrectly reported. You should only take full ownership of a project from a different Burp installation if no other instance of Burp is working on that project."

Since that Burpsuite is an advance tool for testing web applications, This guide will cover most of the basic testing activities for Burpsuite. To learn more of the advance features, it is important that you have a licensed version.

Basic BurpSuite Testing Excercises:

Attacking web application using simple payload set (Bruteforce attack): - Verify that your Burp is working - You must first try to test if your Burp and browser are both configured

- Login page of target application
  - Now try visiting any login page of your target web application (you can use any test site mentioned above)
- "Intercept On" - Make sure that you have your burpsuite's intercept function set to "ON".
  - Before you click "ENTER" to submit your sample credentials, you can intercept web traffic request from your browser to the server under **Proxy** > **Intercept** tab, then "Intercept" button is set to "ON".
- Review contents of the requests under **Proxy** > **Intercept** > **Raw**
  - On the **Raw** tab, Once you see the "POST /login.php" request of your browser to the web application server, select ALL and right-click on the selected/highlighted texts and select **Send to Intruder**
- Now under **Intruder** > **number tab** > **Target** uncheck "Use HTTPs".
- Now click under **Intruder** > **number tab** > **Position** to view all replaceble variables.
- Try looking for email and pass,
  - You can either change your variable for email and pass for earch or just include ONE variable. For this exercise, we will use the pass variable.
- Now under **Intruder** > **Payloads**
  - You can define here the number of payload sets depdening on your attack type (for our case, since we only have 1, let's use 1)
- Now below the options Payload Sets, you can see Payload Options where you can add, Paste, add from list strings that you can use as your payload.
- After typing your list of strings or passwords, let's go to **Positions** tab, and on the right side of Payload Options click **Sta Attack**
- After clicking "Start Attack" it will open a window of results usually your HTTP responses codes.

Take note of these errors to see how the target web application respond when given certain types of strings.

OWASP ZAP (Active)

OWASP ZAP allows an auditor to quickly identify common web vulnerabilities using the OWASP framework - either by a relatively intense spidering of the website or through a more tailored use of the proxy functionality of the tool.

OWASP ZAP provides a highly configurable tool to test for common website vulnerabilities. In addition to supporting organizational change to support general best practices for websites, OWASP can expose more specific vulnerabilties that may warrant action above and beyond general best practice work.

For a website that can be expected to withstand a dedicated spidering of its content, the automated mode will dig through and expose common vulnerabilities. The tool itself is relatively easy to use.

For more delicate sites, private sites, or other situations, OWASP can also proxy your web browser and test the pages you click through.

Additional OWASP ZAP references:

- Wiki and QuickStart Guide https://code.google.com/p/zaproxy/wiki/HelpStartStart
- Overall walkthrough: http://resources.infosecinstitute.com/which-weapon-should-i-choose-for-web-penetration-testing-3-0/
- Testing with Metasploitable VM: http://cyberarms.wordpress.com/2014/06/05/quick-and-easy-website-vulnerability-scans-with-owasp-zap/ (see also https://www.owasp.org/index.php/Webgoat and http://sourceforge.net/projects/samurai/)
- Walkthrough of automated mode https://blog.codecentric.de/en/2013/10/automated-security-testing-web-applications-using-owasp-zed-attack-proxy/
- Walkthrough of proxy usage https://blog.42.nl/articles/securing-web-applications-using-owasp-zap-passive-mode/

Recommendation

CHECK CONFIG FILES

Summary

Examine configuration files for vulnerabilities using "hardening", or "common mistake" guides found online.

Overview

- Explore default configurations.
  - Identify if systems are using default passwords or users
- Use hardening guides & common min-configurations to identify weak/vulnerable configurations.

Materials Needed

Considerations

Walkthrough

Recommendation

NETWORK VULNERABILITIES

See the Network Access and Mapping activities for methods to expose insecure wireless networks and for methods to use network mapping and traffic analysis to discover further potential vulnerabilities or points to investigate.

ROUTER BASED ATTACKS

Summary

Many wireless routers still use the default password listed in "Router Default Password Search", meaning that anyone with access to the network could also take complete control of the router - adding in remote access tools or setting up other attacks.

Overview

- Find the router(s) (route works well for this)
- Test using default passwords
- Check for upgrades / un-patched vulnerabilities and backdoors
- Investigate potentially valuable data (logs, connected users)

Materials Needed

Considerations

Walkthrough

Material that may be Useful:

- *Search Engine:* "Router Default Password Search" (RouterPasswords.com)
- *Framework:* "Router Exploitation Framwork"

Recommendation

Change Default Router Passwords

Passwords - particularly on core network devices - is very important. Use a password manager to save the new password (or be prepared to reset the router to a factory default).

While nominally "inside the firewall" and protected from remote attacks, leaving routers with default passwords, particularly wireless routers whose networks are often shared with visitors, is a potentially very high risk for an organization. Anyone who has gained access to the network via legitimate or other means could subtly alter the router's configuration to provide remote access, or route traffic to an attacker-designated server. Such changes can easily go undetected for long periods of time.

A common fear is forgetting the new router password. A password management system is an obvious solution, but if the router is in a secure location, even a stickie note would be better than the default password.

DATA ASSESSMENT

SUMMARY

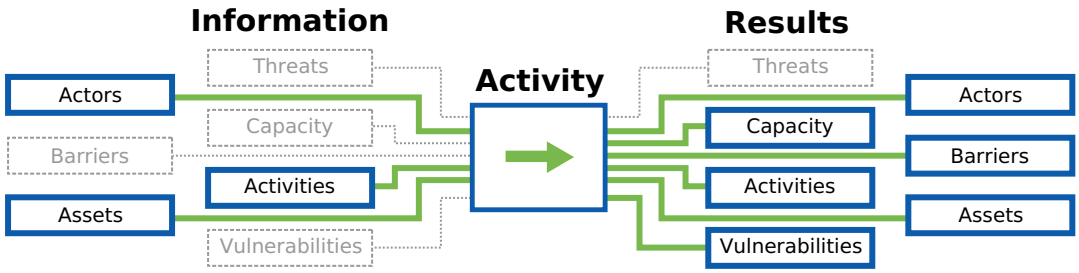
This component allows the auditor to identify what sensitive data exists for the organization, where it is stored, and how it is transferred.

PURPOSE

Sensitive files are often stored across multiple devices with different levels of security. A data assessment allows the auditor to 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.

An adversary who obtains a laptop, workstation, or backup drive will be able to read or modify sensitive information on the device, even if that staff member has set a strong account password. This applies to threats involving loss, theft, and confiscation, but also to "checkpoint" scenarios in which they may only have access for a few minutes. Furthermore, in the event of a burglary or office raid, an adversary could obtain all sensitive information on the organization's devices, possibly even undetected.

THE FLOW OF INFORMATION



Data Assessment Information Flow

GUIDING QUESTIONS

- What are the most important data sets to keep available? Are there backups?
- What are the most important data sets to keep private?
- How does the organization currently determine who should have access to data?
- Is there currently anyone who has access to data who should not?
- Does the staff agree on what constitutes sensitive data?
- What data does each staff member need to be able to access in order to do their job?

APPROACHES

- **Data Mapping Activity:** Have staff identify where that data is currently (what devices/physical locations), who has access (physical, login, permissions), and who needs to have access to get the organizations work completed.
- **Risks of Data Lost and Found Activity:** Have rank the impact if different data within the organization was lost, and if adversaries gained access to that data.
- **Private Data Activity:** Guide staff through an activity to have them list private data within the organization [71]

If it was not possible to conduct these activities in person, you can conduct them remotely through applying one of the remote facilitation approaches described in the Remote Facilitation appendix.

OUTPUTS

- 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.

OPERATIONAL SECURITY

- Ensure that any physical notes/drawings are erased and destroyed once digitally recorded.
- Ensure that any digital recordings of this process are kept secure and encrypted.
- Consider who has physical and visual access to the room where this process takes place, and if the room can be secured if this activity may span long/overnight breaks.

PREPARATION

- Facilitation skills or experience is useful for these exercises
- Carefully review the exercises you plan to use

RESOURCES

- *Activity:* "Backup Matrix: Creating an Information Map" (LevelUp)
- *Activity:* "Identifying and prioritizing your organization's information types " (NISTIR 7621)
- *Guide:* "Data Risk Checker: Categorizing harm levels on knowledge assets to inform mitigation and protection" (Responsible Data Forum wiki)
- *Guide:* "Awareness and Training" (Information Security Handbook: A Guide for Managers - NIST 800-100)
- *Guide:* "Managing Information Security Risk: Organization, Mission, and Information System View" (NIST 800-39)
- *Guide:* "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" (NIST 800-122)

ACTIVITIES

SENSITIVE DATA

Summary

Data and meta-data about an organization and its staff is incredibly difficult to keep track of over time, as people or projects use cloud services like Dropbox or Google Drive for some activities, a shared server for others, and a mix of work and personal devices (laptops, phones, tablets...).

This is natural, but it is important to keep track of where your organization's data lives and who can access it.

Overview

- With staff input, post up popular places where data is kept (laptops, email, shared drives...)
- Using stickies, gather from the staff what data is kept in what locations - duplicating notes when needed
- Rank data by sensitivity
- Discuss the impact of one of the devices where data is stored being lost - are there backups?
- Discuss the impact of a device being exposed / taken by an adversary
- Identify who has access (physical access, login access, and permissions), and who needs to have access to get the organizations work completed.

Materials Needed

- Stickies and markers for activities
- Flip chart paper or a whiteboard
- Camera to record outputs digitally

Considerations

- Some of the stickies generated in this activity may provide sensitive data, dispose of them responsibly.
- If you take photos for reporting needs, save the image files in a secure, encrypted container.

Walkthrough

Sensitive Data Assessment Activity

Duration: 45 minutes

This exercise is adapted from the LevelUp Activity, Backup Matrix, part of the curricula for Data Retrention and Backup by Daniel O'Clunaigh, Ali Ravi, Samir Nassar, and Carol.

Materials to Prepare:

- Stickies
- Markers
- Flipchart paper
- One larger sheet of paper taped to wall in landscape orientation, with or without prepared titles. (For an example with prepared headings, see the matrix below.) The Sensitivity axis is optional in the original exercise, but critical for this one. It can be added after the initial round of brainstorming however to streamline the flow.

Relative Sensitivity	Computer	USB / External Drive	Cloud Storage	Phones, Print, etc.
High				
Moderate				
Low				

Explain to participants that we're going to conduct an information mapping activity to get a sense of where our important information actually is.

Start by listing the different places where our information is stored, according to participants. If no suggestions are forthcoming, we can prompt participants with the obvious stuff:

- Computer hard drives
- USB flash drives
- External hard drives
- Cellphones
- CDs & DVDs (and BDs)
- Our email inbox
- The Cloud: Dropbox, Google Drive, SkyDrive, etc
- Physical copies (or “hard copies”) in the office
- Multimedia: Video tapes, audio recordings, photographs, etc.

Use large stickies to place these as column headers on a wall. More will come up later in the course of the exercise.

Elicit from participants what type of information or data they have in each of these places. For example:

- Email

- Contact details, such as a member database
- Reports/research
- Funder information / contracts
- Accounts/spreadsheets
- Videos
- Images
- Private messages on Facebook, etc.

To encourage participant interaction, write one example on a sticky and place it in the appropriate box in the matrix. Then, ask whether there is another copy of this data somewhere. If there is, you can use another sticky and put it wherever they keep the duplicate.

TIP: Place Computers, Phones, and Email next to each other, so you won't have to create duplicates for everything "stored" in email (and therefore on laptops and phones)

Introduce a new vertical axis representing sensitivity. The higher on the chart, the more sensitive the data. Ask the participants to rank data.

For a large group, divide the group into smaller teams for the next steps (it helps if there are relatively clear thematic distinctions within the group, such as nationality, type of work, area of interest, etc.)

Provide stickies to the group(s). Have the group(s) brainstorm about all of the data they work with, focusing on the most important data first.

Participants should write ONE type per sticky, and create duplicates if the data is stored in multiple locations.

For a small group, this can be done as a "live" brainstorm. For larger groups that have been subdivided, have each group finish listing out their most important data and then have each group place the stickies on the matrix. Invite discussions around the sensitivity of the data.

An example may look something like this:

Level Up Backup Matrix Example

Explain that this gives us an idea of where our data is. Elicit whether or not this is all the data we generate? Of course it isn't: It's only a small percentage.

The LevelUp lesson uses this primarily to discuss the importance of backups, and this is a valuable point to make.

Call out the information that they are keeping on their computer's hard drive (which will usually be the fullest one). Elicit some of the things that can cause a computer to stop working. Maybe take a show of hands: Who has had this happen to them?

- Virus or malware attack destroyed a computer or some data
- Stolen computer, confiscated computer
- Infrastructural problems, like a power failure broke a computer
- Inexplicably bricked computer, etc.

For SAFETAG, we focus on the "Sensitive data in the wrong hands" section. Based on the clustering of sensitive data along the vertical access, choose a column that has an unsual amount of sensitive data (email or computers, usually).

Remove the stickies from the column but keep them in your hand and read them. Now I have this information. What can I do with it? And what are you left with? Is anyone at risk - yourselves? partners? If this were published on the Internet, what would happen?

Recommendation

RISKS OF DATA LOST AND FOUND

Summary

Have staff rank the impact if different data within the organization was lost, and the impact if various adversaries gained access to that data.

Overview

Materials Needed

Considerations

Walkthrough

See the Sensitive Data activity for an interactive way to gather the types of data in the organization for this ranking exercise.

Recommendation

PRIVATE DATA

Summary

Guide staff through an activity to have them list private data within the organization (e.g. Using the "personal information to keep private" handout. [72])

Overview

Materials Needed

Considerations

Walkthrough

Personal Information To Keep Private

Information that can be used to identify individuals, organizations, and even communities of practice should be treated with the utmost care. Some data, like names, phone numbers, and addresses are obvious, while others, like computer names, the MAC addresses of wifi cards, or pseudonymous social media accounts may be less obvious. Also, combinations of information - location, data, and type of activity, or even an issue area of interest and a city name may specify a very small number of activists or organizations.

This spreadsheet, part of the Responsible Data Forum documentation sprint provides a useful baseline of types of data and ways to manage or obfsucate it usefully: Data Anonymization Checklist

Recommendation

For the internal audit report back to the organization, much of the information will require specific identification of user devices (and by extension, their users), as well as very sensitive organizational data. None of this data, by intention, accident, or adversarial action, should be shared with third parties.

Please refer to the Analysis and Reporting section for the limited data set that is required for project reporting, and to the Operational Security section for guidance on data security.

PHYSICAL AND OPERATIONAL SECURITY

SUMMARY

The organizational security methodology is focused on how to mitigate against threats that occur because of the arrangement of digital assets in the physical world -- how secure are the devices at an organization's office, where and how staff travel with organizational devices, and whether staff work outside of the office (e.g. in remote offices, at their homes, while traveling, or at cafes). Further, is organizational information accessed from personal devices, and how are those devices secured?

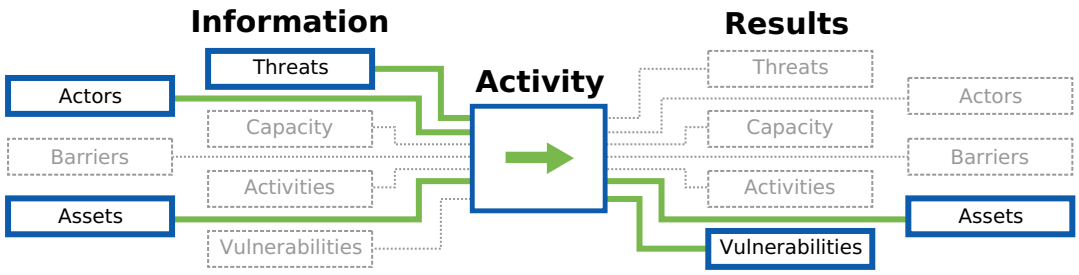
PURPOSE

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.

For many organizations, digital threats that depend on physical access are considered the least probable. So much so, that many security specialists concede that there is no proper defense against an attacker with physical access to sensitive hardware. While there is some truth to this, it is not useful advice for small scale civil society organizations or independent media houses. The risks that advocacy and media organizations face are far more varied, and the cost of lost information can be crippling to their ability to operate. As such, these risks have high severity, despite their equally high probability for these organizations.

Depending on the specific threats for each organization, the auditor should consider the challenges of not only one-time exfiltration of data as well as potential ways an adversary could use physical access or proximity to the organization or its devices to gain ongoing remote access, track, or cause harm to the organization through the outright destruction of data.

THE FLOW OF INFORMATION



Data Assessment Information Flow

GUIDING QUESTIONS

- Who has physical access to what? When are devices not monitored by trusted staff?
- Who has independent access to the office space?
- How could adversaries gain access? (forced entry, theft, social engineering, seizure)
- How are daily devices used and stored -- where are they when employees go home?
- Where are the servers and network components that host and manage the organizations assets? Are there active network jacks that are unused, are they in public spaces, are they in places where people would not notice if there was somthing plugged into them?
- How is data accessed and stored outside of the organization's main offices/workspaces?
- Do staff travel with organizational information?
- How are backups managed? Where are they stored?

APPROACHES

- **Physical Access to the Lan, wifi, and Servers:** Tour the office and look for exposed network devices, servers, and network jacks, document how difficult it would be for a visitor or after-hours break-in to access sensitive systems. Determine the reach of the wireless network and how easy it is to identify it as connected to the organization.
- **Mapping potential physical vulnerabilities with digital security impacts:** Document potential vulnerabilities to the

organization's information security based on physical aspects -- e.g. unencrypted devices which could be stolen, written passwords, or even wireless network metadata.
- **A Day In the Life:** Have staff walk you through a usual "day in their life" showing you what devices they use, how they use them, and what data they have to interact with to conduct their work.

OUTPUTS

- Notes on specific unsecured servers, workstations, and digital storage media.
- Access controls to the office
- Travel policies and practices
- Remote work and other external / non-organizational device access to organizational data.
- Depending on the risk level of the organization, observations on digital media (USB sticks) and digitally-related items (print-outs)
- Office Map with potential vulnerable locations and the extent of wifi access outside of the controlled office space.
- Discussion of potential risks associated with broadcast wireless data.

OPERATIONAL SECURITY

- Any physical notes taken on physical security should be destroyed. Digital notes should be kept in line with overall SAFETAG standards.
- Note relevant laws regarding wireless signal monitoring.
- Ensure and mapping tools used do not themselves leak or share data

PREPARATION

RESOURCES

- *Guide:* "Step Zero: The Go / Don't Go Decision" (Level-Up)
- *Standard:* "PGP and Other Alternatives" (The Penetration Testing Execution Standard: Pre-Engagement Guidelines)
- *Guide:* "Participant Security" (SaferJourno)
- *Guide:* Operational Security Management in Violent Environments
- *Guide:* "Workbook on Security: Practical Steps for Human Rights Defender at Risk" (Frontline Defenders)
- *Guide:* "Protect your Information from Physical Threats" (Frontline Defenders)

ACTIVITIES

GUIDED TOUR

Summary

During this component an auditor tours the audit location(s) and flags potential risks related to physical access at that location.

Overview

Have your point of contact walk you around the office (often as part of introductions on the first day) - mentally note physical security concerns. Document how difficult it would be for a visitor or after-hours break-in to access sensitive systems. Identify physical assets with sensitive content, such as:

- Networking equipment and servers
- User devices (workstations/laptops, smarthpones, USB drives)
- Sensitive information or external storage drives lying on desks
- Accounts/passwords written on post-its, white-boards, etc.
- Unattended, logged in computers
- Unlocked cabinets, computer rooms, or wiring closets
- Network ports that are not in use, especially ones not in plain sight

This can be done remotely via secure videoconference over a smartphone or tablet that can moved around the office easily.

Combining this activity with Office Mapping helps to reduce the awkwardness of taking notes while walking around the office, and if being done remotely, the two separate activities can be used to cross-verify the accuracy of each.

Materials Needed

- A camera and/or notepad may be useful
- For remote support, a secure and portable videochat system (such as Signal) which works with the available bandwidth.

Considerations

- Any physical notes taken on physical security should be destroyed. Digital notes should be kept in line with overall SAFETAG standards.
- Any remote communication on physical security should be done over secured channels from a private space
- It should be noted that SAFETAG is focused only on the digital impacts of physical security. This guide does not provide a full physical security assessment.

Walkthrough

As part of your first day, have your point of contact walk you around the office - this is primarily a chance to understand the office layout and meet the rest of the staff, but take mental note of the devices in use and laying out on desks as you walk around the office. Note as well the location and access to components such as servers and networking components. Taking actual notes may make the staff feel that you are judging them, especially if this is your first interaction -- refrain from this, and if needed, also consider a more "neutral" note-taking process by integrating the Office Mapping activity.

If the auditor is unable to go to the office (or can only visit one of multiple offices), consider having the point of contact use a video call. You will want to have the entire staff be aware of this activity and know the person who is walking around the office. This requires sufficient bandwidth (and unmetered or low-cost) for a 1-hour video call. This could be scheduled for before or after office hours to both discover how devices are left overnight as well as reducing the impact on the network.

Similarly, the in-person tour can also be done outside of normal business hours. Please note: this can damage the trust the staff has in the auditor, as well as unintentionally embarrassing specific staff members in the eyes of the point of contact. It is not recommended to do this except for organizations who have already received training and worked on improving their physical/operational security practices and face an active adversary. This could be before the staff arrives in the morning, during lunch, or after hours (perhaps have dinner with your point of contact, and come back to check the organization afterwards). This gives a clearer picture of how devices are secured outside of the work day (are desktops and laptops unsecured, still on, logged in?). Are backup drives or other storage media easily accessible? Are doors to server rooms/closets locked? Are keys to these locked cabinets/rooms visible?

Materials that may be useful

Recommendation

Office Equipment is unsecured against burglary

Unsecured physical network components and devices such as computers, servers, and external drives present a risk of sensitive data loss through theft, seizure, and malicious interference. Access to network compontents and servers should be limited and devices should be secured when not in use.

In the event of a burglary or office raid, an attacker could easily obtain sensitive information from devices without encryption, external hard drives, and other easily accessible items. An advanced attacker could compromise the network for later surveillance.

Secure Devices

Lock in desks or via security cables all easily portable items

Any device which connects to the organization's digital assets (and therefore has passwords or cached data) or stores organizational data (including backup drives, laptops, desktops, cameras, other storage media), should be secured (ideally out of sight, such as in a locked cabinet or desk drawer) when not in use to prevent theft and discourage seizure.

Follow the Device Assessment guidelines on drive encryption.

Encrypted drives offer the best protection against data loss from stolen or seized devices. Follow the recommendations of the Device Assessment section, paying specific attention to the need for strong passwords, automatic locking of logged-in accounts, and the importance of turning a machine off to fully benefit from drive encryption.

Place core network components and servers in a locked space.

Direct access to servers and network components such as routers, cablemodems, patch panels and switches provides an adversary multiple ways to extract sensitive information and cause extensive, yet hard to detect, damage. Ensuring that not only are these physically protected, but that there are organizational policies around which staff have access to them is critical - a locked cabinet that always has the key in the lock does not provide security. If a particular component needs, for example, regular rebooting, creative solutions should be found to balance security and staff needs.

De-activate unused network ports

Hard-wired network ports tend to connect directly into the most trusted parts of a network. De-activating any that are in public areas of the office (front desk, conference rooms, break rooms), as well as any that are not needed is recommended.

OPERATIONAL SECURITY SURVEY

Summary

This activity helps the auditor assess the organization's current operational security policies and practices through in-person or remote surveys and/or interviews. By also requesting to review and official policies as well as conducting multiple iterations of this with different staff members, some basic verification of the practices and awareness/understanding of existing policies can be achieved

Overview

The auditor interviews and/or requests survey input from organizational representatives, requests supporting documentation (e.g. policies) as relevant, and iterates/repeats as needed.

This activity is used to solidify the auditor's understanding of the physical risks the organization faces in its work as they impact information security:

- Discuss potential risks and history
- Explore the physical office setup
- Determine access controls and related policies (who has access to what, when?)
- Determine where and when staff members work (office, cafe, co-working spaces, home, on travel/remote assignments)

This can be done entirely remotely over secure communications channels (see operational security considerations), and may be useful to be done partially or fully in advance of an in-person audit to further understand operational risks of traveling to the office location.

Materials Needed

- (optional) Survey system with appropriate security precautions and access controls
- Note-taking device that can be secured.
- For remote support, a secure videochat system (such as Signal) which works with the available bandwidth.

Considerations

- Any physical notes taken on physical security should be destroyed. Digital notes should be kept in line with overall SAFETAG standards.
- Consider the threat context if an online survey tool is used to collect information and manage data access and storage responsibly.
- Any remote communication on physical security should be done over secured channels from a private space
- It should be noted that SAFETAG is focused only on the digital impacts of physical security. This guide does not provide a full physical security assessment.

Walkthrough

This activity should build on the preparation work of the auditor, as well as the capacity assessment and context research work:

- **Capacity Assessment:** If the auditor has already completed the Capacity Assessment interview, many of the answers from its introductory "Open Up" questions (5-22) provide threat history, likelihood, and some basic policy information, and the questions grouped as "Threat Information," (58-68) go deeper into previous problems and responses. If those were not asked, they can be included here as a follow-up interview/survey.
- **Context Research:** Ensure context research has revealed whether the organization would be targeted by adversaries due to their work (e.g. advocacy, engagement in or media coverage of socially sensitive topics, etc.). Threat identification and technical context research should provide insight into likely technical capabilities of adversaries (are malware or other surillance tools used (https://sii.transparencytoolkit.org/) ? Physical surveillance/monitoring? Keyloggers?)

Once an initial interview or survey has taken place (as part of capacity assessment or dedicated to the above-mentioned questions), Send a follow-up request for any policies mentioned or referred to (travel policies, onboarding/offboarding policies for staff changes, personal device usage ("BYOD") policies, etc.). After reviewing those documents, request any additional policies those may refer to (general IT or security policies), and/or schedule a follow up interview or informal survey to dig deeper into remaining unanswered questions on the operatioal security situation of the organization as well as their adaptations to it. In the (likely) case where there are no policies governing these topics, the auditor can ask their points of contact for these discussions what the general practices are and expand and verify this through additional activities.

In creating new questions, be careful to not "lead" on security in a way that would discourage honest and transparent responses. For example, ask "Do you host community events and trainings?" instead of "Do you allow outside people into your office"?

Below are questions not already covered in the capacity assessment interview process, and after that selected questions from that process which are of particular use here.

Office layout and proximity concerns

Describe your office - is it on a floor of a building? An entire floor? (What level of the building?) How close are other buildings? Is it a shared, open office space or co-working space? (shared network? open access?)?

Has the organization dealt with robberies/theft, break-ins, or office raids? If so, what happened, when, and how did you respond (or do you have a policy or contingency plan? When was that last reviewed/updated?)

What other wifi networks can you see? (See https://wigle.net/)

Physical Access Controls

Do you consider your office space to be secure?

- [ ] No
- [ ] Yes

Who has independent access to the office space, and routine after-hours access (i.e. who is able to unlock the space). This may include security, cleaning or other building service personnel.

Do you have policies and procedures for authorizing and limiting unauthorized physical access to digital systems and the facilities in which they are housed?

- [ ] No
- [ ] Yes

Describe the measures to restrict physical access to the following

- Servers (Data server, Internet server, etc)
- User workstations/laptops
- Network devices (eg routers, switches, etc)
- Printers

Do your policies and procedures specify the methods used to control physical access to your secure areas, such as door locks, access control systems, security officers, or video monitoring?

- [ ] No
- [ ] Yes

Device Controls

Do you have procedures for physically securing portable devices such as laptops and mobile phones?

- [ ] No
- [ ] Yes If yes, please highlight them

Do you have a key personnel responsible for the security of digital resources?

- [ ] No
- [ ] Yes

Do you have policies covering laptop security (e.g. cable lock or secure storage)?

- [ ] No
- [ ] Yes

Are there procedures to automatically lock digital devices if left unattended for sometime?

- [ ] No
- [ ] Yes If yes, what are the procedures?

Emergency Planning

Do you have a business continuity plan in case of serious incidents or disaster to your digital resources and is it current?

- [ ] No
- [ ] Yes If yes, please highlight the steps taken.

Does your plan identify areas and facilities that need to be sealed off immediately in case of an emergency?

- [ ] No
- [ ] Yes

Are key personnel aware of the plan and how to respond to the emergency?

- [ ] No
- [ ] Yes

Programs and staff

- Do you host events or trainings at the office? Open "cybercafe" or community meeting space?
- Do you host 1:1 meetings with funders, partners,
- Do staff work from or meet at homes or cafes/restaurants?

Selected questions from the Capacity Assessment Interview, "Open Up" section:

- What issues does the organization work on? Are these issues sensitive where you work?
- Where does your organization have activities?
- Does the organization have activities in more than one (city/provence/country/region)?
- What kind of funding does you organization receive?
- Does the organization have its own office space?
- Does the organization have a domain name or brand identity that is used for all online communications?
- Does the organization have a staff member responsible for working with digital or mobile technology?
- How regularly do staff members of the organization travel outside of your country
- Does the organization do any of the following activities when travelling internationally
- Run programs
- Participate in events
- Run trainings
- Receive trainings
- Fundraising

From "Threat Information"

- To your knowledge, how often do the below incidents occur in the geographic areas or issue areas in which your organization is active? Could you please tell me if you think they happen never, sometimes or often
    - The government lawfully intercepts information communicated by civil society or private person
    - The government lawfully confiscates equipment because of the information it contains
    - Government, public officials, non-state actors, police or security forces use digital or mobile technology to identify and target individuals for arrest or violen
    - Government, public officials, non-state actors, police or security forces use digital or mobile technology to attack the reputations of individuals or organizations

- To your knowledge, how often do the below actors use digital or mobile technolog to target or to identify individuals for arrest or violence? Do they use it never, sometimes, or often?
    - government or public officials
    - non-state actors (corporations, social groups)
    - police, security forces or paramilitary groups
- And how often would you say that these actors use digital or mobile technology to monitor or gather information on civil society activities? Never, sometimes, or often.
    - government or public officials
    - non-state actors (corporations, social groups)
    - police, security forces or paramilitary groups
- What do you feel are the most immediate and serious digital threats to the organization?
- How much risk do you feel each of these digital threats presents to your organization?
    - Online surveillance
    - DDOS (Distributed Denial of Service) Attack
    - Targeted for physical violence on the basis of digital activity
    - Data loss
    - Other.
- Do you feel that any of these threats place the physical security of your staff in danger?
- Do you feel that any of these threats place the physical security of your stakeholders in danger?
- Do you feel that any of these threats place the physical security of your beneficiaries in danger?
- In the last six months, have you or any of your civil society peers experienced any of the following?
    - Intimidation or threats of violence by public officials, police or security force
    - Intimidation or threats of violence by private or non-state actors.
    - Threats of arrest or detention
    - Arrest
    - Threats of Torture.
    - Confiscation of equipment
    - Threats to administrative standing, such as stripping individuals of professional accreditation or organization of licenses
    - Other
- How has your organization responded to these threats?
    - Addressed the issue in the press/online
    - Told other organizations about the threat
    - Contacted the authorities
    - Trained staff to prevent and mitigate such threats in the future
    - Requested help from other organizations
    - Invested in hardware
    - raised funds
    - has not responded
    - other
- Has the organization taken any of the following steps to prepare against digital or physical threats?
    - Staff have been trained
    - There are specific plans in place for specific situations
    - Equiptment and/or supplies have been made ready
    - Other

From the Technical Only section:

- Are Disaster Recovery Procedures in place for the application data?
- Are Change Management procedures in place?
- What is the mean time to repair systems outages?
- Is any system monitoring software in place?
- What are the most critical servers and applications?
- Do you use backups in your organization?
- Are there any data/devices that are not backed up?
- Are backups tested on a regular basis?
- When was the last time the backups were restored?

Recommendation

See recommendation section in the Guided Tour activity.

For useful organizational policy recommendations, review the SANS Information Security Policy Templates

OFFICE MAPPING

Summary

This activity seeks to identify potential physical vulnerabilities to an organization's information security practices by documenting the current physical layout of the office and the locations of key assets, as well as potential "external" risks such as nearby/shared office spaces.

This can be done in person independently or alongside the "Guided Tour" activity, and can also be done in advance of an assessment or remotely by a willing staff member who knows where these assets are located (often a technical or administrative staff person). This can also be conducted in a multi-office or home-office environment where the auditor is unable to visit every location.

Overview

In this activity, the auditor or the organization draws a map of the office space and notes locations of potentially valuable information or assets.

This activity can be paired with the Guided Tour activity, to reduce the awkwardness of taking notes while walking around the office during the Tour, and if being done remotely, the two separate activities can be used to cross-verify the accuracy of each. This can also be done by an organizational point of contact in advance to provide additional preparation for the auditor.

Materials Needed

- Notepad and/or simple drawing or floorplan software
- A willing participant (auditor, staff member) who is known to the staff able to walk around and map the office.
- A camera (see operational security considerations)

Considerations

- Any physical notes taken on physical security should be destroyed. Digital notes should be kept in line with overall SAFETAG standards.
- The location of certain high-value assets is highly sensitive, and may be controlled/secret information. Handle with care when discussing with the organization, and if conducting this remotely/in advance, ensure the point of contact can handle and destroy the data responsibly.
- If using drawing software, note that using free online tools could easily leave sensitive data exposed. Offline tools such as LibreOffice Draw, Pencil, or even Microsoft Powerpoint or Visio all work, but the product should be securely managed.
- Any photos taken (of the map drawing or specific office areas/rooms) should be securely deleted or taken using a secure camera app such as ObscuraCam
- It should be noted that SAFETAG is focused only on the digital impacts of physical security. This guide does not provide a full physical security assessment.

Walkthrough

Walk around the office and draw a map of the floor-plan (do not rely upon memory). Consider taking photos of specific areas (e.g. confusing layouts or areas difficult to capture in drawing). Make notes of where intruders could gain access to the office, where sensitive data may live (in the executive director's desk, in a storage closet, on devices), and relevant other items. Also note the overall privacy that the office provides (is it a shared office space, shared building, etc.)

Note the locations of any of the following that apply:

- Office rooms and storage:
- Meeting rooms
- Staff offices/desks
- Paper File Storage, such as human resources and financial records storage
- Closets
- Safe room
- Main entry to office
- Additional Entry/Exit doors
- Windows accessible to the outside (terraces, ground floor, etc.)
- Fire escapes
- Basement/Roof access
- People (staffing varies widely, adapt as relevant)
- Executive Director
- Other directors
- Financial lead
- Human resources lead
- Team leads
- Office admin
- IT staff
- Additional staff
- Infrastucture and Devices:
- Fuse box / electricity mains
- Cable/DSL modem
- Router / network switch
- wifi access points and "repeaters"
- printers/scanners
- Paper shredder
- Servers (fileserver, email, backup, etc.) and/or desktop/tower computers (which never leave the office)
- Digital backups (tape drives, hard drives, "time machines" etc.)

If doing this activity remotely and/or in advance of an audit, it may be useful to have multiple staff members independently draw maps and to provide the organization with additional guiding questions:

- If you were playing hide and seek, where would be the best place to go? how they enter /exit, whwere they store stuff (clkosets, etc.)
- What is nearby the office? Is it in a shared/open/co-working space? Is it in an office building? A home? An apartment? What floor of the building is the office on? What else is nearby (other offices? Residential buildings, restaurants/cafes)?
- If you discovered your office had been broken in to, what would your first guess of where or how the burglar broke in be?

Recommendation

See recommendation section in the Guided Tour activity.

Summary

This activity assists in identifying potential physical security concerns at an organization, particularly when an auditor cannot travel to the office location or cannot visit every office location. The scavenger hunt approach is focused on involving the organization staff members into mapping out potential threats based on the abstraction and the gamification of the physical security mapping process. See the "Risk Hunting" exercise in SaferJourno, page 19, for additional ideas and guidance on conducting this activity.

Overview

A local facilitator is required to lead this "scavenger hunt" where staff members seek out potential physical security challenges themselves. This activity should only be conducted within an environment with a high level of trust and consent. The auditor should get the agreement from the host NGO to involve all staff members into the exercise to avoid causing trust issues. By involving the staff members in identifying physical security risks, you are also taking a step forward to increase awareness on these issues.

With facilitation, staff members will explore their own office looking for potential physical security risks and share results. To reduce the risk of individual staff embarrassment, they will first review their own working space and secure it before looking around other parts of the office. The facilitator, in consultation with the auditor and the organizational point of contact may declare some areas "off limits"

Materials Needed

- (Optional) Mobile phone cameras (see operational security considerations)
- Notepad + Pen for each staff member
- Printout of example security risks
- Encrypted file sharing platform (Signal)

Considerations

- Reset credentials found during the process.
- Any photos taken (of the map drawing or specific office areas/rooms) should be securely deleted or taken using a secure camera app such as ObscuraCam. Photos of keys in particular can be used to duplicate a key. The instructions below simply use notepads to track concerns, reducing this risk but possibly being less impactful.
- Any physical notes taken on physical security should be destroyed. Digital notes should be kept in line with overall SAFETAG standards.
- The location of certain high-value assets is highly sensitive, and may be controlled/secret information. Handle with care when discussing with the organization, and if conducting this remotely/in advance, ensure the point of contact can handle and destroy the data responsibly.
- It should be noted that SAFETAG is focused only on the digital impacts of physical security. This guide does not provide a full physical security assessment.

Walkthrough

The auditor should first meet with the facilitator (possibly over secure videochat) to brief them on the activity and map out potential challenges (particularly around trust, organizational hierarchies, and any potential repercussions).

The auditor then prepares a checklist of physical vulnerabilities with the facilitator, based on the current understanding of the organization's assets and the context they are operating within. The auditor, facilitator, and organization point of contact

should decide if any areas are "off limits." Note that this is only a list of a suggestions. As with the "Risk Hunting" exercise in SaferJourno, and it should be modified to fit the requirements, assets, and threats the organization faces:

- Open windows.
- Door with key hanging from the lock and/or unlocked doors to secure areas
- Unlocked access to networking equipment - routers, wifi, modem / cablemodem / servers
- Unsecured Laptop(s) (e.g. no locked cabinet for overnight storage, no cable lock)
- Computer left unattended with active Outlook, Gmail, Skype or other communication application open and visible.
- Wires or cables for devices that have been strewn on the floor where someone would need to step over them.
- Portable backup drives, USBs, and/or other external hard drives on desktops or plugged in to computers
- Passwords written on a “sticky note” or other paper taped to a monitor or onto the surface of a desk.
- Smartphones, cameras or other valuable devices left unattended

At the organization, the facilitator explains the activity to the organization members. To balance the need for consent with the benefits of identifying actual daily practices which may need improvement, the staff should already be aware that examining physical devices is part of the audit scope, but not the specific activity. Staff will be able to first identify and address their personal concerns before others.

- Each staff member will get a paper and a pen to note the physical vulnerabilities that they notice (cameras/cellphone cameras can also be used, note the operational security considerations listed).
- For each vulnerability noted, the staff member will get a point. The facilitator should encourage staff to also look for other, not listed, vulnerabilities. For vulnerabilities that staff members suggest which were not listed; if they can explain how that vulnerability would realistically be exploited, the facilitator can award a point.
- If possible, a prize should be provided to the "winner" with the most points.
- Staff must first check their own desks for 5-10 minutes total:
  - Review the physical security of their work space.
  - Take pictures or notes on their findings
  - Fix each vulnerability they found
  - Report back to the facilitator
- In the entire office space, staff members will spend 15 minutes to:
  - Review the physical security of other desks, meeting rooms, shared spaces etc...
  - Take pictures or notes on their findings without touching anything
  - Report back to the facilitator
- Debrief:
  - After the "hunt" time is up, the facilitator should gather the staff back together.
  - The facilitator will gather the notes and review quickly for any high-risk or embarrassing findings. If those exist, the facilitator should privately tell the finder to not bring that up in discussion
  - The facilitator can lead a discussion on interesting findings, but focus on moving towards changes in practice and policy for the organization to consider.
  - If possible, quickly calculate scores and announce the winner
- Reporting:
  - The facilitator should combine the notes and communicate them securely to the Auditor, and securely destroy the notes.

Recommendation

(See "Guided Tour")

MONITOR OPEN WIRELESS TRAFFIC

Summary

It can be valuable to to listen to broadcast wireless traffic at the physical office location, even before knowing anything about the organization's network itself. This outside, passive information gathering can reveal a surprising amount of data on not only what devices are connecting to which networks, but also what type of devices they are (based on their unique

MAC addresses), and what other networks those devices have historically connected to. These probes can reveal personal, organizational, locational, and device information that, taken in context, can be dangerous or lead to other vulnerabilities.

Overview

Each wireless device maintains a "memory" of what networks it has successfully connected to. When it is connecting to a network, it sends out "probes" to all of the networks it has in this memory. It is important to note that this data gets broadcast widely, and can be collected without any network access, only proximity to the device.

These network probes can often contain names (especially from mobile phone tethers), organizational affiliations, device manufacturers, and a mixture of other potentially valuable data (home network names, recent airports/travel locations, cafés and conference networks). If there are many networks in the office's vicinity, this activity can also help identify the specific office network (if there is any doubt). In many cases, an organization may not want the name of their wireless network to be associated with to their organization, but it may be revealed by this additional meta-data.

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.

- Scan for wireless networks nearby, identify (and confirm) the office network(s).
- Monitor traffic of that network and capture potentially sensitive metadata (wireless security settings, beacons, and MAC addresses).
- Research likely device hardware using MAC addresses.
- Do the staff devices leak sensitive metadata?
- What can be determined about the organization based on broadcast wireless data?

Materials Needed

- Wifi card (and drivers) that can be set to monitor mode.

Considerations

- Despite this exercise covering only broadcast data, check the local laws which might cover this process before conducting it.
- Consider how it looks to third parties as you are scanning a network, especially from outside an office.
- Confirm that all devices you are accessing/scanning belong to the organization.
- Delete all devices from your scan that do not belong to the organization.
- Study outputs for any obviously embarrassing personal information (especially network beacon records) before sharing.

Walkthrough

Step 1: Monitor Mode

You should disconnect from any wifi network you may be connected to to capture the widest amount of data.

Switch your wireless adapter to monitor mode**

```
$ airmon-ng start <interface>
```

You may need to stop your network manager system to prevent it from interfering. Running

```
$ airmon-ng check
```

to list anything that is causing problems, and

```
$ airmon-ng check kill
```

to try and stop them automatically, and running stop network-manager && stop avahi-daemon may keep them from re-starting automatically.

Step 2: Listen for wifi probes.

Run airodump-ng on the monitor mode interface (usually mon0). This listens to wifi beacons and you can begin analyzing who is on what network, and see historical networks.

```
airodump-ng -w filename mon0
```

This scans all networks and channels, collecting broadcast network information. Note that, despite its broadcast nature, this is privacy invasive and can be considered illegal: http://www.slate.com/blogs/future_tense/2013/09/16/google_street_view_wi_fi_snooping_case_good_news_and_bad_news . You can restict this to a specific channel or base station ID (BSSID) with -c and --bssid:

```
airodump-ng -c 1 --bssid 00:11:22:33:44:55 -w filename mon0
```

Step 3: de-auth (optional)

Send de-authentication packets to force clients to reconnect and send out additional probes. Take note that by its very nature, de-authentication causes annoying interruptions to wifi traffic. **This breaks connections, drops skype calls, and can make the wireless network temporarily unusable -- Make sure to check with staff before going through this** (to make sure no one is doing a live webcast or on an important VOIP call, and to expect some network instability).

```
$ aireplay-ng -0 1 -a 00:11:22:33:44:55 -c AA:BB:CC:DD:EE:FF mon0

15:54:48  Waiting for beacon frame (BSSID: 00:11:22:33:44:55) on channel 1
15:54:49  Sending 64 directed DeAuth. STMAC: [AA:BB:CC:DD:EE:FF] [ 5| 3 ACKs]
```

This command de-authenticates one targeted user with one attempted deauth packet. "-0 10" would try 10 times (potentially disconnecting the user multiple times!). With permission, you can also target all users on a network by leaving out the "-c ..." flag.

There are scripts, like wifijammer, which use this same approach to jam *all* wifi connections in range of the attacking computer, so check against the documentation at http://www.aircrack-ng.org and act responsibly to protect yourself and the organization.

Step 4: MAC Address Research

The first three hex numbers of each MAC address designate the vendor, which can reveal useful information in matching MAC addresses to devices. The MAC address is a unique identifier, so never post or search using the full address. Note that increasingly, devices are using MAC address randomization, but if it implemented, it often is poorly implemented against even minimally determined adversaries, as per this 2017 research study .

To compare found MAC addresses to the bendor database offline you can download the full vendor database from IEEE or use the Wireshark list

Step 4: Ongoing Monitoring

The longer you leave this running (particularly when staff are first entering the office or returning after lunch/meetings), the better sense of what devices are connected to the network you will get.

Watch what probes the various devices are sending out (especially when they are deauthenticated, as above). You will see each computer on the network, as identified by their mac addresses, broadcast information about previous networks to which they have connected.

```
BSSID              STATION            PWR   Rate    Lost    Frames Probe

00:11:22:33:44:55   0F:3E:DF:DA:2D:E2   -67 0    0   234567  SampleOrg,linksys,John Smith's iPhone,Free Public Wifi
00:11:22:33:44:55   F8:7E:FC:03:CC:43   -80 -24 0   234567  amygreen,SampleOrg,android-hotspot,Starbucks,united_club,Dulles Airport WiFi
00:11:22:33:44:55   F8:19:F3:DF:75:19   -58 -54 0   234567  SampleOrg
00:11:22:33:44:55   38:08:95:EB:7E:0B   -75 -12 0   234567  HolidayInn,SampleOrg,John Smith's Mac mini,android-hotspot
```

Recommendation

Recommendation: Cleanse wifi network connection history

For most devices, deleting networks from the “saved” network list will stop them from being probed. Obviously, this can be an annoyance for networks you regularly connect to, so renaming these networks to non-revealing names would help, as would creating non-name-associated “guest” networks for colleagues connecting to your home network.

On iPhones and iPads, it is not possible to selectively remove historical networks unless you are currently in range of that network. It is however possible to remove all history: go to Settings > General > Reset > Reset Network Settings . When you take this step, it is worth going through this reset multiple times – approximately once per year of device ownership, as the first reset appears to only remove recently-connected networks, and older networks will be broadcast.

Recommendation: Use innocuous network names

Organizations may want to choose innocent or generic network names, and/or not broadcast network names. It is worth noting that devices seeking out hidden networks will "beacon" for the actual network name, so this has extremely limited security use and must be combined with other protective measures. See this Acrylic blog post for further details.

It is worth noting that wifi access points are also tracked to assist in location services, and as such the location of a wireless network can be learned from its name or the MAC address of the access point. WiGLE is a community-managed database for such information, but both Google and Microsoft, and likely many others, also track this locational information, so the opt-out information below is only minimally useful.

Removal options: See wikipedia for public listings. Some opt-out options exist below:

- WiGLE: WiGLE's FAQ: "To have your record removed from our database, or if you have any questions or suggestions, send an email to: WiGLE-admin [at] WiGLE.net […] include the BSSID (Mac Address) of the network in question!"
- Google Location services : https://support.google.com/maps/answer/1725632?hl=en
- Mozilla Location Services: follows the Google standard of adding _nomap to a wifi name.
- Microsoft Location Services: https://support.microsoft.com/en-us/help/20039/opt-out-of-location-services ; See also using _optout and blocking wifi login information in Windows 10

- Apple: No clear opt out, more information: https://www.apple.com/newsroom/2011/04/27Apple-Q-A-on-Location-Data/
- Skyhook: http://www.skyhookwireless.com/opt-out-of-skyhook-products

WIRELESS RANGE MAPPING

Summary

This component allows the auditor to show the "visibility" of an organization's wireless network to determine how far the organization's wireless network extends beyond a controlled area. Wireless networks are often trusted as equivalent to the hardwired office networks they have largely replaced, but they have important differences. Wireless networks are often "visible" from outside the walls of the office - from common spaces or even the street. Without further access, this reveals a wealth of information about the organization's size and the type of devices connecting to their network.

Overview

This component consists of wireless scanning and wireless signal mapping. It is useful for organizations with offices in shared spaces/buildings/apartment complexes or near locations where an adversary could easily "listen" to network traffic. In conjuction with Monitoring Open Wireless Traffic exercise, it can also identify devices using that network. It is useful to do this in parallel with Office Mapping to build a more comprehensive view of the information assets of the organization.

- Identify and verify the network(s) belonging to the organization
- Create a map or photos indicating the range of each relevant wireless access point.

Materials Needed

- A portable wireless device (like an Android phone/tablet) is useful to map the network boundaries without causing undue suspicion. Some Apps like Wifi analyzer and Wifi Mapper can help.

Considerations

- Despite this exercise covering only broadcast data, check the local laws which might cover this process before conducting it.
- Consider how it looks to third parties as you are scanning a network, especially from outside an office.

Walkthrough

Map the range of the organizations wireless network outside of office space, using wifite or other tools to track network strength.

A variety of apps and tools can support this work without reosting to professional "wifi site survey" tools. If the Office Mapping exercise has taken place, that map can serve as the starting point to expand the map outside the office. If using a third party tool or app, ensure that the app is not sharing sensitive data. Using simple signal strength monitors in combination with location notes is more than sufficient. In Linux systems, one can use wavemon, kismet, wifite, and even the networkmanager command line tools to track visible networks and their strengths as described on StackExchange:

```
watch  "nmcli -f "CHAN,BARS,SIGNAL,SSID" d wifi list ifname wlx10feed21ae1d  | sort -n"
```

- https://www.netspotapp.com/ (OSX, Windows, free for non-commercial uses)
- http://wifianalyzer.mobi, http://wifiheat.com/ (Android)

Recommendation

Depending on office layout, moving the wireless access point may help to reduce how far the network is transmitted outside of the office space, and changing devices which do not move to better enable this without loss of functionality.

See also Monitoring Open Wireless Traffic recommendations and Network Access security recommendations.

A DAY IN THE LIFE

Covered in full in User Device Assessment:

- Integrated with other activities/interactions, interview staff on their usage of technology and remote services

PROCESS MAPPING AND RISK MODELING

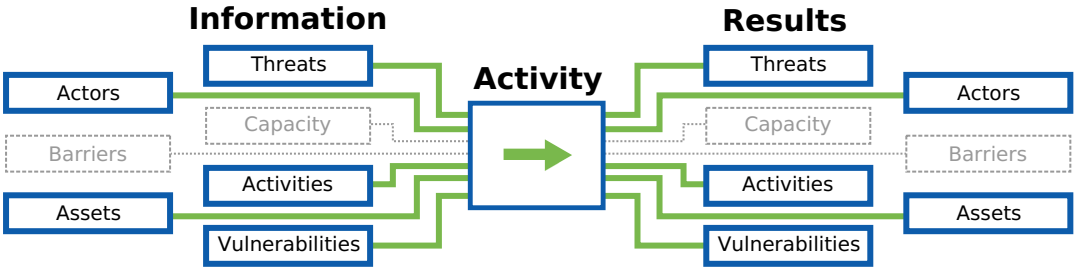
SUMMARY

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. [73] 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.

THE FLOW OF INFORMATION



Risk Modeling Information Flow

GUIDING QUESTIONS

- What are the critical organizational activities?
- What threats does the organization, its programs, partners, and beneficiaries face?
- What would the impact of these threats be if they were to occur?
- What adversaries (people or groups) may attempt to carry out threats?
- Are those adversaries capable of carrying out these threats?

APPROACHES

- Process and/or data mapping exercises
- One-on-One interviews with staff to supplement other group activities.
- Risk identification based on process or data mappings
- A classic group Risk Assessment Activity.

Note: Risk modeling will require a mixed approach of exercises, and the order which you identify each component will vary depending upon the organization.

If it was not possible to conduct these activities in person, you can conduct them remotely through applying one of the remote facilitation approaches described in the Remote Facilitation appendix.

OUTPUTS

- Maps of critical processes.
- A list of organizational assets.

OPERATIONAL SECURITY

- Ensure that any physical notes/drawings are erased and destroyed once digitally recorded.
- Ensure that any digital recordings of this process are kept secure and encrypted.
- Consider who has physical and visual access to the room where this process takes place, and if the room can be secured if this activity may span long/overnight breaks.

PREPARATION

- Risk Modeling and Proccess Mapping exercises can be intense and challenging to facilitate. Prepare and review your exercises, and plan for how they will flow together. Note your specific desired outcomes to easily recover or re-direct the activity based on emergent needs.

RESOURCES

- *Overview:* "An Introduction to Threat Modeling" (Surveillance Self-Defense)
- *Guide:* "Risk Assessment" (Workbook on Security: Practical Steps for Human Rights Defenders at Risk - Chapter 2)
- *Guide:* "Threat Assessment: Chapter 2.5 p. 38" (Operational Security Management in Violent Environments (Revised Edition))
- *Guide:* "Defining The Threshold Of Acceptable Risk" (Integrated Security)
- *Guide:* "Guide for Conducting Risk Assessments" (NIST 800-30)
- *Report:* "Risk Thresholds in Humanitarian Assistance" (European Interagency Security Forum)

Threat Modeling Resources (General)

- *Book*: "Threat Modeling: Designing for Security" (Adam Shostack)
- *Website*: "An Introduction to Threat Modeling" (Surveillance Self-Defense)
- *Article:* "Security for Journalists, Part Two: Threat Modeling" (Jonathan Stray)
- *Guide:* "Managing Information Security Risk: Organization, Mission, and Information System View" (NIST)
- *Guide:* "Guide for Conducting Risk Assessments" (NIST)
- *Activity:* "Threat Model Activity" (Tow Center)

Risk Assessment Activities

- *Guide:* "Risk Assessment" (Operational Security Management in Violent Environments (Revised Edition) - Chapter 2)
- *Guide:* Risk Assessment (Workbook on Security: Practical Steps for Human Rights Defenders at Risk - Chapter 2)
- *Book*: "Pre-Mortum Strategy" (Sources of Power: How People Make Decisions - p.71)

Threat Assessment Activities

- *Guide:* "Threat Assessment: Chapter 2.5 p. 38" (Operational Security Management in Violent Environments (Revised Edition))

Example text for introducing threats - Integrated Security

Written exercise: Threats assessment - Integrated Security

Facilitators Manual (With PDF download of "Threat Introduction Example Text" and "Threat Assessment Written Exercises") - Integrated Security

Analyzing Threats: Chapter 3 - Workbook on Security: Practical Steps for Human Rights Defenders at Risk

- *manual:* Establishing the threat level of direct attacks (targeting) (Protection Manual for Human Rights Defenders)

Risk Matrix Activities

- *Guide:* "Defining The Threshold Of Acceptable Risk" (Integrated Security)
- *Guide:* "Risk Analysis: Chapter 2.7 - Operational Security Management in Violent Environments (Revised Edition)" (HPN - Humanitarian Practice Network)

Risk Assessment: Chapter 2 - Workbook on Security: Practical Steps for Human Rights Defenders at Risk

Alternative Risk Modeling Activities

- *Article:* ["Operational Security Management in Violent Environments (Revised Edition)
- Chapter 2 Risk assessment"](http://www.odihpn.org/index.php?option=com_k2&view=item&layout=item&id=3159) (HPN - Humanitarian Practice Network)

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

- *Guide:* "Risk Assessment For Personal Security" (CPNI - Centre for the Protection of National Infrastructure)s
- *Guide:* "Threat Assessment & the Security Circle" (Frontline Defenders)
- *Case Study:* "Case Study 1 Creating a Security Policy" (Frontline Defenders)

ACTIVITIES

PROCESS MAPPING

Summary

This activity helps to identify the processes that allow the organization to function (publishing articles, payments, communicating with sources, field work etc) the assets and systems (websites, software, PayPal accounts) they rely on, and which ones are critical to their work.

Participating organization/s are asked to "brain-storm" a list of all the processes that are critical for their work and the auditor works to map the details of critical processes out to expose points of risk.

If done correctly, process mapping can help the auditor - Identify risk exposure - Communication issues and effective incident response - Identify what are affected (people, systems, technologies) - Identify areas of improvement in securing organization's process - Generate a mitigation/solution plan for missing security controls - Show the importance of digital security to staff, management team and stakeholders

Overview

- Brainstorm with staff on the organizational processes -- Try to make sure that everyone is present as the processes mapping involves them who use the process. Depending on the size and structure of the organiation, it may be valuable to have a separate meeting per team or with the staff separate from the management.
- Identify a smaller sets of processes which are mission critical. Preparatory research into the organization and its activities will help you guide towards particularly critical processes such as:
- Communicating with sources
- Sending sensitive information to colleauges and 3rd party organizations
- Managing online accounts/presence (website security, social media accounts)

- Access to organizational resources (e.g., Organizational funds, banking etc)
- Finish the process mapping first - take note and park the discussions of improvements after
- It is common for participants to resolve issues, discuss exceptions and errors during the activity
- Map the basic process first, then go back the exceptions and errors. You can't prioritize until you have the whole picture
- Completely mapping interactions and events that compose a process will lead you to the areas that are expose to risks
- Put everything in a drawing board
- Modifying & changing a flow in a process is easy and more chance to change. It can also make the participants interactive.
- Slides looks formal and official, and somehow difficult to change and modify

If it was not possible to conduct these activities in person, you can conduct them remotely through applying one of the remote facilitation approaches described in the Remote Facilitation appendix.

Materials Needed

- Stickies
- Markers
- Whiteboard or flip-chart

Considerations

- Treat device assessment data as well as any additional service information learned with the utmost security
- Ensure that any physical notes/drawings are erased and destroyed once digitally recorded.
- Ensure that any digital recordings of this process are kept secure and encrypted.
- Consider who has physical and visual access to the room where this process takes place, and if the room can be secured if this activity may span long/overnight breaks.

Walkthrough

- **List all organizational processes:** The goal of this exercise is for the auditor to lead the host participants in "brain-storming" a list of all the processes the organization takes part in to carry out their work. It is important to remember this is a brainstorming session of all of the processes that occur in the organization. To get started, the auditor may find it useful to give the participants a few examples such as:
    - Research gathering and source management
    - Editing / Publishing
    - Outreach and advocacy
    - Paying Staff
    - Managing grants or other funding
- **Determine critical processes:** During this exercise the aim is for the auditor to lead the attendees in narrowing down the subset of activities to those that are crucial to their work. Once the participants have brainstormed these out the facilitator leads the participants in identifying critical processes (this may be all of the processes identified).
    - Quickly identify the main purpose of the organization.
    - Once a complete list has been created, the auditor will then go through through to identify with the participants the critical processes within the organization – that is, without these processes the organization would not be able to function or function at a very poor level, or would not fulfill its mission

NOTE: If an auditor does not ensure that the uniquely identified subset of processes speaks to the full range of participants, their recommendations are more likely to be met with resistance.

- **Map out critical processes:** In this exercises the auditor does free-hand drawing (ideally on a whiteboard to allow for easy changes) mapping for each process guided by the host participants. The auditor needs to make sure that they work to develop a broad understanding of the overall process. This is a time consuming activity, and managing their overall time to complete the entire needs assessment, and respect the time constraints of the staff, is critical.

- Clearly identify the process name on the whiteboard or flipchart
- Have your participants explain to you what the process is step-by-step, while making a note on the side where there will be follow on processes.
- Keep it simple to facilitate broad understanding of the OVERALL process. Too much detail early on can be overwhelming and/or lead to confusion. If you agree that more detail is required on a particular action, it is easy to highlight that box and produce a separate chart showing the process taking place within.
- Take quick notes to remind yourself of any key points not clearly marked on the map before they move on to the next activity.
- Keep track of participant engagement and reactions in case there are edge cases you may need to follow up on individually afterwards.
- After completing all the key events take a photo of the whiteboard / store the chart-paper for later documentation.

While doing this it is important to consider level of detail you will be mapping out (this should be pre-determined or established so everyone is on the same page). You will generally want to capture:

- The people involved;
- The tasks, conversations, and decisions they carry out;
- The flow of materials, information and documents between them;
- How the actions take place (email, calls, travel)
- The relationship and dependance between the steps.

- Actual processes, not idealized ones

- **Identify points of failure:** Begin to ask questions of how or why a particular process or step could be problematic or risky. Depending on the organization, you may want to do this as only mental notes to yourself or as a more interactive discussion. The goal is to improve the organization's understanding of their own processes and the risks they include.

Recommendation

This activity can lead to feelings of hopelessness; it is important to remind the staff that any risk can be mitigated, and indeed it is the goal of an audit to identify the highest priority ones based on actual likelihood and provide guidance on mitigation.

RISK MODELING USING THE PRE-MORTUM STRATEGY

Summary

The pre-mortum strategy was devised to take participants out of a perspective of defending their plans and strategies and shielding themselves from flaws. They are given "a perspective where they [are] actively searching for flaws in their own plan." [74].

Overview

- "Pre-Mortum" Activity
- Identification of critical processes
- Selected critical process mapping
- Threat Identification (Control/Confidentialy/Idenity/Integrity/Authentication/Access)
- Impact Identification
- Adversary Exploration (Likelyhood)
- Impact Ranking

Materials Needed

- Stickies
- Whiteboard or flip-chart
- Markers
- Camera to digitally capture the data

Considerations

- Treat risk modeling data with the utmost security
- Ensure that any physical notes/drawings are erased and destroyed once digitally recorded.
- Ensure that any digital recordings of this process are kept secure and encrypted.

Walkthrough

Additional Material

- Chart Paper / whiteboard.
- Marker pens / whiteboard markers.
- Multiple colors of post-its.
- Camera for documenting the process.

GETTING STARTED

- Prepare a flipchart / space on the white-board to keep track of process', threats, impacts, and adversaries that are identified during other activities. Participants can easily get ahead of the process as they explore individual ideas. Keeping a space for these "upcoming" activities will help re-center them on the activity at hand.

CONDUCTING THE ACTIVITY

Pre-Mortum Strategy: (30 Minutes) The pre-mortum strategy was devised to take participants out of a perspective of defending their plans and strategies and shielding themselves from flaws. They are given "a perspective where they [are] actively searching for flaws in their own plan." [75]

- Explain the pre-mortum activity. The participants are to imagine that it is months into the future and they have continued doing their work as normal. And something happened that left them entirely unable to function or functioning at a very poor level. "That is all they know; they have to explain what has happened." [76]
- Create a broad list of possible explanations for what has happened.
- Identify the most likely explanations.
- List the process' that would have to fail for those causes to take effect.
- Identify two to three process' that are central to the failures and write them on a list of *critical process'.*

Process/Interaction Mapping (30 minutes per process):

- Pick a process from the list of *critical processes* identified above.
- Clearly identify the process name on the whiteboard or flipchart.
- Create a list of individuals who take part in the process.
- Draw a symbol of the person.
- Write a label describing their role or title.
- Draw lines with arrows connecting individuals who interact with each other in this process.
- Label the lines with words describing the interaction.
- Write numbers on the interactions to show the order they occur in.

- Continue this activity with the next *critical process.*

- **NOTES:**
  - You can add follow-on processes to examine if they are identified as critical by the participants during this activity. Specifically, the exercises in the Threat Assessment section pair well.

- Put people on post-its to make them moveable.
- Verbally walk the participants through the completed process so you ensure you didn't miss anything.
- Take quick notes to remind yourself of any key points not clearly marked on the map before they move on to the next activity.
- After completing all the key events take a photo of the whiteboard / store the chart-paper for later documentation.

Recommendation

This activity can lead to feelings of hopelessness as well as stir up direct fears or challenges that the staff face. It is important to remind the staff that any risk can be mitigated, and indeed it is the goal of an audit to identify the highest priority ones based on actual likelihood and provide guidance on mitigation.

RISK MATRIX

Covered in full in Threat Identification:

- 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.

CRITICAL DATA ACTIVITY

Covered in full in Data Assessment:

- With staff input, post up popular places where data is kept (laptops, email, shared drives...)
- Using stickies, gather from the staff what data is kept in what locations - duplicating notes when needed
- Rank data by sensitivity
- Discuss the impact of one of the devices where data is stored being lost - are there backups?
- Discuss the impact of a device being exposed / taken by an adversary
- Identify who has access (physical access, login access, and permissions), and who needs to have access to get the organizations work completed.

RESPONDING TO ADVANCED THREATS

SUMMARY

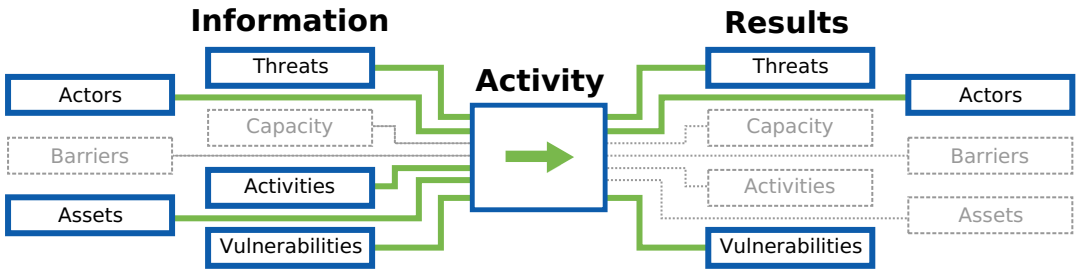
This component allows the auditor to be able to identify, triage, and analyze suspicious behavior on a device or in a network. Depending on the analysis, the auditor may need to further investigate a malware infection, or analyze a binary and determine if it is malicious or not.

PURPOSE

It is very common to find suspicious behaviors, processes, traffic and other 'weird activities' during a SAFETAG audit. SAFETAG practitioners should always be on the lookout for suspicious activities as they apply other SAFETAG methods and their activities, from interactions and discussions with staff to hands-on device assessment and traffic analysis.

Due to the limited window of time, the auditor should focus on identifying suspicious activities and triaging them rapidly. Many of these will be false positives related to other non-malicious software causing the machine to act weird or (most commonly) other type of less serious (and non-targeted) malicious software like adware. When this cannot be ruled out, collecting evidence, running basic analysis, and assessing the risk and impact against organizational priorities will help prioritize further action. In-depth binary analysis is usually best kept for post-audit work during the reporting and follow-up phases.

THE FLOW OF INFORMATION



Information Flow

GUIDING QUESTIONS

- Does the organization suspect they already have malware? If so, what evidence supports that?
- Based on the context research and the organization's activities, how likely are targeted attacks?
- How much time should be devoted to more complete analysis during the audit itself, and what other factors change that?
- What are the implications of targeted malware for the organization, and for the current assessment process?
- What types of malware should trigger an incident response approach?

APPROACHES

- **Adversary Capability Assessment** - This likely should be an output from the context research work. Are there Advance Persistent Threats which should be taken in to account? How do they operate? Are there known IOCs to look for?
- **Analyzing Specific Suspicious Events/Activities** - If the organization have specific concerns or evidence suggesting a targeted attack, the auditor can focus attention to match them against any known attacks or flag them for further research.
- **Threat Hunting** - If the organization suspect that they have been compromised, but does not have any specific, suspicious device/process/email, the auditor can leverage techniques to intelligently spend their time to investigate further.
- **In-Depth Analysis** - If malware is discovered, but cannot be identified, further analysis will be necessary. This may also trigger a change in assessment scope and/or an incident response approach.

OUTPUTS

- Identification and initial triage of suspicious processes, files, URLs, and messages (via anti-virus scanning results, VirusTotal information, network traffic analysis, and other research).
- Collection of necessary forensic evidence for further analysis (including hard disk image, memory image, suspicious files, emails, network traffic captures, URLs).
- Agreement with organization on sharing protocols (such as with malware researchers).

OPERATIONAL SECURITY

- The auditor should ensure they have a clear understanding set with the organization on an incidence response plan, points of contact, and a process to allow for safe discussions.
- Dealing with malicious software is risky, you have to be aware of the threats around it, don't infect yourself or more machines
- Don't upload files to third party services (use hashes). Take extreme care with identifying or potentially targeted information
- Use VPNs or Tor to search if conducting the search from a country that is highly competitive with the organization's country, or is known to surveil.

PREPARATION

Baseline Skills

- Knowledge of spotting malicious elements, scanning machines and cleaning them
- Ability to image a machine
- Contacts with malware analysis experts for more in depth investigation

RESOURCES

Malware Analysis

- *Guide:* "Digital First Aid Kit: Malware"
- *Guide:* "Recommendations for Readiness to Handle Computer Security Incidents" (CIRCL)
- *Guide:* "Guide to Integrating Forensic Techniques into Incident Response" (NIST)
- *RFC:* "Guidelines for Evidence Collection and Archiving" (IETF)
- *Guide:* "Electronic evidence - a basic guide for First Responders" (European Union Agency for Network and Information Security)
- *Procedures:* "The ThreatHunting Project" (ThreatHunting.net)
- *Resource Collection:* "Annotated Reading List" (ThreatHunting.net)
- *Guide:* Recovering from an intrusion (UCL Security Baselines)

ACTIVITIES

ADVANCED THREAT

Summary

Malware is a common tactic to target organizations, Malwares like RAT (Remote Access Trojan) can provide an attacker with a back-door access to a targeted machine which enables the attacker to steal information, record audio and video and run commands on the infected machine.

To stop that, you have to identify the malicious process within the system and stop it, or reformatting the machine in case you don't feel spending time on stopping the malicious process.

It's important to keep evidences, in case the auditee still have access to the original malicious software, email..etc they received, keep a copy of the file if you feel doing more investigations on it or submit it to other organization working on analyzing such issue.

Scanning the possible infected machine or the original suspicious file will allow you to save time and efforts in case the Anti-Virus knew the malware and had it in its database, also it will help you relax in case the machine was infected with a non-serious malware like adware or not infected at all.

After knowing the machine is infected you can process in helping the auditee to back up their information, scan it from malware and then reformat the infected machine, it's hard to clean an infected machine in a short window of time.

In case the machine was infected, taking an image from the operating system will allow you to replicate the infected machine and run it after you finish your audit for more in depth investigation or send it to an expert to work on investigating it. ##### Overview

- In case they still have the original binaries (Attachment, email..etc.)

    1. Download the file to your auditing machine, Scan the file via Anti-Virus or hash the file and use virustotal.com to search for it (Note, don't upload the actual file to virus total as uploaded files are discoverable by paid subscribers in most cases)

    2. Check the email's header and see if it looks suspicious

- In case there is no binaries (Attachment, email..etc.) or they have no access to it

    1. Take the machine offline

    2. In case you have time, Image the hard disk

    3. Help the auditees to operate another machine to fill the gap of the suspicious machine

    4. Run a non-depth scan for the machine and try to locate any suspicious files

    5. Collect the suspicious files, hash them, then search for them on virustotal.com

    6. Scan the open ports and monitor which applications is connected to external address

Scanning suspicious files

Scanning suspicious machines

Take an image from the hard disk

Submit the image for in depth investigation

Back up data

Reformat the machine

Transfer the data back

Materials Needed

A Linux Virtual machine connected to the Internet

VPN

USB drive

External Hard disk

Considerations

- Confirm that the device belongs to the organization
- Make sure to take the device offline before start working on it
- Don't transfer files from the infected machine to any other machines
- Use a USB drive to move files from the infected machine to your Audit machine for investigating proposes
- Study outputs for any obviously embarrassing personal information
- Don't test anything on your virtual machine without VPN
- Consider the time you have, investigating a malware can take days

Walkthrough

We will be using the following walkthrough

- Investigating a suspicious file or attachment

  In this part, you will be investigating a file and determine if it's malicious or not

Questions to ask the user / organization

* What suspicious behaviors are you witnessing on the Machine?
* What makes you feel that the machine is somehow infected?
* Do you have an alternative to this machine so you can use it until we clear things up?
* Did you receive any email, attachment or different form of communication that made you feel this way?
* Do you still have access to the original email, attachment or any form of communication?
* Can you share it with me?

- Step 1

Collect the binary from the targeted person or organization by asking them to forward you the suspicious email including any attachment in it, or by coping the file if it's still on the machine by copying it to a USB drive. In case the user did not remember where the file is located, ask the user to walk through their browsing history or download folder and try to locate the file and then copy it to your USB drive.

- Step 2

Initial investigation, in this stage you will be scanning the file using ClamAV which comes with Kali-Linux

- Update CalmAV by running the following command in the terminal `sudo freshclam`

- Create a new folder and copy-paste the suspicious (file)s inside, then scan the targeted folder by running the following command in the terminal which is going to show the infected files and give you more information about it
  `clamscan -r –bell -i /your/target/folder`

- You can also hash the file and look for it on VirusTotal using their 50+ Anti-Virus which is going to offer you a better result

After scanning the file, in case it was malicious, the result will show you what type of malware is, in case the result showed the file as Trojan, Backdoor, agent or Remote access Trojan RAT then it's time to consider taking an image from the hard drive, the original file, the header of the email and submit them for in depth investigation.

In case the organization was highly targeted with advanced attack, there will be a high probability that the attacker will use costume design malware which means no Anti-Virus will find it as malicious, in this case, and if you feel you still have doubts that a clean file is still malicious, submit it for in depth analysis.

- Step 3 (Optional)

You will need at least one hour to prepare and carry the advanced investigation. this step is optional in case you have time and you think you still have doubts about the file and you need a more advanced result. In this step, you will analyze the suspicious file using Cuckoo Sandbox, an automated malware analysis system. In case you decided to go with this option, you will need an installed Linux on your audit machine you can use this guide to install Kali Linux.

- Make sure you have that you have Cuckoo Sandbox installed on your audit Linux machine by running the following command `cuckoo`
- In case Cuckoo was not installed, follow the following instructions on how to install it. Make sure cuckoo is running without errors the previously posted documentation will provide you with details steps on how to install and run Cuckoo
- Create a new folder and copy-paste the suspicious (file)s inside
- You can use 'submit' to start analyzing the binary, you can find more options here , the easiest way to do it is by running the following command: `cuckoo submit /folder/targeted/binary`
- To view the analysis results, once an analysis is completed, you will find the result in `$CWD/storage/analyses/`
- You can find more information on how to read the results here
- Step 4

In this step, you will be dealing with infected machine by one of the binaries you analyzed in step 1 and 2, or you are sure that the machine is infected and you have no time to analyze it. In this case, you will take a backup, migrate the data safely to a new machine and take a full image from the system and submit it for more in depth analysis.

- It's better to start with taking a full hard disk image, using 'dd' a tool that takes bit-by-bit copy of the hard drive, after taking the image, you will have an identical copy of infected machine and you can send the hard drive to experts for more in depth analysis. To take the image, you will need to boot the infected machine with a Live Kali Linux and apply the following steps:
    - Identify the `<source>` which is the infected hard disk, and `<destination>` the external hard disk you will put the image on, run the following command which will list all the drive *lsblk*
    - After identifying the source and destination, apply the following command the start the process `dd if=<source> of=<destination> bs=<byte size>` *Where bs is byte size, read more about how to use dd here*
- Taking back up in this stage is to back-up all the important data and save them on a hard drive, usually it's the document, desktop, download, favorite and personal data, save them on external storage then Scan them using ClamAV or any available Anti-virus on your auditing virtual machine.

- Make sure the data is clean then transfer it to the clean replacement machine.

Threat Hunting

Threat Hunting In case you went through the entire process and still you have doubts about a file, email, process, or have other reasons to believe the organization may have undetected malware, you will probably need to work on specific threat hunting procedure that matches your needs, the organization's assets, and the threat profile of potential adversaries.

The ThreatHunting.net project, is collecting different Threat Hunting techniques on their GitHub ripo.

The provided Threat Hunting procedures will guide on how to address your doubts on specific issue which means, you have to be able at least able to identify the category of the possible threat then apply the steps provided by ThreatHunting.net project.

Recommendation

THREAT ASSESSMENT

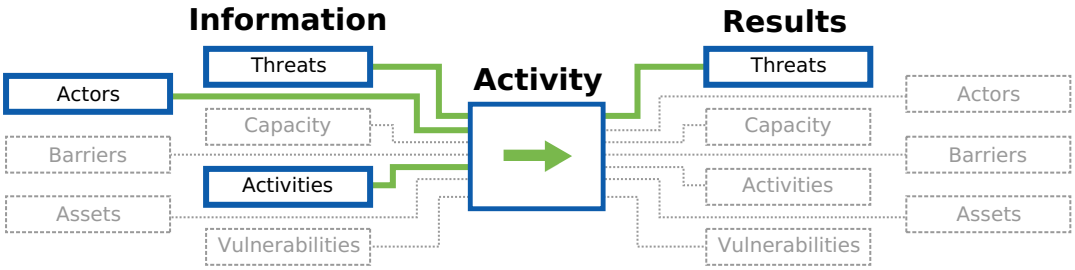
SUMMARY

This objective uses a variety of activities to identify possible attackers and gather background information about the capability of those attackers to threaten the organization. This consists of identifying a particular attacker's history of carrying out specific threats, their capability to carry out those threats currently, and proof that the threat has intent to leverage resources against the target.

PURPOSE

Checking the assumptions both of the organization and of the auditor by researching the current threats 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. With greater ownership of the process the staff provides an opportunity to explore their threat landscape and become more engaged in addressing the threats identified when the audit is complete. By engaging with as many staff as possible the auditor is providing a framework for staff to explore threat identification processes when the auditor is gone.

THE FLOW OF INFORMATION



Threat Assessment Information Flow

GUIDING QUESTIONS

- Who are potential adversaries for the organization?
- Do these threat actors have a history of attacks? Against whom?
- What types of organizations have they targeted?
- Does the threat actor have the means to leverage widespread threats against, or will they have to prioritize their targets? Is the organization a priority threat target?
- Do they have the desire and ability to conduct an attack?

APPROACHES

- **Open Source Threat Research:** Identify possible adversaries and threats using publicly available reports, news, and databases.
- **Threat Mapping:** Facilitate group activities where staff identify possible adversaries and the threats that they have/can leverage against the group.

OUTPUTS

- A host driven threat-matrix including the following:
  - **Adversaries** (threat actors) with capabilities and willingness
  - **Impacts** of attacks against **critical processes**, ranked by severity
  - **Likelihood** of each (based on adversaries)
- Latest general cyber-security threats
- Identify existing in/formal security practices that the participants use to address risks.

OPERATIONAL SECURITY

- Data generated in this component is highly sensitive - in addition to standard practices of saving only in encrypted containers and destroying physical copy versions (stickies, etc.) ans using VPNs/Tor to conduct research, also take note of the physical location where you are conducting any exercises to prevent eavesdropping/viewing.

PREPARATION

- Threat Identification works best grounded against mapped out organizational processes or a data/asset map. See the Process Mapping and Data Assessment methods for exercises to generate these.

RESOURCES

Threat Assessment Activities

- *Guide:* "Threat Assessment: Chapter 2.5 p. 38" (Operational Security Management in Violent Environments (Revised Edition))

Example text for introducing threats - Integrated Security

Written exercise: Threats assessment - Integrated Security

Facilitators Manual (With PDF download of "Threat Introduction Example Text" and "Threat Assessment Written Exercises") - Integrated Security

Analyzing Threats: Chapter 3 - Workbook on Security: Practical Steps for Human Rights Defenders at Risk

- *manual:* Establishing the threat level of direct attacks (targeting) (Protection Manual for Human Rights Defenders)

Threat Modeling Resources (General)

- *Book*: "Threat Modeling: Designing for Security" (Adam Shostack)
- *Website*: "An Introduction to Threat Modeling" (Surveillance Self-Defense)
- *Article:* "Security for Journalists, Part Two: Threat Modeling" (Jonathan Stray)
- *Guide:* "Managing Information Security Risk: Organization, Mission, and Information System View" (NIST)
- *Guide:* "Guide for Conducting Risk Assessments" (NIST)
- *Activity:* "Threat Model Activity" (Tow Center)

Threat research by focus area

- Human Rights
  - Freedom House's "Freedom in the World" index is the standard-setting comparative assessment of global political rights and civil liberties.
  - Amnesty International regional news on human rights
  - Human Rights Watch - Browse by Region
- Transparency [77]
  - Corruption Perception Index
- Public Service Delivery
- Health
- Free Media and Information
  - Threatened Voices: Tracking suppression of online free speech.
  - IREX's Media Sustainability Index (MSI) provides in-depth analyses of the conditions for independent media in 80 countries across the world.
  - Freedom House's "Freedom on the Net" index, assessing the degree of internet and digital media freedom

around the world.
    - Freedom House's "Freedom of the Press" index assess' global media freedom.
    - ARTICLE 19 freedom of expression and freedom of information news by region.
    - Open Society Foundation - Mapping digital media
    - Press Freedom Index (RSF)
- Climate Issues
- Gender Issues
- Poverty Alleviation
- Community Building
- Peace promotion
- Agricultural Development
- Entrepreneurship
- Water, Sanitation
- Transportation
- Disaster Relief

Threat research by method

- Country threat reports [78,79]
- Examine Transparency Reports
    - Find most used sites in region. [80]
    - Search for transparency reports for most used sites. [81]

General Threats by Region

- *Database:* "The Aid Worker Security Database (AWSD) records major incidents of violence against aid workers, with incident reports from 1997 through the present." (The Aid Worker Security Database (AWSD))
- *Platform:* "The HumanitarianResponse.info platform is provided to the humanitairan community as a means to aid in coordination of operational information and related activities." (Humanitarian Response)
- *Organization:* "ReliefWeb has been the leading source for reliable and timely humanitarian information on global crises and disasters since 1996." (ReliefWeb)

Legal Threats by Region

- *Monitor:* "CNL's NGO Law Monitor provides up-to-date information on legal issues affecting not-for-profit, non-governmental organizations (NGOs) around the world." (NGO Law Monitor)
- *Survey:* ["This is a survey of existing and proposed laws and regulations on cryptography - systems used for protecting information against unauthorized access."(http://www.cryptolaw.org/)] (The Crypto Law Survey)
- *List:* "Who publishes Transparency Reports? - a list of transparency reports from Google, Facebook, and other popular websites. Cross-check with Alexa for locally popular services" (James Losey)
- *Website:* "This website contains information on regulations, policies, and local organizations working on issues related to digital rights in Latin America. The information is organized by country" (RedLatAm)
- *Article:* "Legal Issues in Penetration Testing" (Security Current)
- *Wiki Page:* ["Anti-circumvention: Laws and Treaties"(https://en.wikipedia.org/wiki/Anti-circumvention)] (Wikipedia)
- *Guide:* "Encryption and International Travel" (Princeton University)
- *Guide:* "World Map of Encryption Laws and Policies" (Global Partners Digital)
- *List:* "National Cyber Security Policy and Legal Documents" (NATO Cooperative Cyber Defence Centre of Excellence)

Technical Threats

- *Database:* "APT Groups and Operations"
- *Database:* "APTNotes"
- *Country Profiles:* "Current cybersecurity landscape based on the five pillars of the Global Cybersecurity Agenda namely Legal Measures, Technical Measures, Organisation Measures, Capacity Building and Cooperation." (Global Cybersecurity Index (GCI))
- *Reports:* Privacy International's in-depth country reports and submissions to the United Nations. (Privacy International)
- *Organization:* "The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, Canada focusing on advanced research and development at the intersection of Information and Communication Technologies (ICTs), human rights, and global security." (The Citizen Lab)
- *Database:* "International Cyber Developments Review (INCYDER)" (NATO Cooperative Cyber Defence Centre of Excellence)
- *Guide:* "This handbook sets out an overview of the key privacy and data protection laws and regulations across 72 different jurisdictions, and offers a primer to businesses as they consider this complex area of compliance." (Data Protection Laws of the World - DLA PIPER)
- *Reports:* "Country Reports" (Open Network Inititiative)
- *Reports:* "Regional Overviews" (Open Network Inititiative)
- *Portal:* "Country Level Information security threats" (The ISC Project)

Targeted Malware

- *Reports:* "APWG Phishing Attack Trends Reports" (Anti-Phishing Working Group)

Censorship and Surveillance Reports

- *Map:* "Cyber-Censorship Map" (Alkasir)
- *Dashboard:* "At-A-Glance Web-Blockage Dashboard" (Herdict)

Travel Threats

- *List:* "Foreign travel advice" (GOV.UK)
- *List:* "Travel Advice" (Australian Government)
- *Alerts:* "Travel Alerts & Warnings" (US Department of State)
- *List:* "List of airlines banned within the EU" (European Commission)
- *List:* "A list of aircraft operators that have that have suffered an accident, serious incident or hijacking." (Aviation Safety Network)
- *Map:* "A global display of Terrorism and Other Suspicious Events" (Global Incident Map)

ACTIVITIES

PRE-MORTUM RISK MODELING

Covered in full in Risk Assessment:

- "Pre-Mortum" Activity
- Identification of critical processes
- Selected critical process mapping
- Threat Identification (Control/Confidentialy/Idenity/Integrity/Authentication/Access)
- Impact Identification
- Adversary Exploration (Likelyhood)
- Impact Ranking

CRITICAL DATA ACTIVITY

Covered in full in Data Assessment:

- With staff input, post up popular places where data is kept (laptops, email, shared drives...)
- Using stickies, gather from the staff what data is kept in what locations - duplicating notes when needed
- Rank data by sensitivity
- Discuss the impact of one of the devices where data is stored being lost - are there backups?
- Discuss the impact of a device being exposed / taken by an adversary
- Identify who has access (physical access, login access, and permissions), and who needs to have access to get the organizations work completed.

THREAT IDENTIFICATION

Summary

These activities build off of a process or data mapping exercise to connect actual processes or assets and data of the organization with potential threats, then drilling down into specific, likely threats the organization faces, adversaries who might take advantage of them, and the impact of this happening.

The goal is to be able to answer the following questions:

Threat History

- What history of attacks does the threat actor have?
- What techniques have they used? Have they targeted vulnerabilities that the organization currently has?
- What is known about the types of threats used by an threat actor to attack similar organizations?

Threat Capability

- Does the threat actor have the means to exploit a vulnerability that the organization currently has?
- Does the threat actor have the means to leverage widespread threats against all similar organizations, or will they have to prioritize their targets?

Threat Intent

- Have they targeted similar organizations?
- Does the threat actor currently have the desire to conduct an attack against this type of organization?
- Is the organization a priority threat target for the threat actor?

Overview

- Identify and categorize threats to processes or data (requires a process or data mapping exercise) by Confidentiality, Control, Integrity, Identity, Availability, and Auditability
- Identify the impact of each threat against People, Organization, and Program
- Brainstorm potential Adversaries and note their History, Intent, and Capability per Threat

- For Threats with identified Adversaries, rank them on a linear scale from "Inconvenient" to "Severe" (no two items can have the same rank)

Materials Needed

- The outputs from a process or data mapping exercise to work from
- Stickies
- Whiteboard or flip-chart (whiteboard preferred)
- Markers
- Camera to digitally capture the data

Considerations

- Treat threat and adversary data with the utmost security.
- Ensure that any physical notes/drawings are erased and destroyed once digitally recorded.
- Ensure that any digital recordings of this process are kept secure and encrypted.
- Consider who has physical and visual access to the room where this process takes place, and if the room can be secured if this activity may span long/overnight breaks.

Walkthrough

- Requires a process or data mapping exercise's outputs

Threat Identification: (30 minutes per process)

- Give participants a "cheat sheet" of threats.
- Explain the types of threats.
  - **Confidentiality**: If unauthorized individuals find out an asset/process exists.
  - **Control**: If an asset/process can be accessed by unauthorized individuals.
  - **Integrity**: If an asset/process is changed without permission.
  - **Availability**: If an asset/process becomes unavailable.
  - **Consistency**: If an asset/process becomes unreliable. (Some use **Identity** instead or in addition to Consistency, if an asset/process can be spoofed to appear as owning/coming from someone else.)
  - **Auditability**: If you cannot verify that an asset/process is secure.
- Identify a "interaction line" from the process map to start with.
- Generate a list of threats that would cause that interaction to fail.
- Mark the back of the post it with the interaction name or number.
- Write the threat and their impact on post-its and arrange them in an orderly way.
- If multiple risks cause the same consequence create a new post-it near the new risk.
- Continue doing this for all the interactions in the critical process'.
- Discuss and rearrange threats as groupings emerge.

- Label threat clusters that appear.

- **NOTES:**
  - If any of the impacts identified in the pre-mortum or other process-mapping exercises are not covered ask participants where they would go.
  - Take photos of the threats once you have finished enumerating them.
  - Write risks on one set of post-its and impacts on another color of post-its to make it easy to keep track.
  - Look at the"CVSS V2 Base Metrics" for an example of the severity of different threats.

Impact Identification: (30 minutes per process) This exercise has the trainee lead the participants on a brainstorming of hypothetical consequences (impacts) when the threats identified earlier occur.

- Give participants a pen and three sticky note pads.
- Explain the topic and the categories. [82]

    - Staff/People - (which includes families, friends, and beneficiaries): temporary or permanent physical injury, temporary or longer-term psychological damage, death, legal costs, cost of medical treatment, loss of morale or trust in management.
    - Organization - loss of or damage to assets, operational inefficiency, loss of program quality or outright suspension; loss of reputation; loss of funding.
    - Program - reduced program quality, temporary suspension of the program, forced termination of the program.
- Instruct each person to generate DIRECT impacts based upon the exiting threat clustering from **Threat Identification.**
- Include only one impact per sticky note.
- Have one participant quickly describe then place an impact on the board writing along side it the threat that causes it.
- Invite others to place similar/the same impacts in proximity and quickly describe how it can occurs.
- Repeat the process until all impacts are included.
- Have participants add stickies for any secondary/cascading impacts
- Discuss and rearrange impacts as groupings emerge.

- Label impact clusters that appear.

- **NOTES:**
    - Tell participants to write multiple impacts per color.
    - Look for opportunities to create sub-groups.
    - Limit the time frame for discussion.
    - Take photos of the impact clusters once you have finished enumerating them.

Adversary Exploration (Likelyhood):

- Explain the topic and the categories. [83]
    - "History – a past incidence or pattern of attacks on similar organizations."
    - "Intent – specific threats, a demonstrated intention or mindset to attack."
    - "Capability – the wherewithal to carry out an attack."
- Brainstorm adversaries who have demonstrated likelihood to impact their work or one of the process'.
- Pick an adversary and write their name on the board.
- Write specific instances of adversary history, intent, and capacity announced by the participants.

- Repeat the process until all adversaries are completed.

- **NOTES:**
    - Limit the time frame for discussion.
    - Take photos of the adversary lists.

Impact Ranking: The goal of this exercise is to have the trainee lead the host organization in classifying the severity of the possible impacts from the threats they have just explored.

- Create a post it for each impact.
- Place two points on the wall. On one side are "Inconvenient" impacts that disrupt the organization in a very small way. On the other side are "critical" impacts that may pose life-safety risks to employees, partners, or the general public.
- The low end of the scale may include a fire alarm may cause the staff to lose a half an hour of work time, but does not impact any short or long-term activities.
- The high end of the scale would include events such as a fire that destroys the organizations headquarters and endangers staffs lives or legal issues that cause termination of the program.
- Place each item along the severity line from least to most severe impact.

- Give each item its own place on the scale. No two items can be the same severity.

- **NOTES:**
    - Listen carefully to every point of deliberation.
    - As risks are placed on the wall, the trainee can use other already ranked risks to help participants identify the right place. "Is a robbery more or less likely than a fire?"
    - Take photos of the impact scale once you have finished it.

Recommendation

CREATING A RISK MATRIX

Summary

Overview

- 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.

Materials Needed

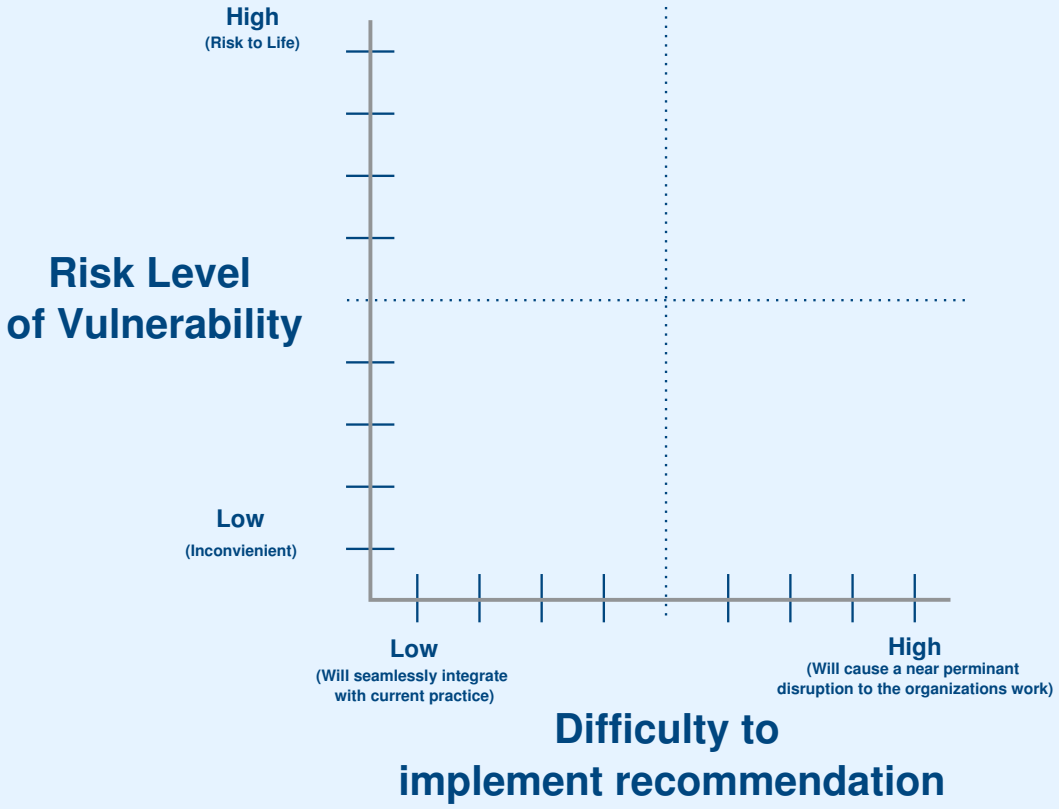
- Stickies
- Markers
- Whiteboard or flip-chart

Considerations

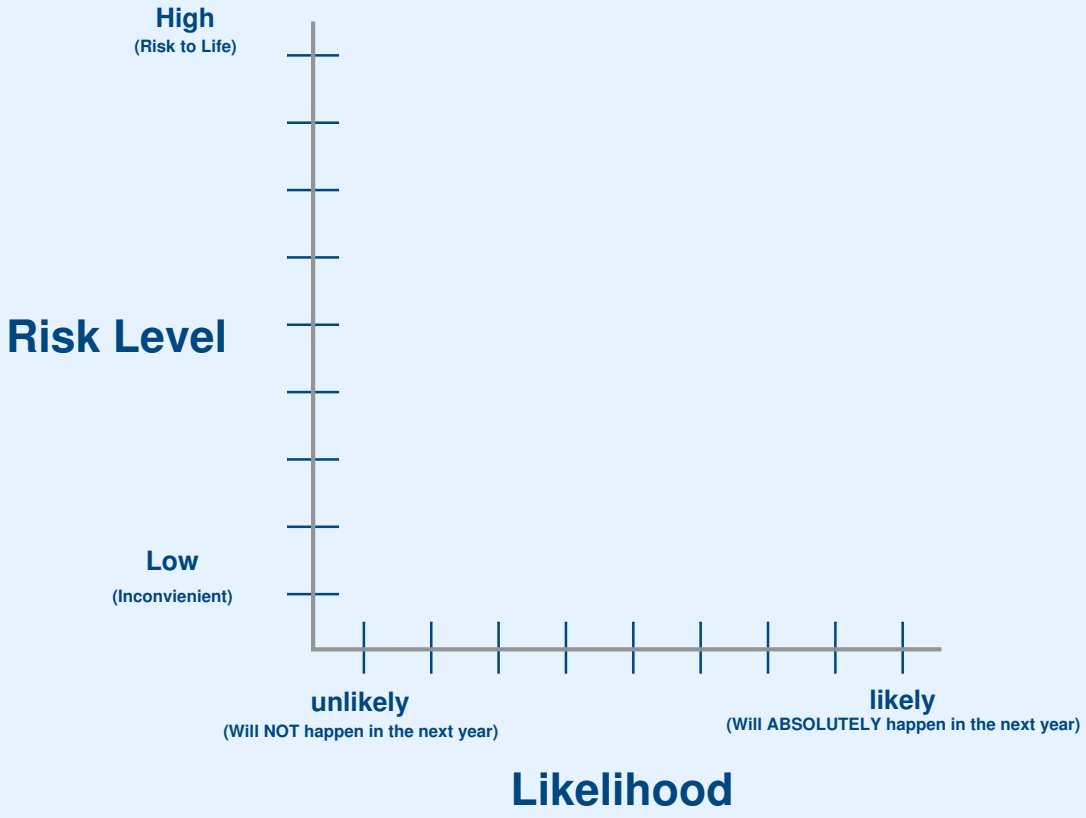
Walkthrough

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

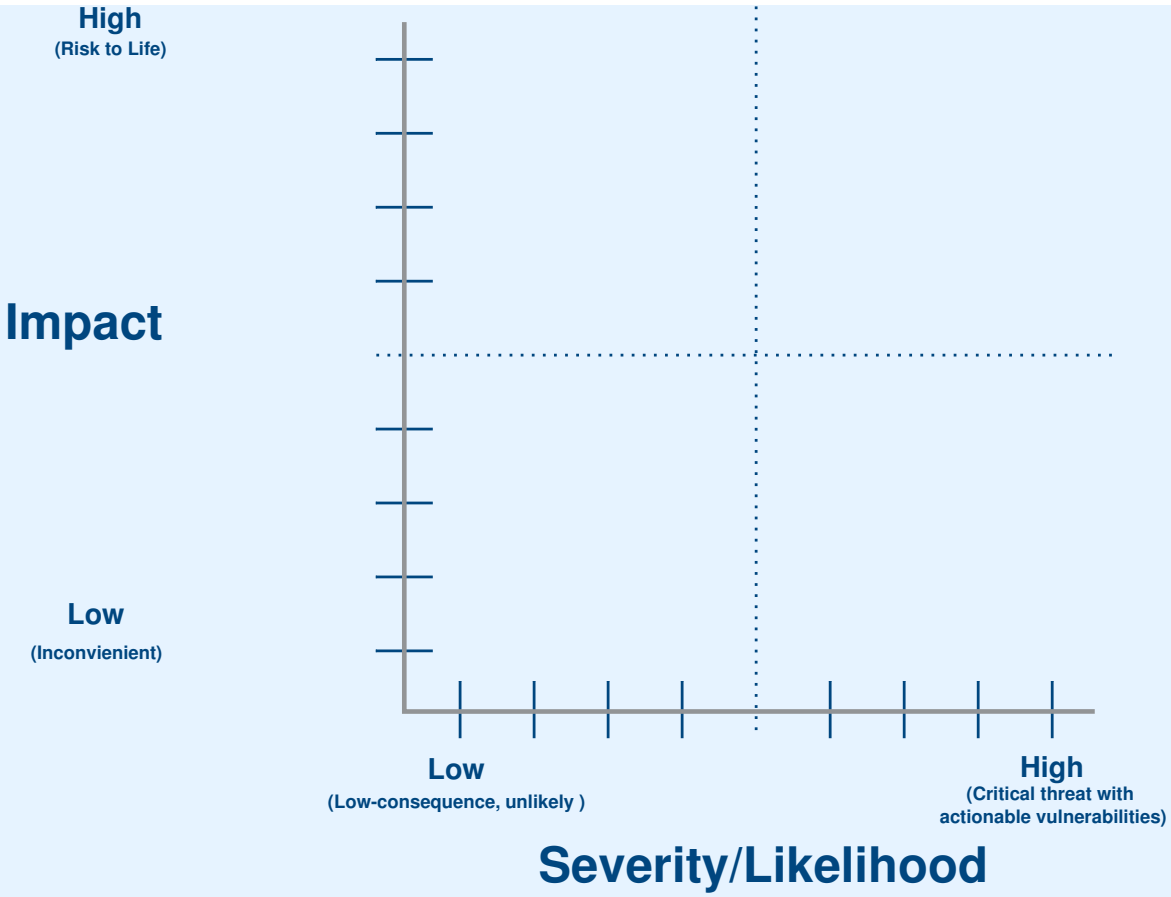
- Create a risk matrix placing *impacts* against a range of likelihood.
- Clean up critical process maps for use in reporting.
- Create a list of all services or assets that were identified during the activity that were not already known by the auditor.



Risk vs Difficulty



Risk vs Likelihood



Impact vs Severity

Recommendation

THREAT INTERACTION

Summary

This helps the auditor enumerate threats that the organization is concerned about and the internal priorities of them. At the same time, it enables a discussion of how threats can interrelate and helps define the difference between a threat and a risk (a threat that has a vulnerability associated with it), and the value of mitigation.

This exercise works well with larger groups, and can be woven in to the Threat Identification activity.

Overview

- Split participants into small groups and have them brainstorm on all possible threats, writing each on a separate stickie
- Cluster the stickies to reveal duplicate concerns across the group and thematic areas
- Mark the threats which have occurred
- Select one threat and arrange other threats, where relevant, as potential causes or outcomes of that threat

Materials Needed

- Stickies (ideally 3 colors)

- Pens/sharpies for participant groups
- Markers
- Camera to digitally capture the data
- Whiteboard or flip-chart

Considerations

- Treat threat and adversary data with the utmost security.
- Ensure that any physical notes/drawings are erased and destroyed once digitally recorded.
- Ensure that any digital recordings of this process are kept secure and encrypted.
- Consider who has physical and visual access to the room where this process takes place, and if the room can be secured if this activity may span long/overnight breaks.

Walkthrough

Also review the Threat Identification exercises below to tailor these to best meet your information gathering needs based on your interactions with the organization.

Threat Brainstorming (15 minutes)

Split participants into small groups. This grouping is particularly valuable for larger organizations, but even for small ones, having multiple separate groups helps reveal shared concerns around the threats the staff face. For a group that is too small to group, have each staff member brainstorm by themselves.

Have each group or staff member quickly write down any possible "threat" they or the organization face. Some examples ("kidnapping," "website hacked") can help seed this activity.

If you have multiple colors of stickies, having them categorize threats by "physical," "digital," or "other/both" will be useful to show their inter-relation.

Keep reminding participants of the time remaining to keep them brainstorming rather than discussing threat details or arguing over whether a threat is physical or digital.

Threat Clustering and Discussion

After the brainstorming (or other exercises to generate or present a list of concerns), gather and cluster the stickies on a wall, revealing duplicate concerns across the groups and thematic areas of concern.

As clusters become clear, ask if any events similar to this threat have already happened to the organization? What was the impact? Has it happened more than once? Regularly? Mark these threats.

Note: Some of these threats may be traumatic experiences, consider skipping public discussion of historical occurrence if many of the threats from the brainstorm (or from one person/group in particular) are particularly intense.

Threat Bow-tie

Select one of the threats that emerged as a concern from the clustering to place at the center of a "bow-tie" like drawing on a whiteboard or flip-chart paper.

Begin asking what other threats identified could come as a result of this threat, supplanting the responses from the participants with additional threats. For example, a hacked website could lead to loss of trust by funders or partners. "Chain reactions" can be illustrated as lines of events (loss of trust by funders could lead to a loss of funding). Do the same for what threats could lead to the "central" threat - a confiscation of a device could lead to email hacking, for example. Some threats can be both potential causes and secondary effects.

Close out this with a discussion of how every threat is potentially connected to both digital and physical impacts.

Threat Analysis Worksheet

The auditor should be able to modify and complete a worksheet like the below at the end of this process. Particularly advanced organizations may be able to fill this out as a survey.

Calculative Impact Identification

Threat type	Impact	Likelihood	Risk
HUMAN THREATS			
1. Accidental destruction, modification, disclosure of confidential information			
2. Ignorance: inadequate security awareness, lack of security guidelines, lack of proper documentation, lack of knowledge			
3. Workload: Too many or too few system administrators, highly pressured users			
4. Users may inadvertently give information on security weaknesses to attackers			
5. Incorrect system configuration			
6. Inadequate security policy			
7. Dishonesty: Fraud, theft, selling of confidential information			
8. Attackers may use telephone to impersonate employees to persuade users/administrators to give user name/passwords, etc			
GENERAL THREATS			
1. Unauthorized use of “logged-in” computers			
2. Installation of unauthorized software or hardware			
3. Denial of service, due to Website traffic, large PING packets, etc.			
4. Malware in programs, documents, e-mail attachments, etc			
IDENTIFICATION AUTHORIZATION THREATS			
1. Attack software masquerading as normal programs (Trojan horses)			
2. Attack hardware masquerading as normal commercial hardware			
3. External attackers masquerading as valid users			
4. Internal attackers masquerading as valid users			
PRIVACY THREATS			
1. Telephone eavesdropping (via telephone bugs, inductive sensors, or service providers			
2. Electromagnetic eavesdropping			
3. Rubbish eavesdropping (analyzing waste for confidential documents, etc.)			
4. Planted bugs in the building			
INTEGRITY/ACCURACY THREATS			
1. Deliberate damage of information by external source			
2. Deliberate damage of information by internal sources			
3. Deliberate modification of information			

Threat type	Impact	Likelihood	Risk
ACCESS CONTROL THREATS			
1. Password cracking (access to password files, use of default/weak passwords, etc)			
2. External access to password files, and sniffing of the networks			
3. Unsecured maintenance of online services, developer backdoors			
4. Bugs in network software which can open unknown/unexpected security holes (holes can be exploited from externally to gain access)			
5. Unauthorized physical access to system			
LEGAL THREATS			
1. Failure to comply with legal requirements			
2. Liability for acts of internal users or attackers who abuse the system to perpetrate unlawful acts (ie, incitement to racism, gambling, money laundering, distribution of pornographic or violent material)			
3. Liability for damages if an internal user attacks other sites			
RELIABILITY OF SERVICE THREATS			
1. Major natural disasters, fire, water, earthquake, floods, power outages, etc			
2. Minor natural disasters, of short duration, or causing little damage			
3. Equipment failure from defective hardware, cabling, or communications system.			
4 Denial of Service due to network abuse: Misuse of routing protocols to confuse and mislead systems			
5. Downloading of malicious Applets, Active X controls, macros, PostScript files, etc through the browsers			
6. Sabotage: Physical destruction of network interface devices, cables			

Risk = Impact * Likelihood

SCALE

Impact Scale	Likelihood
Impact is negligible =1	Unlikely to occur =0
Effect is minor, major organization operations are not affected=2	Likely to occur less than once per year =1
Organization operations are unavailable for a certain amount of time, costs are incurred. Public/customer confidence is minimally affected =3	Likely to occur once per year =2
Significant loss of operations, significant impact on public/customer confidence =4	likely to occur once per month =3
Effect is disastrous, systems are down for an extended period of time, rebuilding and replacement of systems is required =5	Likely to occur once per week =4
Effect is catastrophic, critical systems are completely down for an extended period; data is lost or irreparably corrupted; public and customers are totally affected =6	Likely to occur daily =5

Recommendation

REGIONAL CONTEXT RESEARCH

Covered in full in Capacity Assessment:

- Identify any legal risks associated with conducting the audit (Secure communications and storage, network forensics, device exploitation, digital security training.) [84]
- Determine the sensitivity of the type of work the organization conducts and if its work attracts additional potential threat actors.
- Identify potential adversaries not identified in interviews including domestic or international governments and other, non-state actors (organized crime, corporations, competition, etc).
- Identify capacity and willingness of potential adversaries to act against the organization.
- Has any organization or individual made specific threats, or demonstrated intention or mindset to attack on the organization or similar organizations?

RESPONSIVE SUPPORT

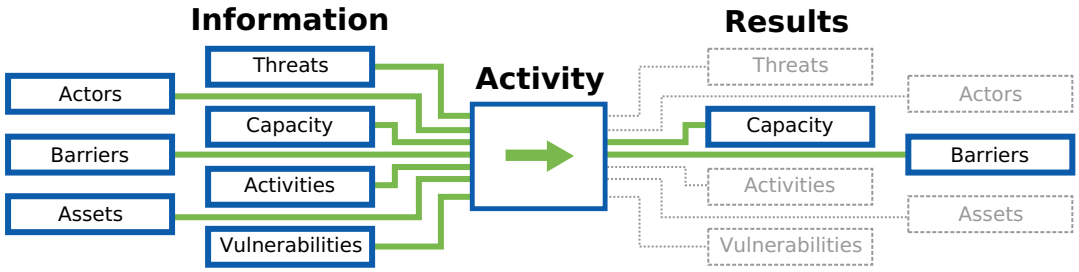
SUMMARY

The auditor provides assistance for any immediate action needed (spot training, tool fixes, consulting on upcoming projects) -- this may also involve addressing vulnerabilities that triggered an incident response.

PURPOSE

In-audit activities and training are used to increase an organization's agency to seek out and address immediate security challenges within their organization, as well as enabling the organization to securely receive and store the audit report.

THE FLOW OF INFORMATION



Responsive Support Information Flow

GUIDING QUESTIONS

- Are there any critical vulnerabilities or remediation activities that the organization needs a deeper understanding to give proper weight to in the report?
- How can you prepare the staff and management for aspects of the audit process might lead to alienation or inhibit the process?
- What is the organization's readiness and likelihood to succeed in engaging with security technology? What factors will complicate or inhibit the effective and safe uptake and use?
- Is the support you want to provide (troubleshooting, fixes, upgrades, training, etc.) critical to the security of the organization? If not, can you provide that support without taking away from the audit?
- Will you have the capacity to support software or hardware that you provided while providing support?

APPROACHES

- **Targeted Training:** Educational components can be introduced in order to cover the digital security basics, satisfy the team's expectations and motivate the target group to include digital security practices in their everyday lives.
- **Targeted Support:** The auditor can provide small targeted technical/policy development support where there expertise overlaps and the audit time-line allows.

OUTPUTS

- Organizational capacity to communicate and store data securely
- Enhanced organizational capacity
- Mitigation of critical risks.

OPERATIONAL SECURITY

- If you are providing software tools, make sure to check file signatures (and explain the process) - do not be the weak link or introduce malware into the organization!
- Do not attempt to train on any topic that you are not knowledgeable on.
- For any targeted training, especially on new tools, ensure that key personnel at the organization successfully use these tools during the audit timeline. This is especially important for secure communications tools the auditor hopes to

use to follow-up with the organization.
- For any specific fixes or upgrades to the system, make sure that backups exist and to test extensively and with staff involvement after your intervention.

PREPARATION

Baseline Skills

- Experience giving digital security training
- Each training guide has detailed lists of materials needed and trainer preparation - preview and prepare for any training you plan to give.

RESOURCES

Facilitation Preparation

- *Tip Sheet:* Facilitator Preparation Tips (Integrated Security)
- *Guidelines:* "Facilitator Guidelines" (Aspiration Tech)
- *Guide:* "Session_Design" (Aspiration Tech)
- *Kit:* "Resource Kit" (eQualit.ie)
- *Questions:* "Pre-Event_Questions" (Aspiration Tech)
- *Guide:* "Break Outs" (Aspiration Tech)
- *Resources:* "Be a Better Trainer" (Level-up)

Digital Security Trainings

- *Curricula:* Level-Up: Resources for the global digital safety training community.
- *Curricula:* eQualit.ie's Trainer's Curricula (also in Russian)
- *Training Manual:* Workbook on Security: Practical Steps for Human Rights Defenders at Risk
- *Trainer Handbook:* "SaferJourno" (Internews)

Digital Security Guides

- *Multi-lingual Guides:* Security in a Box
- *Resource:* Front Line Defenders
- *Guide:* "Surveillance Self-Defense" (EFF)
- *Guide:* "The Digital First Aid Kit" (Digital Defenders Partnership)
- *Guides:* "Protektor Services Manuals" (Protektor Services)
- *Guide:* "Cryptoparty Handbook" (CryptoParty)
- *Guide:* "Bypassing Internet Censorship" (Floss Manuals)

Training Resources

- *Directory:* "Security Training Firms" (CPJ)

ACTIVITIES

Due to the wide variety of needs found during SAFETAG audits, the framework relies on the wealth of existing training curricula and digital security guides, listed below.

Of specific use are the following training guides from Level-Up. Review the Level-Up Curricula Guide prior to using these activities:

- Malware Fundamentals and Social Engineering
- Secure Passwords
- Advanced Email Security

DEBRIEF

SUMMARY

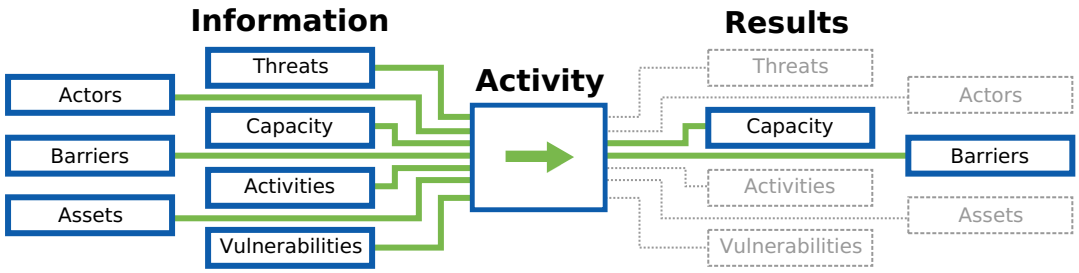
This component consists of an out-brief to key points of contact, providing basic pressure relief through group and individual interactions, and planning future follow-up with the host and key individuals.

PURPOSE

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 organization's agency to seek out and address security challenges independently. This can be an auditor's last in-person chance to engage with the staff to shape their perspective of the audit.

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, and in combination with training or security consultation in the Responsive Support section, the auditor can ensure that the host sees the audit as a guide instead of a condemnation.

THE FLOW OF INFORMATION



Debrief Information Flow

GUIDING QUESTIONS

- Is the organization empowered to make changes?
- Do key personnel have a general understanding of the initial findings?
- Does the organization understand the next steps of the audit process?

APPROACHES

- Discuss next steps and points of contact going forward for the host.
- Provide psycho-social care and re-framing as needed.
- Initiate follow-up with host (organizational and individual).

OUTPUTS

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

OPERATIONAL SECURITY

PREPARATION

RESOURCES

- *Resource:* The Psychological Underpinnings of Security Training (Craig Higson-Smith)

- *Article:* "No money, no problem: Building a security awareness program on a shoestring budget"

Facilitation Preparation

- *Tip Sheet:* Facilitator Preparation Tips (Integrated Security)
- *Guidelines:* "Facilitator Guidelines" (Aspiration Tech)
- *Guide:* "Session_Design" (Aspiration Tech)
- *Kit:* "Resource Kit" (eQualit.ie)
- *Questions:* "Pre-Event_Questions" (Aspiration Tech)
- *Guide:* "Break Outs" (Aspiration Tech)
- *Resources:* "Be a Better Trainer" (Level-up)

ACTIVITIES

FOLLOW UP

SUMMARY

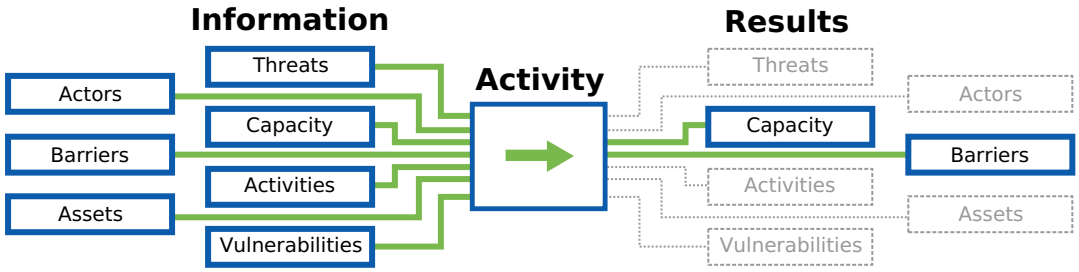
This component allows an auditor to explain and get feedback on their report as well as evaluate the success of the process over time through a continued relationship with the host.

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.

THE FLOW OF INFORMATION



Information Flow

GUIDING QUESTIONS

- What are the barriers the organization faced in implementing the recommended risk mitigation plan?
- Are there new resources that the auditor can provide to supplement the original audit?
- What can you do to make your follow up perceived as additional support instead of as an evaluation of their success?

APPROACHES

- **Staff Feedback Survey:** Receive feedback from the staff on the execution of the audit.
- **Report Follow Up Meeting:** Have a follow-up call to discuss report.
- **Making Introductions:** Introduce organization to known resources as needed.
- **Long-Term Follow Up:** Contact host after a few months to check on progress, get long-term feedback and connect with any new resources.

OUTPUTS

OPERATIONAL SECURITY

- In addition to ongoing secure communication practices, check for any changes in keys or other authentication changes. If these occur re-verify this information using out of band means.

PREPARATION

RESOURCES

- *Directory:* "Selected International and Regional Organisations providing support to HRD" (Workbook on Security: Practical Steps for Human Rights Defenders at Risk)
- *Directory:* "Security Training Firms" (CPJ)
- *Digital Emergency Contacts:* "Seeking Remote Help" (The Digital First Aid Kit)
- *Directory:* "Resource Handbook" (Center for Investigative Journalism)
- *Guide:* "Additional Resources: p. 298" (Operational Security Management in Violent Environments (Revised Edition))

Resource Lists

- *Directory:* "Resource Handbook" (Center for Investigative Journalism)
- *Directory:* "Selected International and Regional Organisations providing support to HRD" (Workbook on Security: Practical Steps for Human Rights Defenders at Risk)
- *Guide:* "Additional Resources: p. 298" (Operational Security Management in Violent Environments (Revised Edition))
- *Database:* "A Collaborative Knowledge Base for Netizens" (Tasharuk)
- *Guidelines:* "Microsoft nonprofit discount eligibility guidelines per country" (Microsoft)
- *Organization:* "TechSoup, nonprofits and libraries can access donated and discounted products and services from partners like Microsoft, Adobe, Cisco, Intuit, and Symantec." (TechSoup)

Possible Financial Resources for Host Organizations

International organisations that may provide security grants

Frontline Defenders Security Grants Programme _See also the "Alternative Sources of Funding" list on this page

Digital Defenders Digital Security Emergency and Support Grants

Freedom House Emergency Assistance Programs

Digital Security Trainings

- *Curricula:* Level-Up: Resources for the global digital safety training community.
- *Curricula:* eQualit.ie's Trainer's Curricula (also in Russian)
- *Training Manual:* Workbook on Security: Practical Steps for Human Rights Defenders at Risk
- *Trainer Handbook:* "SaferJourno" (Internews)

Emergency Resources

Emergency Aid for Journalists

International protection mechanisms for human rights defenders

What Protection Can The United Nations Field Presences Provide?

24/7 Digital Security Helpline: help@accessnow.org PGP key fingerprint: 6CE6 221C 98EC F399 A04C 41B8 C46B ED33 32E8 A2BC

Rapid Response Network: cert@lists.civicert.org PGP key: 7218 4AA7 4ED2 05ED 9863 A2A7 1F84 9150 6BFC 20AC

Organizations providing rapid-response digital security support and funding

ACTIVITIES

FOLLOW-UP MEETING

Summary

Schedule and have a follow up call to discuss the audit report. This provides a valuable touch-point for the organization to read the report and ask any clarifying questions to the auditor, as well as for the auditor to underscore any important steps for the organization.

Overview

- Walk through the report and discuss the priority findings
- Schedule a long-term check-in call

Materials Needed

- A copy of the report
- A secure note-taking system.

Considerations

- A secure, real-time VOIP system is recommended for this call, as many of the highly sensitive audit findings are likely to be discussed in detail. Skype may suffice in some regions, but also consider secure call options (https://ostel.co/).

Walkthrough

Each organization, and often even each key point of contact within the organization, will want to explore the report in different ways. Adapt to the needs of the organization, but make sure you cover the top-priority recommendations that the organization needs to consider in the immediate future.

Ask the organization to fill out Staff Feedback Surveys.

Ask if they need any specific resources or introductions not included in the report.

At the end of the call, schedule a second follow-up call to check in on their progress.

Recommendation

MAKING INTRODUCTIONS

Summary

Make introduction between host and known resources as needed.

Overview

- Introduce relevant organizational representatives to resources
- Follow up with both the organization and the resource later to check on progress

Materials Needed

Considerations

- Consider the implications of the meta-data (email addresses, subject lines, dates) involved in these introductions.
- Provide PGP keys (signed if possible) for introductions where possible

Walkthrough

Based on the specific recommendations in the audit report, as well as the auditor's understanding of the organization's capacity and barriers faced, introduce the relevant points of contact at the organization to resources such as digital security trainers, funding organizations which provide targeted support for digital security, technical experts to help on specific tasks (e.g. server hardening, website migration), as well as services that could help address their needs (e.g. secure hosting providers, rapid response support).

Follow up with both the organization and the resources introduced to check in on process and revise which introductions you make going forward.

Recommendation

LONG-TERM FOLLOW-UP

Summary

Follow up with host after a few months to check on progress, get long-term feedback and connect with any new resources.

Overview

Materials Needed

- A copy of the report
- A secure note-taking system.

Considerations

- A secure, real-time VOIP system is recommended for this call, as many of the highly sensitive audit findings are likely to be discussed in detail. Skype may suffice in some regions, but also consider secure call options (https://ostel.co/).

Walkthrough

This can be combined with the Staff Feedback Survey exercise, or to follow up on any concerns you have based on their responses to that survey. The main goal of the long-term follow-up is to ensure that the organization has ongoing connection points to any resources or connections they need to remove barriers to adoption.

Recommendation

STAFF FEEDBACK SURVEY

Summary

Providing a space for anonymous, guided feedback is valuable to gather information about how your audit work and the SAFETAG framework itself are supporting organizational understanding of risk and their ability to adapt. This long-term capacity building is critical to the SAFETAG framework, so finding ways to measure the impact of an audit towards these goals is important.

Overview

- After providing a report to the organization, send them a survey (that they can complete anonymously) to gauge change in perceptions of risk, your efficacy as an auditor, and willingness to change/adapt
- Compile results

Materials Needed

- Survey questions
- Platform or document for securely recording survey responses

Considerations

- Provide this survey in a method that respects the client's need for privacy, security, and anonymity.

Walkthrough

This exercise provides a simple survey you can implement in a variety of settings (Google Forms, SurveyMonkey, via plain documents, etc.).

SAMPLE SURVEY QUESTIONS

1. **Before the audit:**

	Completely False	False	I don't know	True	Completely True
I understood the risks my organization faces	[ ]	[ ]	[ ]	[ ]	[ ]
I understood the risks that I personally face.	[ ]	[ ]	[ ]	[ ]	[ ]
I understood the risks that my organization's beneficiaries face.	[ ]	[ ]	[ ]	[ ]	[ ]
The auditor understood the risks my organization faces.	[ ]	[ ]	[ ]	[ ]	[ ]
The auditor understood the risks that I personally face.	[ ]	[ ]	[ ]	[ ]	[ ]

The auditor understood the risks that my organization's beneficiaries face.	Completely False	[ ] False	[ ] I don't know	[ ] True	Completely True

2. **After the audit:**

	Completely False	False	I don't know	True	Completely True
I understood the risks my organization faces	[ ]	[ ]	[ ]	[ ]	[ ]
I understood the risks that I personally face.	[ ]	[ ]	[ ]	[ ]	[ ]
I understood the risks that my organization's beneficiaries face.	[ ]	[ ]	[ ]	[ ]	[ ]
The auditor understood the risks my organization faces.	[ ]	[ ]	[ ]	[ ]	[ ]
The auditor understood the risks that I personally face.	[ ]	[ ]	[ ]	[ ]	[ ]
The auditor understood the risks that my organization's beneficiaries face.	[ ]	[ ]	[ ]	[ ]	[ ]

3. **Do you feel the audit took a reasonable amount of time?**

- [ ] I would have been willing to spend more time in the audit.
- [ ] We did not spend enough time on the audit.
- [ ] The audit took more time than it should have.
- [ ] The audit took the right amount of time.
- [ ] I don't know.

4. **Do you have any immediate behavioral changes you intend to make because of the audit?**

- [ ] Yes
- [ ] No

5. **Did the auditor provide you everything you need to start addressing your digital security?**

- [ ] Yes
- [ ] No
- [ ] I don't know.

6. **Did any training that you received specifically address the risks identified during the audit?**

- [ ] Yes
- [ ] No
- [ ] I don't know.

7. **Did the recommendations made by the auditor directly address the digital security needs you identified during the audit?**

- [ ] Yes
- [ ] No
- [ ] I don't know

8. **Did the recommendations made by the auditor address the digital security needs of your organization?**

- [ ] Yes
- [ ] No
- [ ] I don't know

9. **The recommendations from the audit...**

- [ ] Were implemented before we received the report.
- [ ] Will be easy to implement.
- [ ] Will be only slightly difficult to implement.
- [ ] Will hard to implement.
- [ ] Will be impossible to implement.

10. **The biggest barrier you see to implementing the auditor's recommendations is....**

- [ ] Lack of money
- [ ] Lack of time
- [ ] Lack of interest
- [ ] Lack of technical expertise
- [ ] They are too difficult to implement

Recommendation

Reporting

RECOMMENDATION DEVELOPMENT AND RESOURCE IDENTIFICATION

SUMMARY

In this component the auditor identifies the organization's strengths and weakness (expertise, finance, willingness to learn, staff time, etc.) to adopting new digital and physical security practices and documents the possible actions the organization could take on to address the vulnerabilities found during the audit, the difficulty of taking on those actions, and the resources that the host may be able to leverage to address them. Resources can include, but are 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

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. 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. In doing this the 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.

GUIDING QUESTIONS

- What are the organizational areas of strength (expertise, finance, willingness to learn, staff time, etc.) that the organization can leverage when engaging in technological adoption/change?
- What are the organizational areas of weakness (expertise, finance, willingness to learn, staff time, etc.) that need to be taken into consideration when engaging in technological adoption/change?
- What are the organizational barriers to adoption?
- Are the recommendations you are providing directly related to the security audit? If not, do they support the organization in accomplishing their security tasks, or distract from them?

APPROACHES

- **Identify and Explain Un-Addressed Concerns :** Write explanations for why any adversaries or threats that the auditor identifies as "un-addressable" with the organizations current capacity.
- **Identify Recommendations:** Identify possible actions to address each vulnerability.
- **Identify Useful Resources:** Identify resources that the organization can leverage to accomplish the identified recommendations.

IDENTIFY USEFUL RESOURCES

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/resources they can use to support their up-skilling.

Overview

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

Materials Needed

Considerations

- Use VPNs or Tor to search if conducting the search from a country that is highly competitive with the organization's country, or is known to surveil.
- Do not share any organization information or data when reaching out to possible resources.

Walkthrough

- 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.

Recommendation

IDENTIFY AND EXPLAIN UN-ADDRESSED CONCERNS

Summary

Write explanations for why any adversaries or threats that the auditor identifies as "un-addressable" with the organizations current capacity.

Base Line Skills

Operational Security

Materials Needed

Materials Needed

Considerations

Output

Resources

IDENTIFY RECOMMENDATIONS

Summary

Overview

Materials Needed

Considerations

Walkthrough

Recommendation

OUTPUTS

- 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.
- 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.

OPERATIONAL SECURITY

- Treat the data and analyses of this step with the utmost security.
- Use VPNs or Tor to search if conducting the search from a country that is highly competitive with the organization's country, or is known to surveil.
- Do not share any organization information or data when reaching out to possible resources.

RESOURCES

Resource Links

- *Directory:* "Selected International and Regional Organisations providing support to HRD" (Workbook on Security: Practical Steps for Human Rights Defenders at Risk)
- *Directory:* "Security Training Firms" (CPJ)
- *Digital Emergency Contacts:* "Seeking Remote Help" (The Digital First Aid Kit)
- *Directory:* "Resource Handbook" (Center for Investigative Journalism)
- *Guide:* "Additional Resources: p. 298" (Operational Security Management in Violent Environments (Revised Edition))

Digital Security Guides

- *Multi-lingual Guides:* Security in a Box

- *Resource:* Front Line Defenders
- *Guide:* "Surveillance Self-Defense" (EFF)
- *Guide:* "The Digital First Aid Kit" (Digital Defenders Partnership)
- *Guides:* "Protektor Services Manuals" (Protektor Services)
- *Guide:* "Cryptoparty Handbook" (CryptoParty)
- *Guide:* "Bypassing Internet Censorship" (Floss Manuals)

Digital Security Guides

- *Database:* "Safety and confidentiality for technology use by agencies serving victims." (NNEDV's Safety Net Project)
- *Database:* "Technology Safety, Organizational Technology Capacity & Development" (NNEDV's Safety Net Project)
- *Guide:* "Secure Hosting Guide" (equalit.ie)
- *Guide:* "Paper (DRAFT) on Best Current Practices regarding the configuration of cyptographic tools and online communication." (Better Crypto)

Possible Financial Resources for Host Organizations

International organisations that may provide security grants

Frontline Defenders Security Grants Programme _See also the "Alternative Sources of Funding" list on this page

Digital Defenders Digital Security Emergency and Support Grants

Freedom House Emergency Assistance Programs

Training Resources

- *Directory:* "Security Training Firms" (CPJ)

Emergency Resources

Emergency Aid for Journalists

International protection mechanisms for human rights defenders

What Protection Can The United Nations Field Presences Provide?

24/7 Digital Security Helpline: help@accessnow.org PGP key fingerprint: 6CE6 221C 98EC F399 A04C 41B8 C46B ED33 32E8 A2BC

Rapid Response Network: cert@lists.civicert.org PGP key: 7218 4AA7 4ED2 05ED 9863 A2A7 1F84 9150 6BFC 20AC

Organizations providing rapid-response digital security support and funding

Resource Lists

- *Directory:* "Resource Handbook" (Center for Investigative Journalism)
- *Directory:* "Selected International and Regional Organisations providing support to HRD" (Workbook on Security: Practical Steps for Human Rights Defenders at Risk)
- *Guide:* "Additional Resources: p. 298" (Operational Security Management in Violent Environments (Revised Edition))

- *Database:* "A Collaborative Knowledge Base for Netizens" (Tasharuk)
- *Guidelines:* "Microsoft nonprofit discount eligibility guidelines per country" (Microsoft)
- *Organization:* "TechSoup, nonprofits and libraries can access donated and discounted products and services from partners like Microsoft, Adobe, Cisco, Intuit, and Symantec." (TechSoup)

Recommendation Development

- *Guide:* "Mitigation Recommendation" (NIST SP 800-115)
- *Overview:* "How Is Risk Managed?" (An Introduction to Information System Risk Management)
- *Book:* "Digging Deeper into Mitigations - p. 130" (Threat Modeling - Adam Shostack) [85]

ACTIVITIES

IDENTIFY USEFUL RESOURCES

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/resources they can use to support their up-skilling.

Overview

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

Materials Needed

Considerations

- Use VPNs or Tor to search if conducting the search from a country that is highly competitive with the organization's country, or is known to surveil.
- Do not share any organization information or data when reaching out to possible resources.

Walkthrough

- 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.

Recommendation

IDENTIFY AND EXPLAIN UN-ADDRESSED CONCERNS

Summary

Write explanations for why any adversaries or threats that the auditor identifies as "un-addressable" with the organizations current capacity.

Base Line Skills

Operational Security

Materials Needed

Materials Needed

Considerations

Output

Resources

IDENTIFY RECOMMENDATIONS

Summary

Overview

Materials Needed

Considerations

Walkthrough

Recommendation

ROADMAP DEVELOPMENT

"*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 [86]

SUMMARY

This component consists of an auditor sorting their recommendations in relation to the organizations threats and capacity. The auditor prioritizes vulnerabilities, weighs the implementation costs of recommendations and then creates an actionable roadmap for the organization to make their own informed choices about possible next steps as they move forward.

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. 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. 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. The existing in/formal security practices captured during this process will be used to remove organizational and psyco-social barriers to starting new practices.

BASELINE SKILLS

PREPARATION

MATERIALS NEEDED

APPROACH

OUTPUTS

- A risk matrix with all vulnerabilities ranked on it.
- An "implementation matrix" showing each recommendation in relation to its difficulty to implement and its urgency.
- 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 vulnerabilities.
- A listing of the process, impact, and likelihood for each vulnerability.
- 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.

OPERATIONAL SECURITY

- Treat the data and analyses of this step with the utmost security.
- The roadmap may be shared with local IT support, digital security trainers, possible funders, or other consultants in part, or in full. Consider the content in light of this.
    - Individual vulnerabilities should be able to be read, and acted upon, independently from the rest of the report so that the organization can easily provide only the required information for follow up work.
    - The overall posture and risk/ranking profile components should be able to be read independent from the risk model and be free of any specific vulnerabilities to allow the organization to easily provide trusted invested parties with an overview of the results/need without exposing any specific vulnerabilities.
- Use VPNs or Tor to search if conducting the search from a country that is highly competitive with the organization’s country, or is known to surveil.

RESOURCES

- *Guide:* "Risk Thresholds in Humanitarian Assistance" (eisf)
- *Guide:* "Guide to Security Management Planning" (eisf)
- *Guide:* "Developing a Security-Awareness Culture - Improving Security Decision Making" (SANS InfoSec Reading Room)
- *Book:* "The Order of Mitigation - p. 131" (Threat Modeling - Adam Shostack) [87]

Determining the urgency of a vulnerability

ACTIVITIES

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* [88]

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.

BASELINE SKILLS

PREPARATION

MATERIALS NEEDED

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. [89]

OUTPUTS

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

OPERATIONAL SECURITY

- Treat the report with the utmost security. It should only be shared as a complete work between the auditor(s) and the identified leadership and points of contact of the organization.

RESOURCES

- *Guide:* "Reporting" (The Penetration Testing Execution Standard)

- *Guide:* "The Art of Writing Penetration Test Reports" (INFOSEC Institute)
- *Guide:* "Writing a Penetration Testing Report" (SANS)
- *Guide:* "Wow your client with a winning penetration testing report" (Tech Target)

ACTIVITIES

APPENDICES

APPENDIX: CODE OF CONDUCT AND SAFETAG GOVERNANCE

MISSION STATEMENT:

The mission of the SAFETAG community is to improve the security of civil society organizations around the world.

What we do: The community collaborates actively to share knowledge, build capacity, and create resources, while promoting transparency and accountability amongst its members, as well as with other communities of practice.

COMMUNITY STANDARDS

The SAFETAG Community of Practice (SCoP) will a be a closed and private group, initially housed within the existing orgsec.community listserv.

- Community members are encouraged to be active - positively contributing / leading discussions on community channels, creating, curating, or peer-reviewing content or contributing to the issue queue. There will be an annual "introduction" thread on the listserv where all SCoP members are expected to respond with a short note on current (shareable) activities.
- Some SCoP members may have privacy concerns, and should join the community using a pseudonym they are comfortable with engaging online in both public and private spaces with.
- Joining the community: While housed within the orgsec.community, the SCoP will follow the joining process on that list.
- The SCoP is responsible for adhering to the SAFETAG Code of Conduct, below

SAFETAG Code of Conduct

Members of the SAFETAG community are expected to:

- Respect the auditees, their contexts (including the legal framework they operate within), and protect their privacy and security
- Protect the identifying information and audit findings of your auditees, unless you have full, informed consent of the auditee -- and even then, exercise extreme care.
- Never use your knowledge, skills and/or access to do harm against organizations or communities you are working with or your peer auditors through malice or neglect
- Minimize any conflict of interests through transparency in your contracting, reporting, and recommendations; e.g. if you were not hired initially to implement recommendations, suggest options other than yourself for implementation, and provide reporting that would enable that to be a success in every case.
- Perform your job responsibly and well. Ask and consult with fellow members of the community.
- Respect other members of the community as peers and promote a safe, inclusive, and harassment-free environment

Community Manager

There will be, given that funds are available, a paid **community manager** who has at least a quarter of their time to support the SAFETAG community and contribute to and support the broader community around NGO organizational security. This community manager should rotate among organizations implementing substantial organizational security work. There may be gaps and/or overlaps due to project and staff funding requirements; it is important for implementing organizations to coordinate funding this position in order to minimize this.

The CM's role is to cultivate, support, and grow the community. This includes, but is not limited to:

- Proposing, planning, and facilitating discussions to support a vibrant and active community
- To a reasonable degree and avoiding conflicts of interest, supporting and coordinating fundraising work across the community
- Providing transparency to the work being done across the implementing community, including the sharing of any requests for audits.
- Shepherding and supporting the creation of new content (managing peer review, managing pull requests, providing

guidance and direct support on merging content into the SAFETAG architecture)
- Supporting the ongoing development of the SAFETAG mission, vision, code of conduct, licensing, and related "meta" content.
- Managing the technical infrastructure (website, content repository)
- Providing at least quarterly reports to the community summarizing activity such as new content, supporting tools or interfaces, new opportunities, and new members
- Scheduling and joining Advisory Board meetings to participate as well as take notes as relevant.
- Documenting the activities, duties, and challenges for future community managers.

THE ADVISORY BOARD

Structure

- An **Advisory Board** of no more than 10 and no fewer than 3 persons shall be made of individuals and institutional representatives, nominated by the board.
- Board members are to serve 18 month terms; 2 consecutive term limit. Institutions are not term limited, but are encouraged to change their representation to the Board when representatives have served two consecutive terms, and are expected to step down if they are unable to continue contributions defined below.
- There can be up to four institutional members of the board, representing organisations that have a vested interest in SAFETAG, due to using it extensively in their own programs. Institutions should designate a representative with a relevant program role and experience with organizational security. Institutional members of the Board are expected to significantly contribute, through funding the community manager, significant content contributions, infrastructure or activities.
- Board members, including institutions, will be appointed and dismissed by simple majority of votes cast by board members with a voting window of two weeks.
- Board meetings over calls or in person ought to be minuted, the board chair is responsible for identifying a note taker.
- Board members who do not participate in voting processes and fail to join 2 consecutive board calls without excusing themselves in advance to the board are automatically removed from the board and trigger the voting in of a new member

Responsibilities

- The Board is responsible for the stewardship of the SAFETAG framework and supporting and advising the CM.
- The Board is responsible for ensuring that the responsibilities of a CM are performed, whether completely by the CM, by a combination of CM and Board members, or by Board members during gaps in the CM role, as well as measuring the performance of the CM
- The Board will be responsible for proposing changes to these governance rules, through simple majority voting
- All members of the Board will provide an ombudsman service to sensitively manage ethics concerns regarding the community manager, fellow board members, and usage of the SAFETAG framework and trademark more broadly

CONTACT

For SAFETAG content related questions, please file an issue: https://github.com/SAFETAG/SAFETAG/issues You can email the SAFETAG Advisory Board at AdvisoryBoard at safetag.org

APPENDIX: HOW TO READ SAFETAG

MAJOR SECTIONS

The Life Cycle of an Audit

This section contains explanations of the goals of the SAFETAG process and definitions of the major terminology.

Objectives

This section contains the objectives of a SAFETAG audit. These are collections of specific **activities** that an auditor may use to gather and confirm information about the risks an organization faces, their capacity to address them, and potential threat actors.

Reporting

This section contains the post-audit objectives used to document the organizations risks and auditors recommendations based upon a final capacity and risk assessment.

OBJECTIVE COMPONENTS

Summary

A short - one to four sentence - basic overview of the objective.

Purpose

The justification for why we have included this objective.

The Flow of Information

The purpose of audit activities is to acquire risk assessment and mitigation information. As this information is acquired, earlier audit steps will have to be re-visited based upon updated information. The "Flow of Information" shows the types of information that an audit objective builds upon (input), and the types of information that it may reveal (outcomes).

Guiding Questions

Each audit objective is guided by a small set of core questions. Key questions are included to help an auditor identify when they have acquired enough information and customize their approach while still collecting the correct types of information to support the organization.

Approaches

Many of these objectives can be completed in multiple ways depending upon auditor skill and the organizational technical setup and capacity. The approach section includes a list of activites that can be used to carry out parts, or the whole, of the information collection for an audit activity.

Resources

Links to resources that can be used to deepen an auditors understanding.

ACTIVITIES

Summary

A short - one to four sentence - basic overview of the activity.

Base Line Skills

The baseline level of skills that the auditor must posses in order to carry out the intended activity.

Operational Security

Operational security guidelines that are specific to this activity.

Materials Needed

Any materials beyond the norm that the trainers will need.

Instructions

Where relevant, an outline of the steps an auditor will take during this activity. Not intended to replace true documentation, but useful for an auditor unable to connect to the Internet or to provide the organization's technical contact.

Considerations

Some of the activity specific concerns (ethical, skill level, time, relationship, etc.) that an auditor must take into consideration when conducting this activity.

Output

Notes on what data can be created during this activity.

Resources

Links to resources that can be used to deepen an auditors understanding of an activity.

APPENDIX: HOW TO CONTRIBUTE TO SAFETAG

CONTRIBUTING TO SAFETAG

SAFETAG welcomes contributions!

SAFETAG is a community-managed product with an advisory board and community management roles laid out in our Code of Conduct. The Code of Conduct further outlines expectations of not only those using the content herein but also those contributing to it. By participating, you are expected to uphold this code.

When submitting new content, please write in clear, concise, and gender neutral language. This document will be updated with guidance on content translation once we have settled on a process for that. If you would like to submit content in a language other than English or Spanish, please open an issue to set that language up for submission.

GETTING STARTING

Before you start work, it is critically important to review the current content and existing issues and **create a new issue for your proposed work** to solicit feedback -- this will save you a lot of time as the SAFETAG community can help refine your idea and advise on where best to include it in the framework (is it a new method? An activity or variant? Is there existing content in SAFETAG to update or improve?), as well as suggest additional resources worth considering, operational security and safety considerations.

CONTENT CREATION GUIDELINES

This section helps walk you though how SAFETAG is constructed, and what pieces of content are important to provide in a submission. Submissions which do not follow these guidelines will take significantly longer to be incorporated.

SAFETAG has currently three main compiled products - an **overview guide**, the **full guide**, and a **curricula** to help train new auditors. This guide is primarily focused on the non-curricular SAFTAG content. The Curricula is an ADIDS-based approach to training on SAFETAG content (read more about the curricula content at https://github.com/SAFETAG/SAFETAG/wiki/Curricula-Document-Template

The SAFETAG overview is the easiest place to start. The full guide is a comprehensive collection of not only the method-based objectives of the audit, but a variety of specific activities an auditor might choose to use and combine to achieve those. Both of these are built from the collection of Methods and Activities that make up SAFETAG.

Generally speaking, **Methods** are high-level, goal-focused aspects of the assessment. There are inevitable "fuzzy" borders between some methods. Creation of new methods should be minimized to not overly complicate the scope of SAFETAG.

Activities are the meat of an audit, and answer "how" and "where" type questions. To accomplish the goals of a method, one might conduct multiple activities to explore and verify organization practices from different angles - research, policy review, conversations / discussions, and technical verification, exploration, and scanning.

Within both Methods and Activities are smaller chunks of content which are used across the full range of SAFETAG "products." The tables below map out what content chunks exist across which products, and what they are. The Templates folder has sub-folders which provide the default files and indices for methods and activities.

SAFETAG is in the process of being rebuilt in a more interactive, meta-data driven interface at https://github.com/contentascode/safetag. The current structure will be migrated into this format, and updates to the process will be posted here.

CREATING A NEW SAFETAG METHOD

- Follow the Getting Started instructions above.
- Decide on a name for the method, and create the a corresponding folder (lowercased, with _ replacing spaces). If your new method is "Creating SAFETAG Content", the folder would be *en/methods/creating_safetag_content*.
- Copy the Method template files from https://github.com/SAFETAG/SAFETAG/tree/master/en/templates/folders/method into the method folder. The content of these files is described below.

- Create index files for your method: In addition to the content files below, each Method must also have two index files, a method_name.guide.md and a method_name.overview.md . The contents of these index files are generally the same for every method, and templates exist at https://github.com/SAFETAG/SAFETAG/tree/master/en/templates/folders .

New methods must be lined into the master index file, and must have activities linked to them. To link the new method into the master index file (and therefore have the method "included" in the "master" SAFETAG build, these index files must be linked into the relevant master index file in the language folder (*en/index.guide.md* and *en/index.overview.md*). See below for how Activities are linked in to the methods.

Method Content notes:

- Try to focus on creating Activities rather than Methods.
- All Methods must have all of the content listed below unless marked as "optional".
- All Methods must have at least one activity associated with them.
- Ideally, also create curricula content for each Method, or at least notes for someone training on the topic.

Method Section and Stylistic notes:

- Methods should operate at header 2 and 3. The Method title is h2, and the major subheadings (below) are h3. No additional header levels should be used.
- The Flow of Information graphics live in *en/images/info_flows* and follow the *method_name.svg* naming convention.

Section	ADIDS	Guide	Overview	Definition
Quote	-	-	-	OPTIONAL: No longer included in the compiled guides, but an introductory / framing quote for the section
Summary	-	+	+	A short - two to three sentence - basic overview of the methodology -- What is the auditor doing , what are the high-level outputs and processes?
Purpose	+	+	+	The justification for why this methodology is used -- Why is this collection of activities being pursued? what is the end goal?
Information Flow	-	+	+	The "Flow of Information" shows the types of information that an audit activity builds upon (input), and the types of information that an audit activity may reveal (outcomes). As this information is acquired, earlier audit will have to be re-visited based upon this information -- What are the inputs which feed in to this, and what outputs are possible/expected? Modify the Information Flow diagram in images/info_flows
Guiding Questions	+	+	+	Each audit activity is guided by a small set of core questions. Key questions are included to help an auditor identify when they have acquired enough information and customize their approach while still collecting the correct types of information to support the organization -- What are specific guiding or research questions to be answered by conducting activities in pursuit of the larger goal?
Approaches	-	+	+	Many of these audit activities can be completed in multiple ways depending upon auditor skill and the organizational technical setup and capacity. The approach section includes a descriptive, bulleted list of activities that can be used to carry out parts, or the whole, of the information collection for an audit activity. -- What are the high-level approaches to answering the guiding questions? Try to list different types of approaches - some might be technical, some research, some interactive
Outputs	-	+	-	The data or impact is expected from this method -- What are specific outputs to aim for? These should further clarify the information flow diagram above.
Operational Security	-	+	+	OPTIONAL: Operational Security considerations -- Does pursuing this objective have any broad operational security challenges to be aware of that is not otherwise captured in the per-activity detail?
Preparation	-	+	-	OPTIONAL: Any preparation, skills, or materials needed for the method as a whole. Individual exercises will specify this more exactly -- What must an auditor do to prepare for this work that is not otherwise captured in the per-activity detail?
				Resources should include not only the research used in the creation of the method, but also recommended reading, references, and additional options for conducting this work -- What references did you use in creating this method? Are there references

Section	ADIDS	Guide	Overview	Definition
Resources				Links to provide activity style walkthroughs or additional backgrounds? Are there existing collections of references (in the references folder) that an auditor should review when looking at this methodology.
Activities	-	+	-	Specific activities to conduct in pursuit of this objective. See "Creating a New SAFETAG Activity" -- What existing activities are useful to achieve the goal and specific output(s) listed? Do they represent? If creating a new method, often new activities will be needed to ensure the suggested approaches are "filled in". Please note that Activities are separate documents linked in to the Methods

CREATING A NEW SAFETAG ACTIVITY

- Follow the Getting Started instructions above.
- Decide on a name for the activity, and create the a corresponding folder (lowercased, with _ replacing spaces). Activity contents live in the exercises folder under the language folder, so *en/exercise/exercise_name/...*). If your new activity is "Using atom to edit SAFETAG markdown files", the folder would be something like *en/exercises/using_atom/* .
- Copy the Activity template files from https://github.com/SAFETAG/SAFETAG/tree/master/en/templates/folders/activity into the method folder. The content of these files is described below.
- Activity contents also have an index file (within the same folder, not above it as with methods). The index file needs to be updated with the title of the activity but is otherwise the same across most activities.

New activities must be linked to a method. To link an activity to a method, please update both the activities.md file in the method folder, and also add it directly to index.guide.md under the method. The current build process uses the index.guide.md link, but for content tracking, it's best to update both. If adding an activity to multiple methods, select a primary method where it is the most relevant to that method's outputs, and for additional methods, link it in following this format:

```
<div class="boxtext">
#### Activity Title
Covered in full in Primary Method:
</div>
```

Activity Content notes:

- Try to focus on creating Activities rather than Methods.
- All Activities must have all of the content listed below unless marked as "optional".
- All Activities must be linked to at least one Method.
- Ideally, also create curricula content for each Activity, or at least notes for someone training on the topic.

Note: For activities where multiple different approaches could fulfill the exact same goals, activity variants are being explored, see https://github.com/SAFETAG/SAFETAG/issues/315 for detail.

Activity Content and Stylistic notes:

- Activities should operate at header 4 and below, the Activity title is h4, the major subheadings (below) are h5, so any headings within the content (most often used in the instructions/walkthrough file) must only be at h6.

Section	ADIDS	Guide	Overview	Definition
Summary	-	+	-	A concise description of the exercise. This describes the vulnerability of class of vulnerabilities (e.g. "PHP is out of date") and its overall impact -- What does this specific activity accomplish?
Overview	-	+	-	A short, bulleted list that clarifies the general steps, especially for cases where the walkthrough is very complex or involves multiple or parallel processes. Also included when only referencing an exercise from a method, instead of including the full exercise.
Materials Needed	-	+	-	Optional; does this require specific software, hardware, or preparation?
				Optional; Notes on safely carrying out the activity and protecting the data collected, as well as other challenges (psycho-social, legal, ethical) to be

Section	ADIDS	Guide	Overview	Definition
Considerations				Are there operational security concerns, or important baseline skills to master before undertaking this activity?
Walkthrough	-	+	-	A multi-use guide with concise instructions for a skilled technologist to replicate or prove the vulnerability. This is used in the SAFETAG curricula, by auditors needing to recall that random flag for that one command without going online, and for the organization's technical staff to verify that this vulnerability has been addressed. This should provide concise guidance at a peer level for the general steps an auditor should take, but should point to, not re-create existing documentation. For technical aspects, ideal walkthroughs should enable IT staff/contractors to follow along and verify fixes. For research activities, research methods and preferred resources should be provided, and for facilitative exercises, a clear explanation of the process and any tips or challenges should be explained.
Variants	-	+	-	Parallel approaches which can be used for the same affect but might work better in different contexts. See https://github.com/SAFETAG/SAFETAG/issues/315
Recommendations	-	+	-	Optional; Sample text of common recommendations for how to address vulnerabilities identified through this activity; e.g. "Work with the webmaster to update PHP and/or migrate to a hosting system which manages this automatically...") -- for activities which have common findings, provide stock language to assist in report creation

OTHER SAFETAG CONTENT

These sections operate at header level 1, and for the most part should be included in any custom creation of SAFETAG products.

Front and Back Matter

Generally speaking, these sections won't be updated very often.

Section	ADIDS	Guide	Overview	Description
Title Page	+	+	+	Can be customized for your needs, locally only
License	+	+	+	Please do not change the License
Introduction	-	+	+	Welcome language
Overview	-	+	+	An overview of the SAFETAG approach and the audit life-cycle
"Metro" Map	+	+	+	
Risk Assessment		+	+	
Agency Building		+	+	
Operational Security	-	+	-	Overall operational security concerns for the assessment process
Preparation	-	+	+	How to prepare to conduct an assessment
Appendices	-	+	-	Including the Code of Conduct, How To Read this Guide, Contribution guidance, and more.
Footnotes	-	+	+	

Reporting Contents

Reporting content and creation will be revisited shortly

CONTRIBUTING

Once you've scoped your submission as described under "Getting Started" and the "Content Creation Guidelines" sections above, you can follow the fork/pull method or use the templated approach to submit new content. Regardless of the approach you take,

Using Submission Templates

We have developed easy to use templates for SAFETAG Methods and Activities you can use and submit with your issue. These can be found at *en/templates/method-template.md* and *en/templates/activity-template.md*. If you would like to edit these as word processor files, you can use pandoc for conversion: pandoc -i activity_template.md -o activity_template.odt . Final files should be submitted as markdown, however.

Please refer to the current Methods in the SAFETAG guide for additional detail and examples. The template will require manual merging into the repository, so please include how you would like to be credited.

Using Pull Requests

0. Fork the repository, clone a local copy, and a create a new branch for your work (See Resources below for help with using git).
1. Update your issue with your fork so the community can follow along!
2. Follow the content creation guidelines below to create or update new content
3. Making many small, targeted commits with concise, clear commit messages. Keeping each pull request focused is greatly appreciated. Please submit different pull requests (and possibly even branches!) for different thematic work.
4. Test to make sure your changes work by building the PDF and/or migrating the content into the static site generator system.
5. Push to your fork and submit a pull request to the Dev branch!

RESOURCES

- Super Basic Git Guide for Content Development
- Using Pull Requests
- GitHub Help

APPENDIX: DRAFT ENGAGEMENT AND CONFIDENTIALITY AGREEMENT

In order to protect the privacy of SUBJECT, AUDITOR agrees to comply with the following restrictions:

- AUDITOR commits to prioritizing the stability and integrity of SUBJECT’s digital infrastructure over any additional testing could be carried through more aggressive methods. AUDITOR will make every effort to avoid disrupting SUBJECT's work environment, even temporarily. No tests will be performed that would stress the network, or any individual workstation, beyond what could be expected from normal use. If they has any doubt, AUDITOR will consult with SUBJECT before carrying out the test.
- AUDITOR will not share the assessment report—or any notes created, data gathered or knowledge obtained about SUBJECT during the evaluation—with anyone other than a single point of contact, designated by SUBJECT. AUDITOR may need to share some general information with SUBJECT staff, as part of requesting information necessary to carry out the audit itself. If AUDITOR has any concern that this could be sensitive, they will first clear it with that point of contact. This commitment to protecting SUBJECT's private information extends to AUDITOR’s colleagues, supervisor and funder, all of whom have demonstrated their own respect for this policy in three previous audits. The only details about the assessment that will be shared, confidentially, with these three groups (and only these three groups) will include: a) the name and location of the organization audited; b) basic time line information; and, with SUBJECT's approval, anonymized “lessons learned,” which will be aggregated with those from at least one other assessment. During and after the audit itself, all data will be stored securely in an encrypted volume on AUDITOR’s computer.
- AUDITOR will securely delete all data from the audit one week after submitting the final assessment report to SUBJECT or, any time, should SUBJECT's request it.
- If, at any time, AUDITOR feels that they might be called upon to give advice that could be out of line with SUBJECT's own IT policies, they will first clear it with SUBJECT.
- AUDITOR will work with whatever level of access SUBJECT is comfortable providing. This includes access to staff members for brief "interviews," as well as more technical access, such as passwords, local connectivity, privileged or unprivileged accounts on local or remote services, etc.. That said, some level of access typically allows an auditor to produce a report that is significantly more useful than the output a pure "black box" audit. (And this is doubly true when the auditor wishes to tread lightly in order to avoid impacting the stability of the subject’s network infrastructure and the productivity of its staff.)

APPENDIX: TRAVEL KIT AND CHECKLIST

Travel Kit Checklist

Hardware

- Laptop with encrypted drive
- Laptop power supply
- Travel power adapter
- ethernet cord (and adapter if needed)
- aircrack compatible Wireless card if needed
- IEEE 1394 (firewire) card if using
- Non-phone based camera
- Secure storage media for audit findings
- Spare storage media

Software / digital resources

- Update and test Kali and additional software tools
- Dictionaries
- Locally-cached guides
- Prepared and secured SAFETAG audit directory
- Verify tools are ready to go

Facilitation Supplies

- Post-it notes
- Sharpies

Logistics

- Visa and other travel documents
- Hotel reservation
- Travel tickets
- Ground transit plan (to your hotel, to the site)
- Emergency contact numbers
- Travel plan

APPENDIX: SAMPLE CAPACITY INTERVIEW QUESTIONS

Introduction

For this interview, I will mostly ask you about how your organization relates to tech tools in a general sense. I will also ask specific questions about how your organization works with digital security issues.

Together, this information will help me identify _____

All of the information we collect here will be kept completely private.

This interview will last approximately ____ hour.

Please feel free to stop me or ask if a question is unclear, or if you would like to take a break.

The interview starts with some questions about you and the organization. Again, this will all be kept strictly confidential.

Open Up

"Warm up the participant with questions they are comfortable with." [90]

1. What is your name?
2. What is your position in the organization?
3. What are your main responsibilities in this organization?
4. When was the organization created?
5. What issues does the organization work on? (Provide an example if needed - Examples below)
    - Human Rights
    - Transparency
    - Public Service Delivery
    - Health
    - Free Media and Information
    - Climate Issues
    - Gender Issues
    - Poverty Alleviation
    - Community Building
    - Peace promotion
    - Agricultural Development
    - Entrepreneurship
    - Water, Sanitation
    - Transportation
    - Disaster Relief
    - Other
    - No Specific Mandate
6. Where does your organization have activities?
7. Does the organization have activities in more than one (city/provence/country/region)
8. What kind of funding does you organization receive?
9. Could you tell me, approximately, which percentage of the organization's currently annual budget is dedicated to supporting the use of digital or mobile technology?
10. How many projects is your organization currently managing?
11. Does the organization have its own office space?
12. Does the organization have a domain name or brand identity that is used for all online communications?
13. What is the organization's working language? (for password dictionary)
14. What other languages are used by the organization, formally or informally? (for password dictionary)
15. In what language has your organization accessed online resources to support its work?
16. How many paid, full-time staff does the organization employ
17. How many paid, part-time staff does the organization employ?

8. How many unpaid workers, such as volunteers or interns work at least one day a month at the organization?
9. Does the organization have a staff member responsible for working with digital or mobile technology? Yes, more than one
10. Is this staff member responsible for any of the following area
    - Office IT infrastructure
    - Internet Presence or website
    - Outreach or communications
    - Managing programs
11. How regularly do staff members of the organization travel outside of your country
12. Does the organization do any of the following activities when travelling internationally
    - Run programs
    - Participate in events
    - Run trainings
    - Receive trainings
    - Fundraising

Go Broad

"Prompt bigger, even aspirational, thinking that they may not be accustomed to on a daily basis." [91]

Go Specific

"Dig deeper on the challenge at hand & prompt with 'what if' scenarios." [92]

3. What is the most important reason for your organization to exist? (Provide an example if needed - Examples below)
    - To raise awareness in the organization's policy area.
    - To impact policy.
    - To improve policy.
    - To improve service delivery.
    - To change specific legislative or administrative governance structures.
    - To provide citizens with a greater voice in public addaitrs and delberations
    - To expose corruption or malfeasance
    - No concrete strategic objectives.
4. Does the organization provide services directly to individuals (for example health, educational or legal service?)
5. What type of direct services does the organization provide? (Provide an example if needed - Examples below)
    - Legal Services
    - Health Services
    - Education Services
    - Water/Sanatation Services
    - Financial Services
    - Other Services
6. Does the organization primarily rely on digital media in its work?
7. Does your organization use....
    - Email
    - Email newsletters
    - Websites
    - Maintain blog or discussion fora, or another social media account(s)
    - Engage in online discussions and interactions on external sites
    - Maintain interactive websites
    - paid software (like microsoft office or basecamp) to manage the organization or projects
    - Free branded platforms (like google apps) to manage the organization or projects
    - digital or mobile tools to collect data or evidence
    - Digital or mobile tools to deliver health, financial, or other public services
    - Mass communication to mobile phones
    - security software (anti-virus, circumvention tools, etc)
    - disseminate information through third party sites and platforms.
    - Other

8. What other digital tools does your organization use?
9. What are the most important motivations for the organization to use these tools?
0. Are there any specific outcomes for the organization's stakeholders that you hope digital or mobile technologies can facilitate?

1. Does the organization have specific plans to increase their capacity to use digital or mobile technologies in their work

2. Do the organization's staff have access to computers for their work?
3. How many staff members do not have access to their own computer or need to share computers with other?
4. How many people of the organization's staff currently use digital or mobile technology on a daily basis?
5. How many of the organization's currently active projects would not be possible without the use of these media?
6. Does the organization have a hierarchy for decision- making, according to which different people have different responsibility and levels of authority?
7. Has the organization used any of the following methods to build skills and capacities for using digital or mobile technologies?
    - Local Training
    - Training in other countries
    - Online Training
    - Purchesing equiptment or hardware
    - hiring consultants
    - hiring staff or restructring human resources
    - devoting staff time to independant learning
    - participating in international events
    - searching and learning online
8. Which other method(s) to build skills for using digital and mobile technologies?
9. Have these efforts to increase capacity targeted specific staff members in the organization?
0. Has the organization actively worked to strengthen its digital security in the last year?
    - (IF NO) Why did the organization not work to strengthen its digital security in the last year?
    - (IF YES) How the organization work to strengthen its digital security in the last year?
1. Which of the below factors are the three most significant obstacles to the efficient use of digital and mobile technology by your organization?
    - Limited skills of staff
    - Limited infrastructure for media or electricity.
    - Limited technical literacy and media use among staff
    - limited financial resources
    - Insufficient hardware or software
    - None
    - Other
    - don't know
2. What new activities using digital or mobile technologies would the organization like to attempt in the future? Please give examples of programs, activities, or management functions...
3. Has the organization used the internet (including online training, discussions or research) to get better at any of the following activities.
    - Communicating with stakeholders and raising awareness on issues.
    - Keeping the organization and its staff safe.
    - Fundraising and developing the organization's strategic focus.
    - Managing staff and organizational activities (such as payroll, hiring and other administration)
    - Measuring impact of programs.
4. Why are you having the audit done?
5. How well do you believe your organization is able to identify appropriate digital and mobile technology tools for the organization's work?
6. How well do you believe your organization is able to use appropriate digital and mobile technology tools for the organization's work?
7. Has turnaround in staff members been a problem for retaining technical capacity in your organization?
8. In what ways, if any, have you experienced that technology inhibits the organization's work?
9. Are there systems on the network which the client does not own, operate, or rely on, that may require additional approval to test?
0. Does the organization communicate with its beneficiaries/members/sources?
    - How does the organization communicate with its beneficiaries/members/sources?
1. Does the organization use any of these tools to maintain information about its members?
    - Paper lists
    - Mobile phone contact lists

- Email contact lists
- Spreadsheets
- CRM (customer relationship management software)
- Other

2. What other tools does the organization use to maintain information about its members?
3. I will now read a list of hardware tools you might be familiar with. From this list, could you please tell me about the three tools that are most important to the organization?
    - Desktop computers
    - Laptop Computers
    - Mobile Phones
    - Satellite Phones
    - Video Equiptment
    - Cameras
    - USB Dongles
    - Hard Drives
    - Servers
    - Audio Recorders
    - Web Cams
    - Wireless Routers
    - Other
4. Other hardware that is important to the organization's work? Please describe if needed.
5. How important you think each of these hardware tools is for achieving the organization's strategic objectives?
6. I will now read a list of software tools you might be familiar with. From this list, could you please tell me about the three tools that are most important in the daily work of your organization?
    - Social media
    - Blogging Platforms
    - Tools for creating and managing pictures or videos
    - Cloud Based collaboration applications
    - Budgeting Software
    - Tools for building and managing websites
    - project management software
    - Anti-virus software
    - tools for managing databases
    - Graphic design or visualization software
    - software to manage sms or mobile communication for groups
    - circumvention software
    - other

7. Other software that is important to the organization's work? Please describe if needed.

8. To your knowledge, how often do the below incidents occur in the geographic areas or issue areas in which your organization is active? Could you please tell me if you think they happen never, sometimes or often
    - The government lawfully intercepts information communicated by civil society or private person
    - The government lawfully confiscates equipment because of the information it contains
    - Government, public officials, non-state actors, police or security forces use digital or mobile technology to identify and target individuals for arrest or violen
    - Government, public officials, non-state actors, police or security forces use digital or mobile technology to attack the reputations of individuals or organizations
9. To your knowledge, how often do the below actors use digital or mobile technology to target or to identify individuals for arrest or violence? Do they use it never, sometimes, or often.
    - government or public officials
    - non-state actors (corporations, social groups)
    - police, security forces or paramilitary groups
10. And how often would you say that these actors use digital or mobile technology to monitor or gather information on civil society activities? Never, sometimes, or often.
    - government or public officials
    - non-state actors (corporations, social groups)
    - police, security forces or paramilitary groups
11. What do you feel are the most immediate and serious digital threats to the organization?
12. How much risk do you feel each of these digital threats presents to your organization?
    - Online surveillance
    - DDOS (Distributed Denial of Service) Attack

- Targeted for physical violence on the basis of digital activity
- Data loss
- Other.

3. Do you feel that any of these threats place the physical security of your staff in danger?
4. Do you feel that any of these threats place the physical security of your stakeholders in danger?
5. Do you feel that any of these threats place the physical security of your beneficiaries in danger?
6. In the last six months, have you or any of your civil society peers experienced any of the following?
    - Intimidation or threats of violence by public officials, police or security force
    - Intimidation or threats of violence by private or non-state actors.
    - Threats of arrest or detention
    - Arrest
    - Threats of Torture.
    - Confiscation of equipment
    - Threats to administrative standing, such as stripping individuals of professional accreditation or organization of licenses
    - Other
7. How has your organization responded to these threats?
    - Addressed the issue in the press/online
    - Told other organizations about the threat
    - Contacted the authorities
    - Trained staff to prevent and mitigate such threats in the future
    - Requested help from other organizations
    - Invested in hardware
    - raised funds
    - has not responded
    - other
8. Has the organization taken any of the following steps to prepare against digital or physical threats?
    - Staff have been trained
    - There are specific plans in place for specific situations
    - Equiptment and/or supplies have been made ready
    - Other
9. Does the organization experience power outages in its office
10. Does the organization have access to the Internet in its offices?

11. In the last month, has your organization lost access to Internet for reasons other than power outages

Management Only

2. Is the manager aware that a test is about to be performed?
3. What data would create the greatest risk to the organization if exposed, corrupted, or deleted?

Technical Only

4. Are there any systems which could be characterized as fragile? (systems with tendencies to crash, older operating systems, or which are unpatched)
5. Are testing and validation procedures to verify that business applications are functioning properly in place?
6. Are Disaster Recovery Procedures in place for the application data?
7. Are Change Management procedures in place?
8. What is the mean time to repair systems outages?
9. Is any system monitoring software in place?
10. What are the most critical servers and applications?
11. Do you use backups in your organization?
    - Are there any data/devices that are not backed up?
    - Are backups tested on a regular basis?
    - When was the last time the backups were restored?

2. How many websites does your organization have?
3. What are their url's?
4. Where are they hosted?
5. How many wireless networks are in place at the organization?
6. Is a guest wireless network used? If so:
7. Does the guest network require authentication?
8. What type of encryption is used on the wireless networks?
9. Approximately how many clients will be using the wireless network?
10. How many total IP addresses are being tested?
11. How many internal IP addresses, if applicable?
12. How many external IP addresses, if applicable?
13. Are there any devices in place that may impact the results of audit scans such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?

Categories

Below are the categories each question fits within. Use this to help you reduce the information you obtained from the interview into manageable themes, insights, and implications.

Basic Information

5, 6, 8, 10, 11, 13, 14, 15, 24, 25, 7

Threat Information

58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68

Capacity

Capacity questions seek to reflect organizations' readiness and likelihood to succeed in engaging with technology in their work. [93]

23, 26, 27, 28, 34, 35, 36, 37, 38, 39, 40, 43, 45, 46, 29, 30, 31, 55, 9, 16, 17, 18, 19, 20

Challenge

Challenge questions seek to reflect the degree to which internal an external factors will complicate or inhibit the effective and safe uptake and use. [94]

41, 40, 42, 46, 47, 48, 69, 70, 71

Audit Scope

Scope questions explore what the client is looking to gain out of the audit, why the client is looking to have an audit performed against their environment, and whether or not they want certain types of tests performed during the audit. [95]

44, 72, 49, 51, 50, 52

Network Audit Questions

90, 91, 92, 93, 81, 80, 79, 78, 77, 49, 74, 75, 76, 53, 54, 56, 57

APPENDIX: PASSWORD DICTIONARIES

PASSWORD DICTIONARY CREATION

Summary

This component provides resources and recommendations on cracking passwords - both the creation of dictionaries and rules to modify those dictionaries, as well as some basic implementation as well. This is a dangerous (and in many cases, illegal) skill to use, and should be more of a guide to auditors on what password security myths do not work against modern password cracking software, and to use only with permission and only in very specific situations as a demonstration of the power of even a common laptop against weak passwords.

Description

Weak passwords are prevalent - even after hundreds of well-publicized global password breaches, "password" and "12345" remain the most popular passwords. This exercise supports the auditor in building an effective dictionary and using it to attack non-personal and non-disruptive parts of an organization's infrastructure. Weak wifi passwords are specifically a challenge, as wifi signals often are accessible outside of an office's physical limits, but provide full access to the private network.

This skillset, plus demonstration against non-invasive accounts, provides an opening for a discussion with staff on password security. See Level Up for further activities and exercises around passwords.

Approach

- Download basic word lists
- Research dictionary needs
- Create custom word list
- Build core list(s)
- Attack a password hash using increasingly more time-consuming methods

Instructions

Primarily for use in the Network Access component, building a password dictionary, understanding the ways to automatically mutate it, and running it against passwords is a useful skill to have, and to use to explain why simple passwords are insecure. This Ars Technica article provides a good insight into the path to tackle iterative password cracking using a variety of tools to meet different goals.

These instructions use a small set of password cracking tools, but many are possible. If there are tools you are more familiar or comfortable with using, these by no means are required. The only constraints are to be respectful and responsible, as well as keeping focused on the overall goals and not getting bogged down.

A good wordlist with a few tweaks tends to break most passwords. Using a collection of all English words, all words from the language of the organization being audited, plus a combination of all these words, plus relevant keywords, addresses, and years tends to crack most wifi passwords in a reasonable timeframe.

An approach which begins with quick, but often fruitful, attacks to more and more complex (and time consuming) attacks is the most rewarding. However, after an hour or two of password hacking, the in-office time on other activities is more valuable, so admit defeat and move on. See the Recommendations section for talking points around the levels of password cracking that exist in the world. You can work on passwords offline/overnight/post-audit for report completeness.

Here is a suggested path to take with suggested tools to help. You might try the first few steps in both the targeted keyword approach and the dictionary approach before moving on to the more complex mutations towards the end of each path.

- Targeted Keywords
- Begin with a simple combination of organizationally relevant keywords (using hashcat's combinator attack, combining your org keyword list with itself)
- Add in numbers/years (simple scripting, hashcat, JtR)

- Add in other mutators like 1337 replacements, capitalization tricks (John)
- Language dictionary attack (simple scripting, hashcat)
- Run a series of dictionary word attacks:
    - A simple language dictionary attack
    - Add in numbers/years (simple scripting, hashcat, JtR)
    - Add in the org keywords (a full combination creates a massive list, recommend starting with 1:1)
    - Try other combinations of the dictionary, keywords, years
    - Add in other mutators like 1337 replacements, capitalization tricks (John)
- Brute forcing (do not bother with this on-site)
- John's incremental modes, limited by types
- Crunch's raw brute-force attack (very, very time intensive - a complete waste of time without GPUs)

Dictionary Research and Creation

Before you arrive on-site it is important to have your password cracking tools downloaded and relevant dictionaries ready to go, as your main demonstration and use of these tools is to gain access to the organization's network. The effectiveness of this demonstration is drastically reduced if you already have had to ask for the password to connect to the Internet and update your dictionaries, tools, or so on. Some of these files (especially larger password dictionaries) can be quite large, so downloading them in-country is not recommended.

Many password dictionary sites, such as SkullSecurity , maintain core dictionaries in multiple languages. If your target language is not available, some quick regular expression work can turn spell-check dictionaries (such as those used by LibreOffice into useful word lists. It is generally useful to always test with English in addition to the target language.

[CloudCracker(]https://www.cloudcracker.com/dictionaries.html) and OpenWall have, for a fee, well-tested password dictionaries.

KEYWORD GENERATION

In addition, create a customized dictionary with words related to the subject as revealed in the Remote Assessment research -- including, but not limited to:

- Organization name (complete and broken down into syllables)
- Organizational acronyms
- Organizational registration numbers (business/tax ID)
- street address / city / state / country
- phone number
- email/web domain
- wireless network name or BSSID
- Founders
- Keywords from program themes, mission, vision
- Founding date of the organization (note the local date system)

For the organization "ExampleOrg , which has its offices at 123 Central St., Federal District, Countryzstan , which does human rights and journalism work and was founded in 1992, some context-based dictionary additions would be:

exampleorg
example
org
EO
123
central
federal
district
countryzstan
human
rights
journo
journalism
1992
92

Also add common password fragments: qwerty, 1234/5/6/7/8, and, based on field experience, four-digit dates back for ~20 years in both the Gregorian (Western) and (if relevant) local calendar, plus the founding year of the organization). It's quite amazing how often a recent year will be part of a wifi password -- this presentation discusses many common patterns in passwords: https://www.owasp.org/images/a/af/2011-Supercharged-Slides-Redman-OWASP-Feb.pdf

Optional Further steps

Use CeWL, to spider the organization's web properties to generate additional phrases. This list will need review, as some of the generated content is not very useful, but may be useful if the site is not in a language the auditor reads fluently.

For passwords other than WPA, specific policies or patterns may help to focus your password dictionary further. PACK, or Password Analysis and Cracking Toolkit is a collection of utilities developed to aid in analysis of password lists in order to enhance password cracking through pattern detection of masks, rules, character-sets and other password characteristics. The toolkit generates valid input files for Hashcat family of password crackers." PACK is most useful for large sets of passwords, where it can detect patterns in already-broken passwords to help build new rules. Both password cracking tools listed here are powerful, and have slightly different abilities. The auditor should choose the one they prefer and/or the one which has the features they desire for this job.

Combinator Attack with scripting and Hashcat

One quick way to build a more complex password list is to simply double the list up (a "combinator" attack), so that it includes an entry for each pair of these strings:

You can do a 1-way version of this list simply, such as:

```
$ for foo in `cat pwdlist.txt`; do for bar in `cat pwdlist.txt`; do printf $foo$bar'\n'; done; done > pwdpairs.txt
$ cat pwdlist.txt >> pwdpairs.txt
```

Hashcat can do this in a live attack under its "combinator" mode, and hashcat-utils (hiding in /usr/share/hashcat-utils/combinator.bin) provides this as a standalone tool. This provides a true combination of the list, so it exponentially increases the list size - use with caution, or use with one larger dictionary and one smaller dictionary.

For example, use these combination approach on your custom dictionary (combining it with itself, creating combinations from the above list such as example92, journorights, exampleorgrights).

```
$  /usr/share/hashcat-utils/combinator.bin dict.txt dict.txt
```

Hashcat is extremely powerful when you have desktop computer systems to use, but has a few wordlist manipulation tools that are useful regardless.

More References: (http://hashcat.net/wiki/doku.php?id=cracking_wpawpa2 , http://www.darkmoreops.com/2014/08/18/cracking-wpa2-wpa-with-hashcat-kali-linux/)

Word mutation with John the Ripper (JtR)

JtR is a powerful tool you can use in combination of existing wordlists, but it also can add in common substitutions (people using zero for the letter "o"). JtR can be used to generate a static list of passwords for other programs, or it can be used directly against a password database. JtR is a bit weak combining words within a wordlist, so you should apply your customizations and any folding before moving on to JtR.

You can add custom "rules" to aid in these substitutions - a base set is included with JtR, but a much more powerful set is added by [KoreLogic] (http://contest-2010.korelogic.com/rules.html). KoreLogic also provides a custom character set "chr file" that takes password frequency data from large collections of real-world passwords to speed up JtR's brute force mode . This PDF presentation has a good walkthrough of how John and Kore's rules work

Additional guides: * (http://linuxconfig.org/password-cracking-with-john-the-ripper-on-linux)

The bleeding-edge jumbo version combines both the built-in rules and an optimized version of the KoreLogic rules. This list of KoreLogic Rules provides nice descriptions of what the KoreLogic rules do. In bleeding-jumbo, you can remove "KoreLogicRules". BackReference provides a great example of rules usage.

Some particularly useful ones individual rulesets are: * AppendYears (appends years, from 1900 to 2019) and AppendCurrentYearSpecial (appends 2000-2019 with punctuation) * AddJustNumbers (adds 1-4 digits to the end of everything) * l33t (leet-speek combinations)

There are some build-in combinations of rulesets - for example, just --rules runs john's internal collection of default rules, and --rules:KoreLogic runs a collection of the KoreLogic rules in a thoughtful order, and --rules:all is useful if you hate life.

e.g. :

```
$ john -w:dictionary.txt --rules:AppendYears --stdout
```

Building custom rules

PROTIP Create a dictionary with just "blah" and run various rules against it to understand how each ruleset or combination works. Note specifically that each rule multiplies the size of the dictionary by the number of permutations it introduces. Running the KoreLogic ruleset combination against a **one word** dictionary creates a list of 6,327,540 permutations on just that word.

Brute force, using John and crunch

JtR's "incremental" mode is essentially an optimized brute force attack, so will take a very long time for anything but the shortest passwords, or passwords where you can limit the search space to a character set: "As of version 1.8.0, pre-defined incremental modes are "ASCII" (all 95 printable ASCII characters), "LM_ASCII" (for use on LM hashes), "Alnum" (all 62 alphanumeric characters), "Alpha" (all 52 letters), "LowerNum" (lowercase letters plus digits, for 36 total), "UpperNum" (uppercase letters plus digits, for 36 total), "LowerSpace" (lowercase letters plus space, for 27 total), "Lower" (lowercase letters), "Upper" (uppercase letters), and "Digits" (digits only). The supplied .chr files include data for lengths up to 13 for all of these modes except for "LM_ASCII" (where password portions input to the LM hash halves are assumed to be truncated at length 7) and "Digits" (where the supplied .chr file and pre-defined incremental mode work for lengths up to 20). Some of the many .chr files needed by these pre-defined incremental modes might not be bundled with every version of John the Ripper, being available as a separate download." (http://www.openwall.com/john/doc/MODES.shtml)

As a last resort, you can try a direct brute force attack overnight or post-audit to fill in details on key strength. Crunch is a very simple but thorough approach. Given enough time it will break a password, but it's not particularly fast, even at simple passwords. You can reduce the scope of this attack (and speed it up) if you have a reason to believe the password is all lower-case, all-numeric, or so on. WPA passwords are a minimum of 8 characters, a maximum of 16, and some wifi routers will accept punctuation, but in practice these are usually just !@#$. — so:

```
$ /path/to/crunch 8 16 abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890$!@#$. | aircrack-ng -a 2 path/to/capture.pcap -b 00:11:22:
```

This says to try every possible alpha-numeric combination from 8 to 16 characters. This will take a very, very, very long time.

Recommendations

Any important password should be long enough and complex enough to prevent both standard dictionary attacks and “brute-force attacks” in which clusters of powerful computers work in parallel to test every possible character combination. (We recommend 12 or more completely random characters or a passphrase that contains five or more relatively uncommon words.) The key should not contain common “phrases,” expecially from well known literature like Shakespeare or religious texts, but also should not include number sequences or phrases, especially if they are related to the organization, its employees or its work.

Specifically for wireless passwords, choosing a strong WPA key is one of the most ild not mportant steps toward defending an organization’s network perimeter from an adversary with the ability to spend some time in the vicinity of the offices. By extension, mitigating this vulnerability is critical to the protection of employees and partners (and confidential data) from the sort of persistent exposure that eventually brings down even the most well-secured information systems.

Because shared keys inevitably end up being written on whiteboards, given to office visitors and emailed to partners, the WPA key should also be changed periodically. This does not have to happen frequently, but anything less than three or four times per year may be unsafe.

Sample Practice

For practice on any of these methods, you can use the wpa-Induction.pcap file from Wireshark.

Resources

https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

http://zed0.co.uk/crossword/

http://www.instantcheckmate.com/crimewire/is-your-password-really-protecting-you/#lightbox/0/

Note that password cracking systems are rated on the number of password guesses they make per second. Stock laptop computers without high-end graphics cards or any other optimizations can guess 2500 passwords/second. More powerful desktop computers can test over a hundred million each second, and with graphics cards (GPUs) that rises to billions of passwords per second. (https://en.wikipedia.org/wiki/Password_cracking).

This website has a good explanation about how improving the complexity of a password affects how easy it is to break: http://www.lockdown.co.uk/?pg=combi , but is using very out of date numbers - consider a basic laptop able to produce "Class E" attacks, and a desktop, "Class F"

http://rumkin.com/tools/password/passchk.php

http://cyber-defense.sans.org/blog/downloads/ has a calculator buried in the zip file "scripts.zip"

http://www.dailymail.co.uk/sciencetech/article-2331984/Think-strong-password-Hackers-crack-16-character-passwords-hour.html

https://www.grc.com/haystack.htm

https://www.owasp.org/images/a/af/2011-Supercharged-Slides-Redman-OWASP-Feb.pdf

http://www.nytimes.com/2014/11/19/magazine/the-secret-life-of-passwords.html?_r=1

APPENDIX: PASSWORD SURVEY

Password Survey

How many passwords do you have to remember for accounts and devices used to do your work?

- [ ] No
- [ ] Yes

If you tried to login to your computer account right now, how many attempts do you think it would take?

- [ ] No
- [ ] Yes

To how many people have you given your current password?

- [ ] No
- [ ] Yes

Have you ever forgotten your current password?

- [ ] No
- [ ] Yes

If yes, how did you recover it?

Have you ever forgotten old work passwords?

- [ ] No
- [ ] Yes

If yes, how did you recover it?

When you created your current password, which of the following did you do?

- [ ] I reused an old password
- [ ] I modified an old password
- [ ] I reused a password I was already using for a different account
- [ ] I created an entirely new password
- [ ] Other:

Did you use any of the following strategies to create your current password (choose all that apply) ?

- [ ] Password based on the first letter of each word in a phrase
- [ ] Based on the name of someone or something
- [ ] Based on a word or name with numbers / symbols added to beginning or end
- [ ] Based on a word or name with numbers and symbols substituting for some of the letters (e.g. '@' instead of 'a')
- [ ] Based on a word or name with letters missing
- [ ] Based on a word in a language other than English
- [ ] Based on a phone number
- [ ] Based on an address
- [ ] Based on a birthday

How long is your current password (total number of characters)?

- [ ] I prefer not to answer.

What symbols (characters other than letters and numbers) are in your password?

- [ ] I prefer not to answer.

How many lower-case letters are in your current password?

- [ ] I prefer not to answer.

How many upper-case letters are in your current password?

- [ ] I prefer not to answer.

In which positions in your password are the numbers?

- [ ] I prefer not to answer.
- [ ] First
- [ ] Second
- [ ] Second from last
- [ ] Last
- [ ] No Numbers
- [ ] I prefer not to answer.

In which positions in your password are the symbols?

- [ ] I prefer not to answer.
- [ ] First
- [ ] Second
- [ ] Second from last
- [ ] Last
- [ ] No Numbers
- [ ] I prefer not to answer.

Have you written down your current password?

- [ ] No
- [ ] Yes, on paper
- [ ] Yes, electronically (stored in computer, phone, etc.)
- [ ] Other

If you wrote down your current password how is it protected (choose all that apply) ?

- [ ] I do not protect it
- [ ] I stored it in an encrypted file
- [ ] I hid it
- [ ] I stored it on a computer or device protected with another password
- [ ] I locked up the paper
- [ ] I always keep the password with me
- [ ] I wrote down a reminder instead of the actual password
- [ ] Other

Do you have a set of passwords you reuse in different places?

- [ ] No
- [ ] Yes

Do you have a password that you use for different accounts with a slight modification for each account?

- [ ] No
- [ ] Yes

APPENDIX: DEVICE ASSESSMENT CHECKLIST

APPENDIX: REMOTE FACILITATION

Remote Facilitation

Summary

This component suggests approaches to use if in-person facilitation is not possible, and to include participation from remote staff or offices when an organization has multiple locations. This supplements the Data Assessment, Process Mapping, and Threat Assessment exercises, enabling them to be conducted remotely.

This may not provide as deep results as in-person facilitation, but should provide adequate levels of expansion and verification of information needed, and even provide the secondary benefits in most cases of helping the organization build a shared understanding of its processes, risks, and riosk tolerances.

Overview

There are four different approaches you can use, depending on what resources are available, the size and structure of the organization, and which activities you are trying to facilitate remotely. Is there someone that can help as an on-site facilitator? Are video conferences realistic (given bandwidth and cost)? How does the approach you use interact with existing organizational team structures?

- **Approach 1: On-site facilitator**: This provides the most valuable interaction, but requires a person who can take on the facilitation role on-site, while the auditor is over video chat. The facilitator does not have to be a technical person, but should be able to manage the session, making sure that it is as inclusive and as productive as possible. Accommodates more participants per session than Approach 3 per session.
- **Approach 2, hybrid online/synchronous**: This can be used with a large group of participants where it is possible to meet over multiple sessions with enough time to collect and analyse responses in between.
- **Approach 3, multiple small sessions**: Consists of multiple small full sessions over video chats, of no more than four participants at a time to assure inclusiveness. Suitable for medium to large groups where it is possible to conduct multiple small video chats.
- **Approach 4, hybrid offline/surveys**: This leverages surveys and shorters calls or emails. It will provide less information overall, but can be used when it is not possible to meet in person, over video chat, or through a local facilitator.

Materials Needed

- Secure video chat services, (check: ricochet.im, meet.jit.si, chatb.org)
- Fallback communication channels
- Desktop sharing or secure online spreadsheet service to collectively work on information, as an alternative to whiteboard.
- Templates, per activity

Considerations

- Ensure to conduct the exercise over secure communication channels
- Ensure secure management of notes and collected information

Walkthrough

Selecting the most suitable approach requires understanding of the capacity and personel structure of the organization, including their ability to support communication technologies, and the availability of someone that can assist in facilitation.

After selecting the most suitable approach, auditor should make sure to prepare for remote facilitation:

- Work with the organization point of contact to select the most suitable approach.
- Schedule calls/meetings and/or discuss timelines for survey preparation, sending, and deadlines for input.
- Prepare any material to be sent and distributed beforehand.
- Coordinate (including perhaps training) with on-site facilitator if ny.
- Prepare at least one fallback communication channel.
- Test communication channels.

Approach 1, on-site facilitator, with video chat auditor

Suitable when there is a person that can take a facilitation role on-site. Facilitator does not have to be a technical person, but should be able to manage the session, making sure that it is as inclusive and as productive as possible. Accommodates more participants than Approach 3 per session. If the auditor is able to join remotely, this provides an ideal substitute.

- On-site facililtator assists in conducting the over all exercise, ensuring inclusion of all participants. Level of facilitator envolvement needs to be decided between the facilitator and auditor before the session, and if needed training may be provided to the facilitator
- Auditor follows along via video chat through the full exercise and discussion, and is able to contribute or ask follow-up questions as needed.
- Facilitator leads the session and managing note-taking, as well as secure sharing of notes post-session.
- Follow up sessions may be arranged with selected groups of staff.

Approach 2, hybrid online/synchronous

Can be used with large group of participants, where it is possible to meet over multiple sessions with enough time to collect and analyse responses in between.

- An introductory video chat is recommended as a starting point, this allows the auditor to introduce themselves, the exercise, and agree on communication rules. This will help in building rapport, and address any concerns participants may have, as well as allow for further testing of communication channel.
- The auditor ask participants to fill in a template or survey to collect information needed (See Approach 4 for survey details), this stems directly from the activity, whether it is data assessment, process mapping, threat analysis, or any activity requiring facilitation.
- Participants send their input to auditor, either through answering into and online questionnaire, or through any other media agreed on.
- Auditor collect the information and arrange them for analysis and discussion.
- Another video chat is conducted to discuss responses and expand and validate on information collected through the survey.
- Follow up sessions may be arranged with selected groups of staff as needed.

Approach 3, multiple small sessions

Suitable for medium to large groups where it is possible to conduct multiple small video chats. It is recommended for sessions to be arranged to include people from the same organizational level, but different functions/teams/arms/departments of the organization. This approach scales to larger organizations and helps ensure voices at different levels of the organization are heard.

- Auditor works with participants via video chat through the full exercise and discussion.
- Follow up sessions may be arranged with selected groups of staff as needed.

Approach 4, hybrid offline/asynchronous

- Introductory email/session through local facilitator (may need to provide remote training on the activities).
- Collect responses and input through a survey.
- Discuss responses and finding via email or voice chat to expand and validate.

Sample Questions: Data Mapping

- Where does your organizational email live? Please select all devices where email is stored or accesses:
- [ ] Email server / webmail
- [ ] Backup server
- [ ] Office computers
- [ ] Office Laptops
- [ ] Office cell phones
- [ ] Backup drives
- [ ] Personal laptops
- [ ] Personal cell phones
- [ ] Tablets
- [ ] Designated Travel laptops/tablets
- [ ] Other? _____
- Where does the organization share files?
- [ ] Email
- [ ] Shared drive at office
- [ ] Box/Dropbox/OneDrive/etc.
- [ ] Custom hosted (owncloud, etc.)
- [ ] Google Drive/Docs
- [ ] USB drives
- [ ] Other? _____
- What types of files does the organization track and use?
- [ ] Financial records
- [ ] HR / personal contracts (personal data, including ID and bank info)
- [ ] Other personal data (passports, etc.)
- [ ] Funding records
- [ ] Sensitive / internal program records
- [ ] Publications
- [ ] Videos
- [ ] Project proposals

Footnotes

1. Event Planning Inputs - Level-Up↩
2. " 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."↩
3. " 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."↩
4. "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."↩
5. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. Section 7.1 Coordination ↩
6. "Obviously, being able to get in touch with the customer or target organization in an emergency is vital." ↩
7. See the auditor trainee resource list ↩
8. APPENDIX A - Auditor travel kit checklist ↩
9. ^NIST_SP_800-115-travel_prep↩
10. Auditor Tool Resource List - Password Dictionary Creation ↩
11. APPENDIX A - Auditor travel kit checklist ↩
12. "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."↩
13. " 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."↩
14. "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."↩
15. "Obviously, being able to get in touch with the customer or target organization in an emergency is vital." ↩
16. " 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."↩
17. "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."↩
18. Determining Audit Location - The Penetration Testing Execution Standard: Pre-Engagement Guidelines ↩
19. "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."↩
20. 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.↩
21. Determining Audit Location - The Penetration Testing Execution Standard: Pre-Engagement Guidelines ↩
22. "Before starting a penetration test, all targets must be identified. " ↩
23. "Obviously, being able to get in touch with the customer or target organization in an emergency is vital." ↩
24. "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."↩

25. "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."↩
26. "One of the most important documents which need to be obtained for a penetration test is the Permission to Test document."↩
27. Dealing with third parties - The Penetration Testing Execution Standard ↩
28. APPENDIX D - Auditor Consent Template. ↩
29. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. Section 7.1 Coordination ↩
30. "Obviously, being able to get in touch with the customer or target organization in an emergency is vital." ↩
31. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. Section 7.1 Coordination ↩
32. Emergency Contact and Incidents - The Penetration Testing Execution Standard: Pre-Engagement Guidelines ↩
33. " 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."↩
34. "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."↩
35. " 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."↩
36. Accumulating information about partners, clients, and competitors - The Penetration Testing Execution Standard ↩
37. The flow of information through the Recon-ng framework. (See: "Data Flow" section) ↩
38. Accumulating information about partners, clients, and competitors - The Penetration Testing Execution Standard ↩
39. Acquiring API Keys↩
40. The flow of information through the Recon-ng framework. (See: "Data Flow" section) ↩
41. See: Vulnerability Analysis↩
42. Identifying Software Versions↩
43. Examining Firewalls Across OS ↩
44. APPENDIX C - Password Survey↩
45. Password Security↩
46. Privilege Separation Across OS ↩
47. Anti-Virus Updates↩
48. Identifying Software Versions↩
49. Device Encryption By OS Type↩
50. APPENDIX C - Password Survey↩
51. Password Security↩
52. Privilege Separation Across OS ↩
53. Anti-Virus Updates↩
54. Identifying Software Versions↩

55. Device Encryption By OS Type ↩
56. Microsoft Security Bulletin ↩
57. "In-Depth Reading, Vendor Information, & External Advisories" ↩
58. "Security-Related Vendor Information" ↩
59. "CERT/CC Advisories" ↩
60. "Security Tracker" ↩
61. "Known Vulnerabilities in Mozilla Products" ↩
62. Microsoft Security Bulletin ↩
63. "In-Depth Reading, Vendor Information, & External Advisories" ↩
64. "Security-Related Vendor Information" ↩
65. "CERT/CC Advisories" ↩
66. "Security Tracker" ↩
67. "Known Vulnerabilities in Mozilla Products" ↩
68. "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." ↩
69. "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 ↩
70. Network Access ↩
71. APPENDIX B - Personal Information to Keep Private ↩
72. APPENDIX B - Personal Information to Keep Private ↩
73. "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." ↩
74. "Pre-Mortum Strategy" - Sources of Power: How People Make Decisions - p.71 ↩
75. "Pre-Mortum Strategy" - Sources of Power: How People Make Decisions - p.71 ↩
76. "Pre-Mortum Strategy" - Sources of Power: How People Make Decisions - p.71 ↩
77. Corruption Perception Index ↩
78. The ISC Project completes evaluations of information security threats in a broad range of countries. The resulting comprehensive written assessments describe each country's digital security situation through consideration of four main categories: online surveillance, online attacks, online censorship, and user profile/access. ↩
79. EISF distributes frequent analysis and summaries of issues relevant to humanitarian security risk management. ↩
80. The top 500 sites in each country or territory. ↩
81. Who publishes Transparency Reports? ↩
82. "Impacts: Chapter 2.7 p. 46 - Operational Security Management in Violent Environments" ↩
83. "Likelihood: Chapter 2.7 p. 47 - Operational Security Management in Violent Environments" ↩

84. " 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."↩

85. "Threat Modeling: Designing for Security" by Adam Shostack ↩

86. See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 125. ↩

87. "Threat Modeling: Designing for Security" by Adam Shostack ↩

88. See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 401. ↩

89. "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↩

90. "IDEO Human-Centered Design Toolkit"↩

91. "IDEO Human-Centered Design Toolkit"↩

92. "IDEO Human-Centered Design Toolkit"↩

93. "TechScape Indicators - the engine room"↩

94. "TechScape Indicators - the engine room"↩

95. "Questionnaires - The Penetration Testing Execution Standard"↩