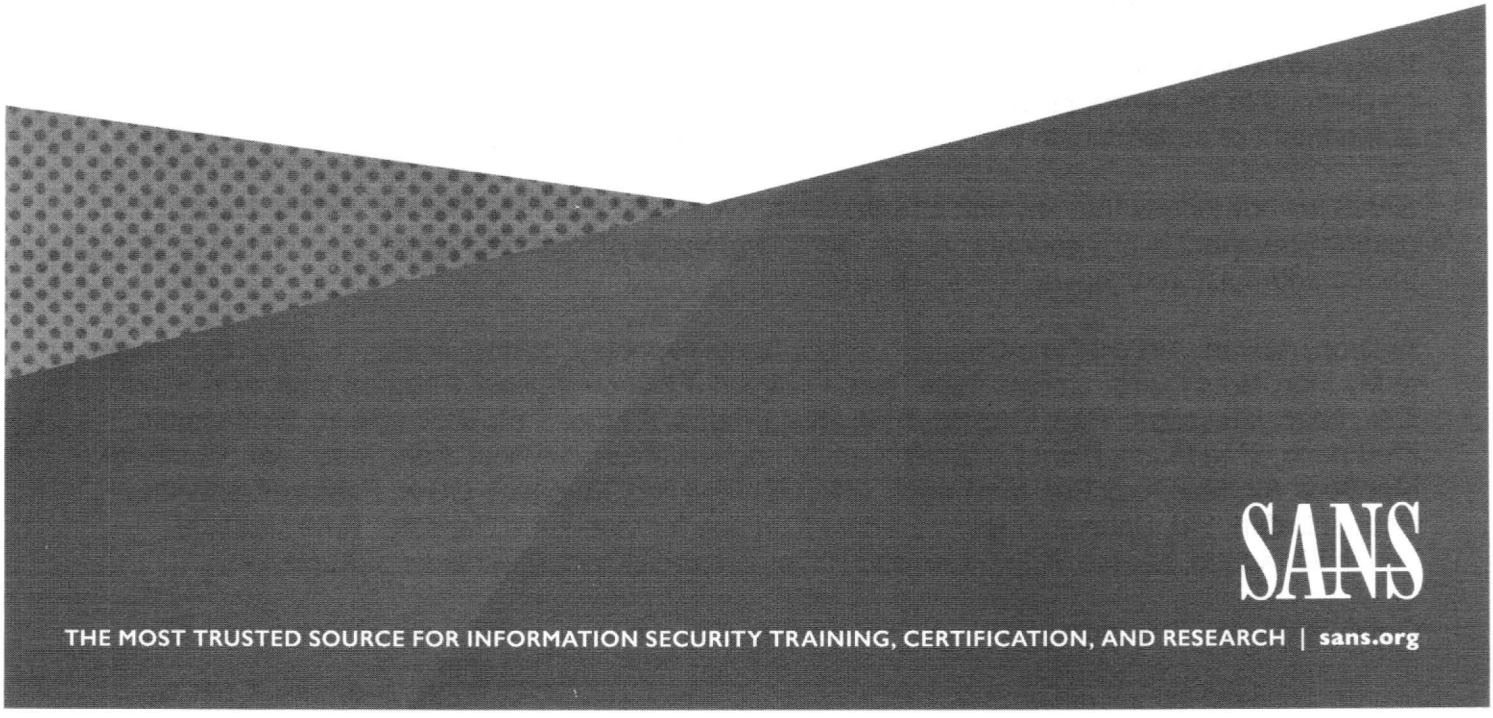
460.4
Validation, Triage, and Mass Data Management



SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

SEC460.4 | Enterprise Threat and Vulnerability Assessment

SANS

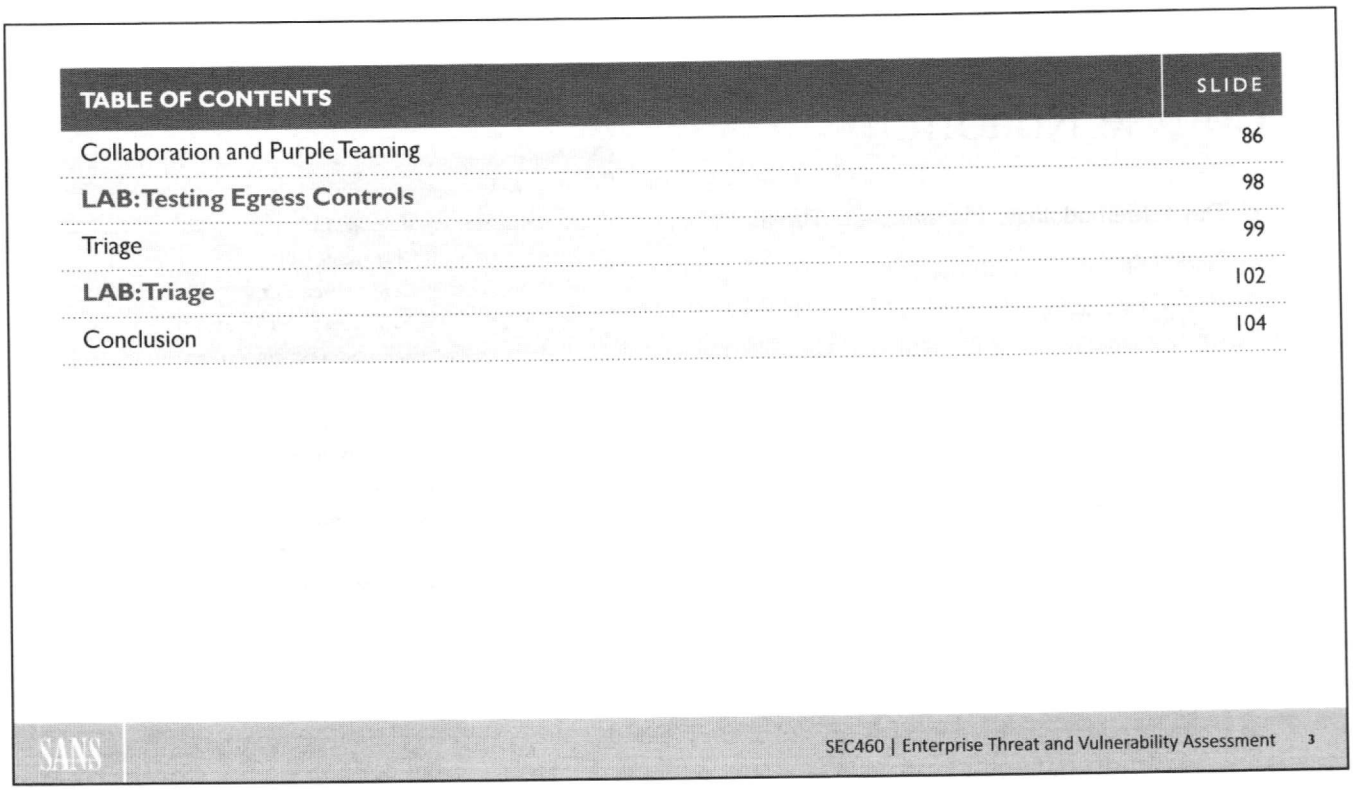
Validation, Triage, and Mass Data Management

Enterprise Threat and Vulnerability Assessment - Validation, Triage, and Mass Data Management

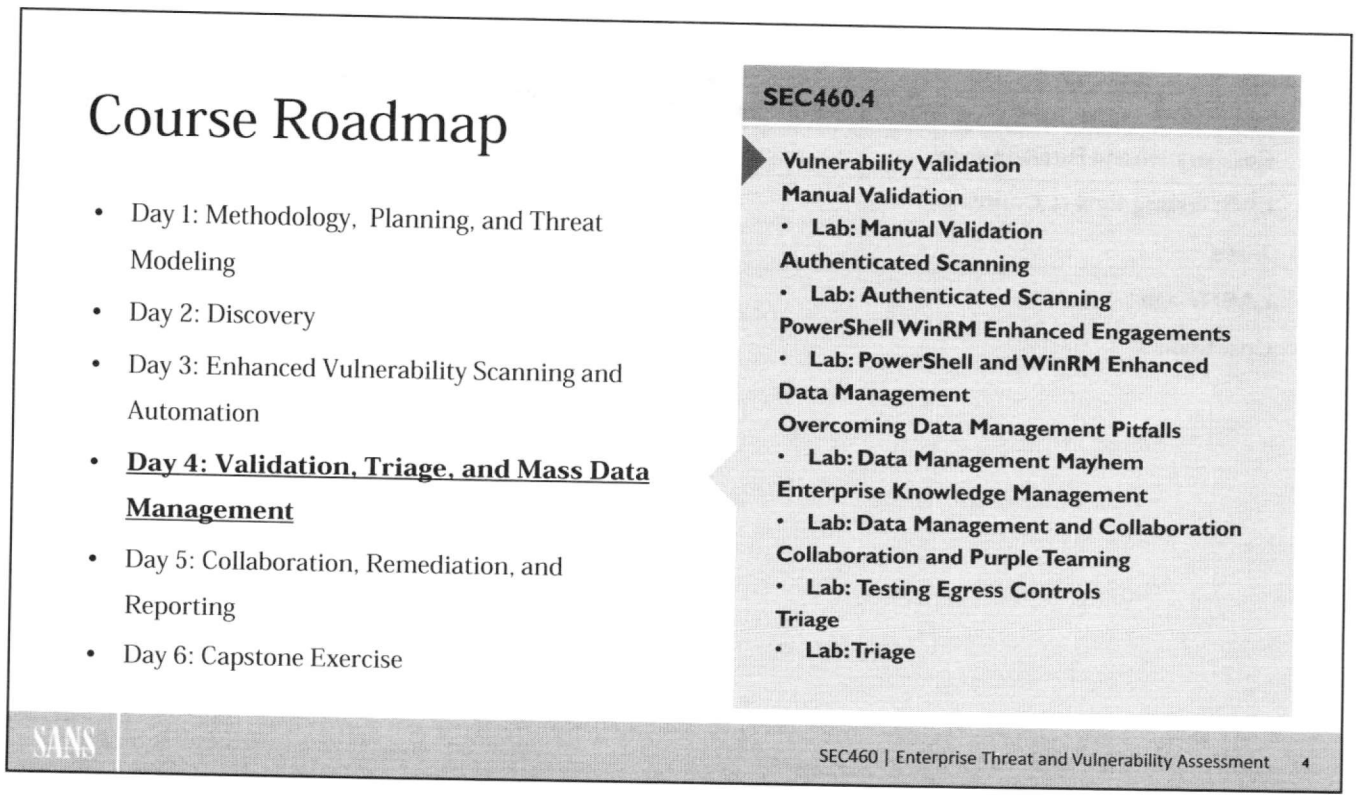
Hello and welcome back as we dive into Enterprise Threat and Vulnerability Assessment day four! In this section, we will plunge into data, data, and more data as we learn the key components and struggles surrounding the fifth phase of the Vulnerability Assessment Framework. The discussion and learning objectives today will examine the mass data management strategies and explore lean techniques for automated validation and PowerShell enabled operations.

TABLE OF CONTENTS	SLIDE
Vulnerability Validation	4
Manual Validation	12
LAB: Manual Validation	22
Authenticated Scanning	23
LAB: Authenticated Scanning	41
PowerShell WinRM Enhanced Engagements	42
LAB: PowerShell WinRM Enhanced Engagements	47
Data Management	48
Overcoming Data Management Pitfalls	55
LAB: Data Management Mayhem	67
Enterprise Knowledge Management	68
LAB: Data Management and Collaboration	85

This slide is a table of contents. Note that labs are in boldface, so you can more easily find and refer to them.

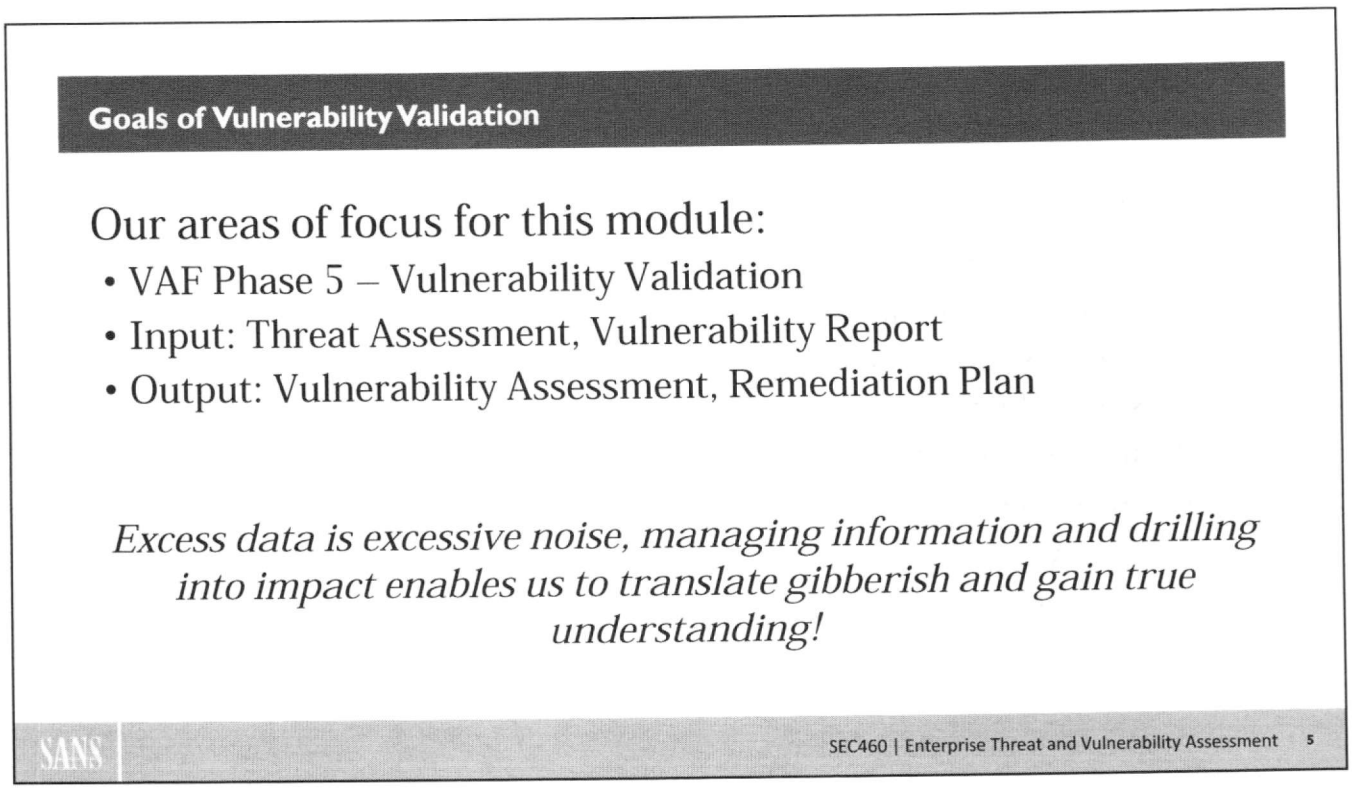


This slide is a table of contents. Note that labs are in boldface, so you can more easily find and refer to them.



Course Roadmap: Vulnerability Validation

Before we can truly work with the vulnerability data gathered from the last module's content we need to guarantee its efficacy. In this module, we begin with manual testing to enable validation of our discoveries.



Goals of Vulnerability Validation

Over the course of the day we will tackle the next phase of our overarching testing methodology, vulnerability validation, while simultaneously confronting the biggest headaches common to a vulnerability assessment at scale. At large scale, vulnerability data can be overwhelming and possibly even contradictory. We will cover the specific techniques needed to wade through and better focus those data. Next, we will examine techniques for collaboration and data management with the Acheron tool for analyzing vulnerability data across an organization.

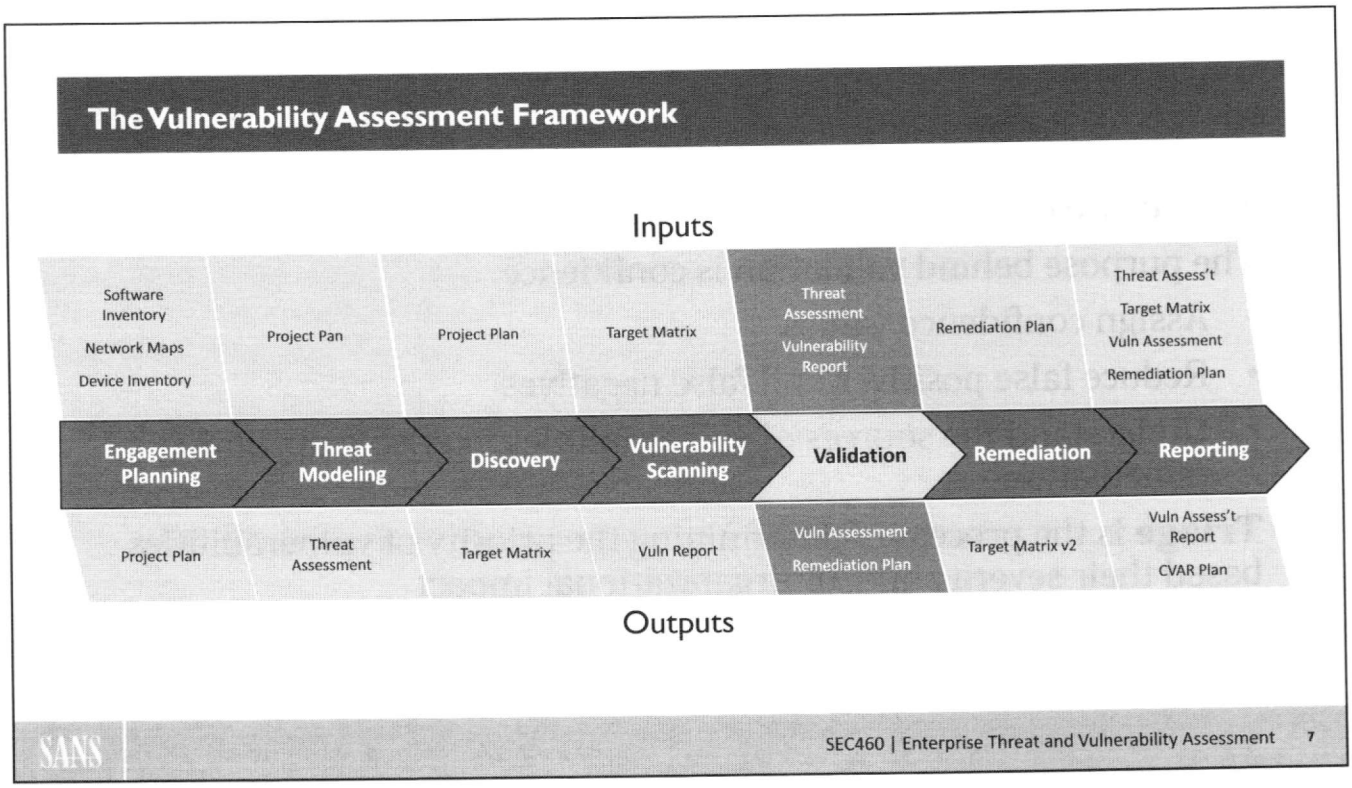
- Assigning a Confidence Value and Validating Exploitative Potential of Vulnerabilities
- Manual Vulnerability Validation Targeting Enterprise Infrastructure
- Converting Disparate Datasets into a Central, Normalized, and Relational Knowledge Base
- Managing Large Repositories of Vulnerability Data
- Querying the Vulnerability Knowledge Base
- Triage: Assessing the Relative Importance of Vulnerabilities Against Strategic Risk

Goals of Vulnerability Validation

Tactics Snapshot

- Manual Validation of Vulnerability Scanning Results
  - False Positive Reduction Techniques
  - Enterprise Scripting Enhanced with WinRM
- Mass Data Management
- Assigning Confidence Values
- Constructing and Maintaining a Vulnerability Knowledge Base
- Triage: Assessing the Relative Importance of Vulnerabilities Against Strategic Risk

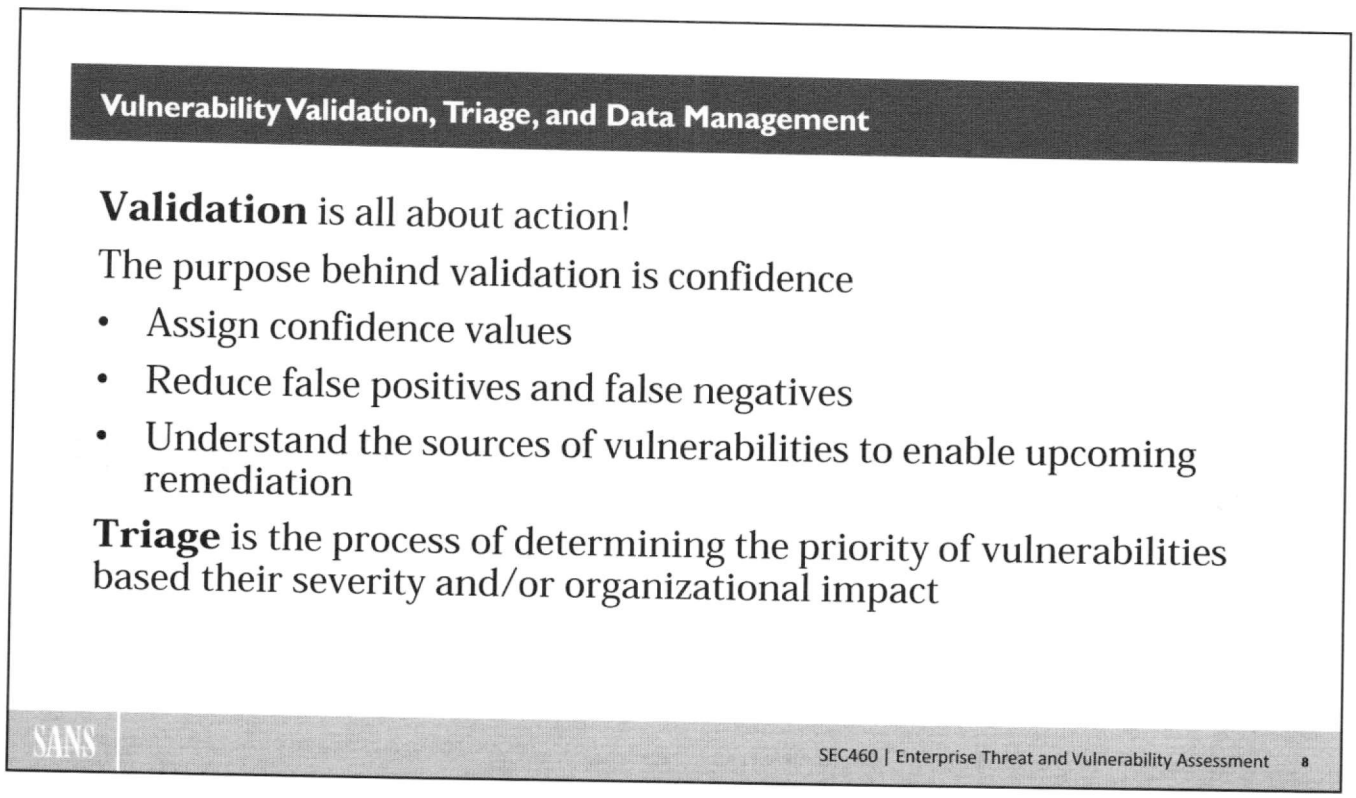
This page intentionally left blank.



The Vulnerability Assessment Framework – 04 | Vulnerability Scanning

Vulnerability Scanning is the fourth phase of the Vulnerability Assessment Framework, but it is often mistaken for the entire process. Today we take a highly technical deep dive into vulnerability discovery focusing on the edges so that we can quickly identify exactly what our scanning systems are able to provide as well as where they may be deficient.

These foci combined will empower us to be value-added members of the information security team from day one!



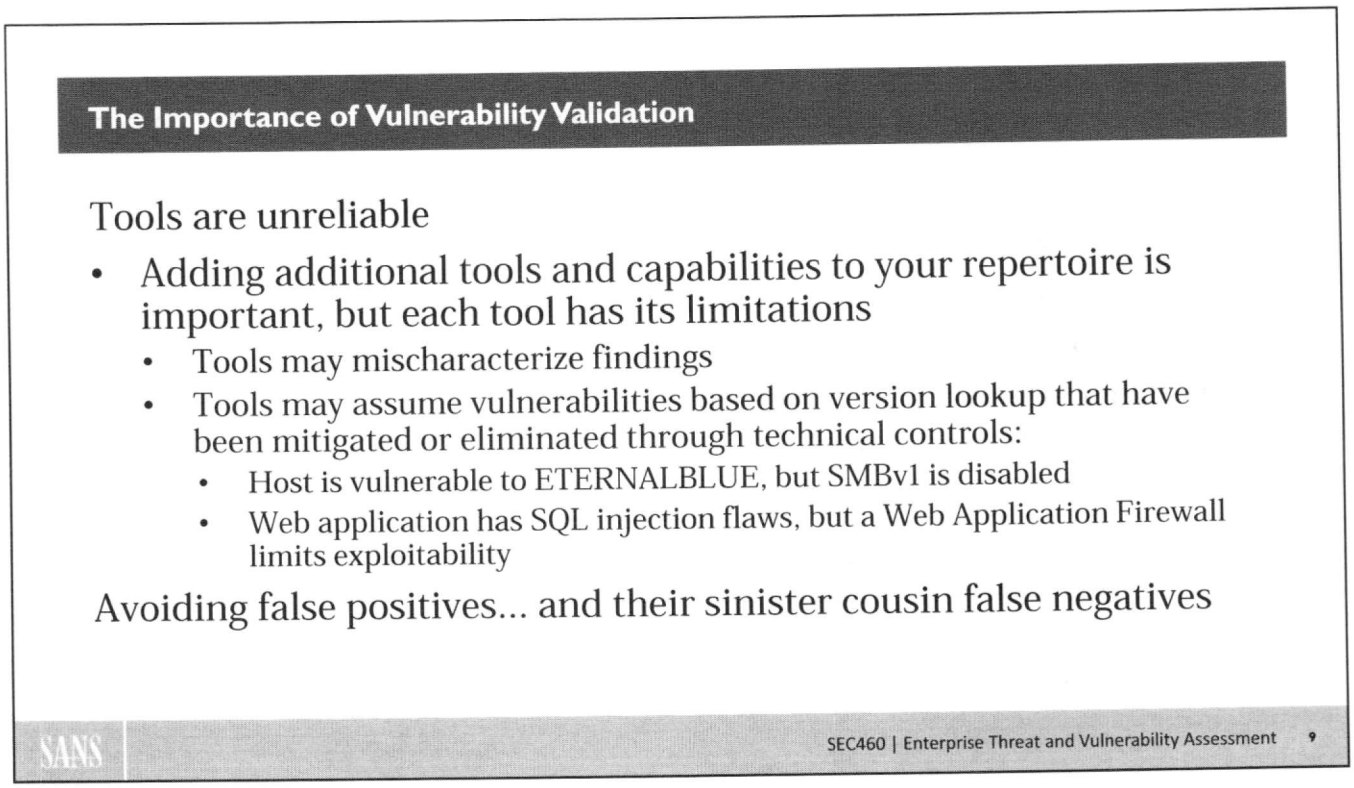
Vulnerability Validation, Triage, and Data Management

Our purpose behind validation is confidence. Assigning confidence values to our outputs is the difference between an allegation and a conviction. Validating potential vulnerabilities enables us to push the scale. Some vulnerabilities may require exploitation, pillaging and/or pivoting to ascertain impact. This process also meets some compliance and audit requirements identified in previous days of SEC460.

Inputs: listing of all potential vulnerabilities. Outputs: listing of validated vulnerabilities and confidence rating values. Feedback to compliance requirements.

Tools: manual validation, scripting.

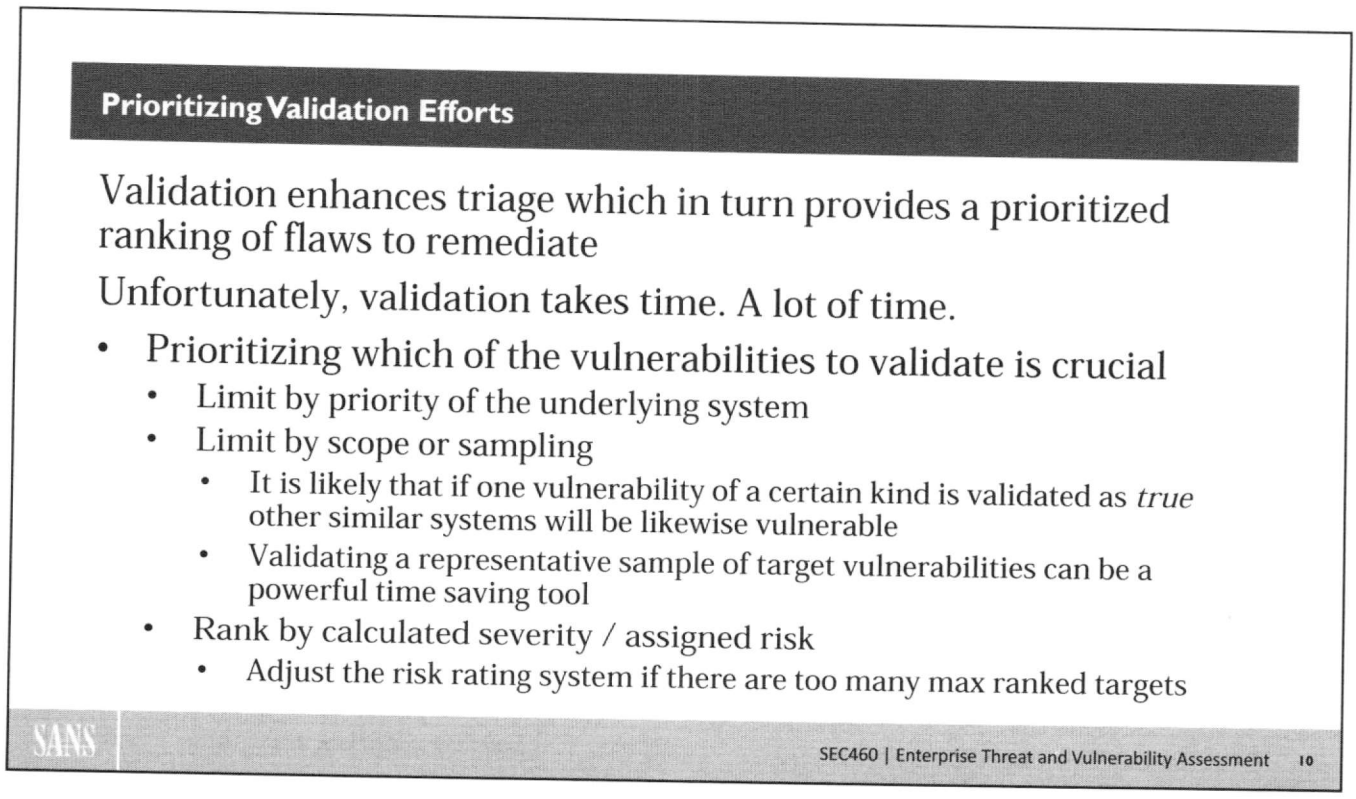
One major issue we face when performing enterprise assessments is collaboration tools and data management. We will discuss various tools and techniques available to do so. Examples include LAIR, MagicTree, Dradis, and Acheron.



The Importance of Vulnerability Validation

Vulnerability assessment is not always able to nail down a definitive conclusion. Whereas more intrusive services like Red Teaming and Penetration Testing come to a defined end state with known resultant fallout, Vulnerability assessment is somewhat more nuanced. Without exploitation how can we be sure of the efficacy of our findings. What about the false positives?

Vulnerability validation is a key aspect of any good assessment strategy and forms the barrier that separates cybersecurity charlatans from value added members of the information security team.



Prioritizing Validation Efforts

Validation enhances triage which in turn provides a prioritized ranking of flaws to remediate. Unfortunately, validation takes time. A lot of time. Prioritizing which of the vulnerabilities to validate is crucial. Some overarching categories to drive your triage planning are:

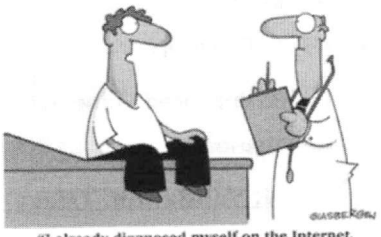
Prioritization – Not all systems are created equal. Reducing the pool of targets to only the most vital systems worthy of your time and consideration is a compelling method to ensure optimal value.

Scope – There are a few ways to turn scope to your advantage when performing vulnerability assessments. Limiting the subset of targets to those systems most likely to produce results is an example of scope control. Limiting scope by manually testing a representative sample of the vulnerabilities discovered is another.

Validation Techniques

Second Opinion – Retest the finding with an alternative tool or technique

- Reduce false positives
- Like getting a second opinion



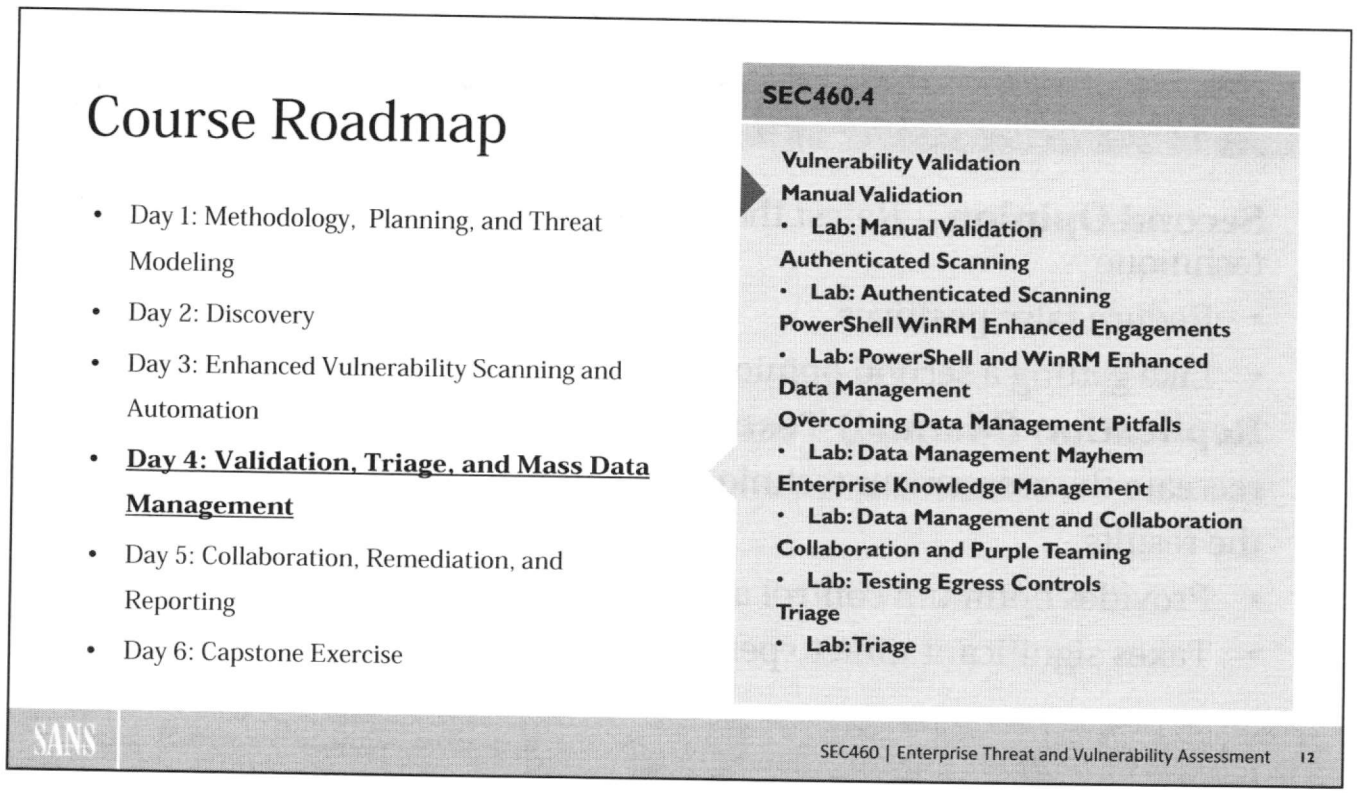
"I already diagnosed myself on the Internet. I'm only here for a second opinion."

Replication (Manual) Testing – Manually recreate the assessment technique to confirm the results

- Provides optimum control and result understanding
- Takes significant time to perform for each finding

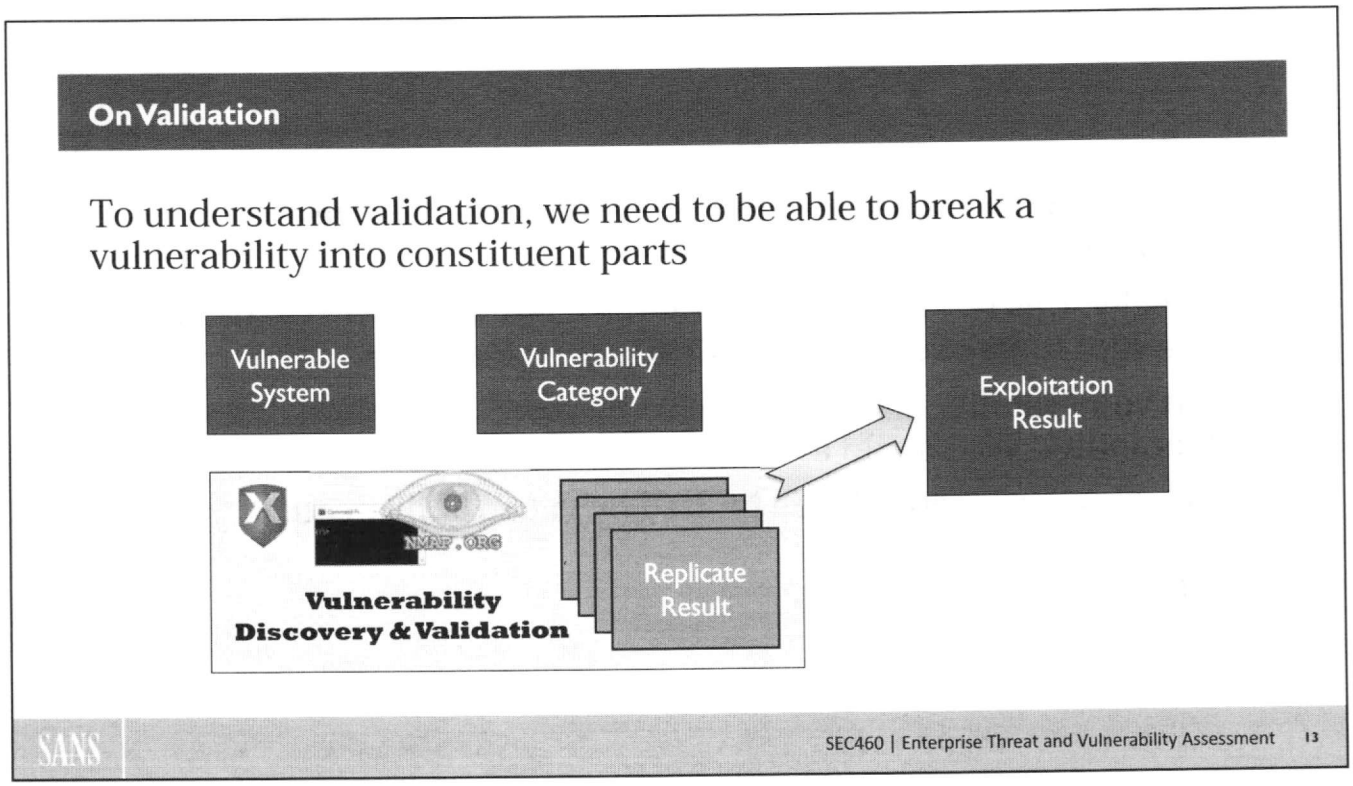
The Importance of Vulnerability Validation

Looking for a second opinion to verify the findings of your tools is a surefire way to begin cutting down the frequency of false positives and it comes with added benefits. Not all scanning tools discover and report the same vulnerabilities. Occasionally, the process of manual validation is an opportunity for deeper degrees of discovery. In addition to seeking second opinions, manually recreating assessment techniques to confirm the result of a tools output provides a further alternative. There is no better path to truly understanding a given vulnerability than dissection!



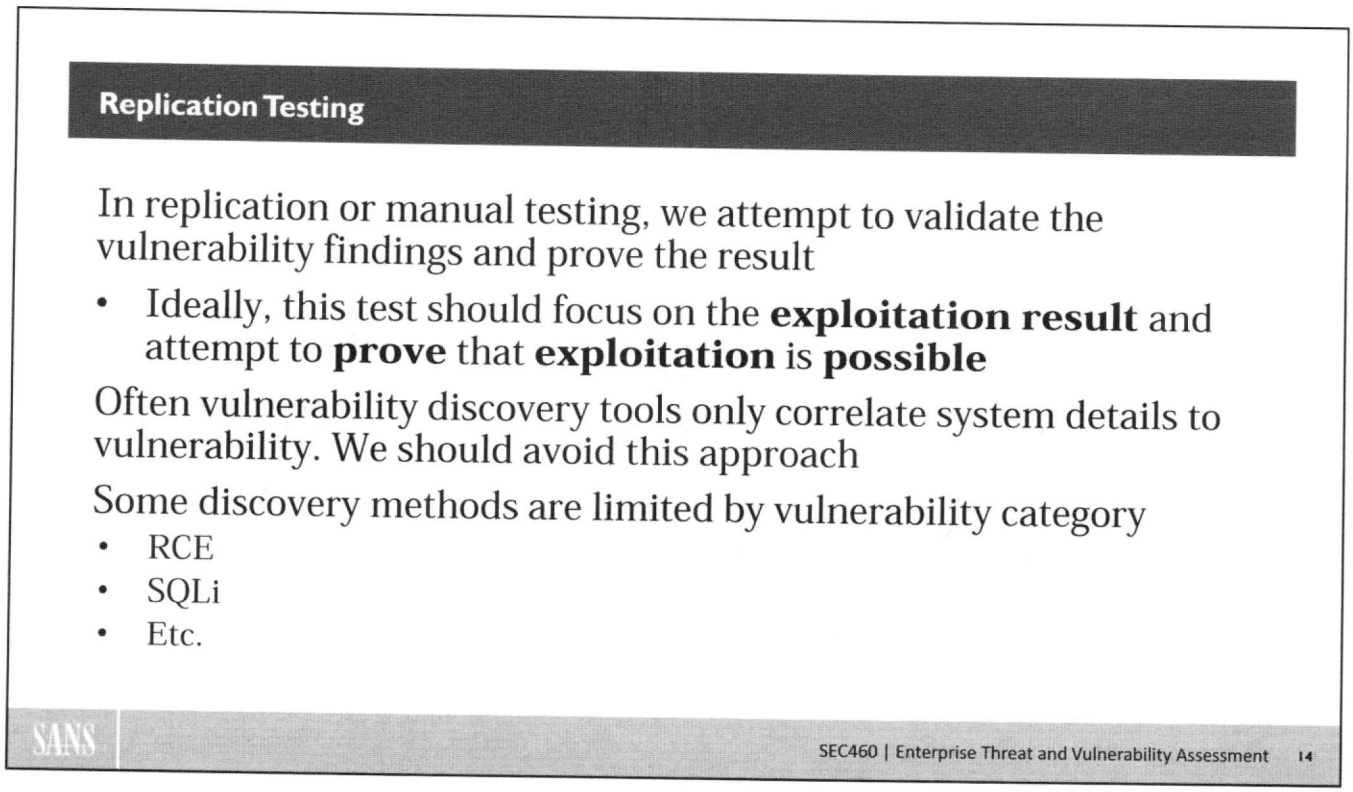
Course Roadmap: Manual Validation

Before we can truly work with the vulnerability data gathered from the last module's content we need to guarantee its efficacy. In this module, we begin with a structured approach to manual validation of potential vulnerability conditions.



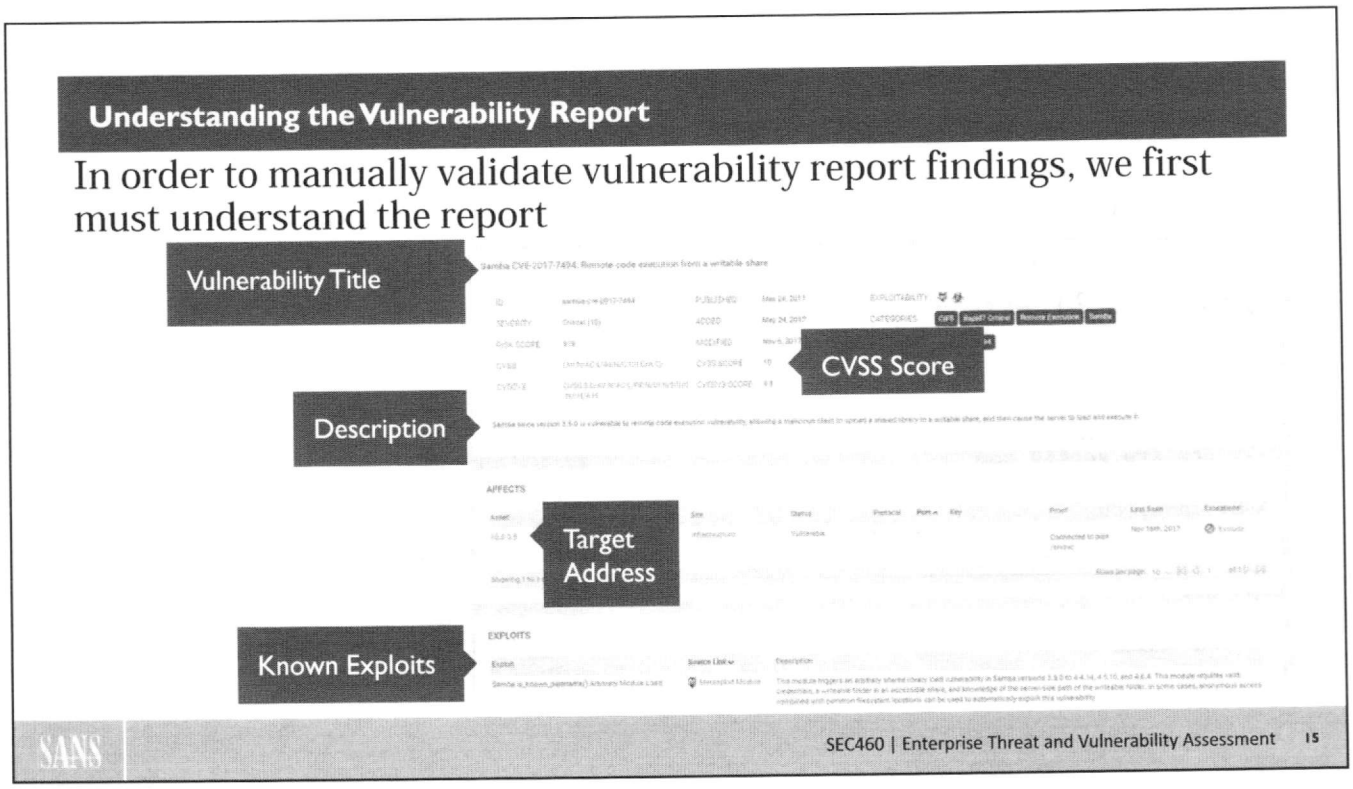
On Validation

Vulnerability validation begins with deconstruction. In this phase the focus is to break tool output into its elemental components, categorizing by **System, Vulnerability,** and **Impact.**



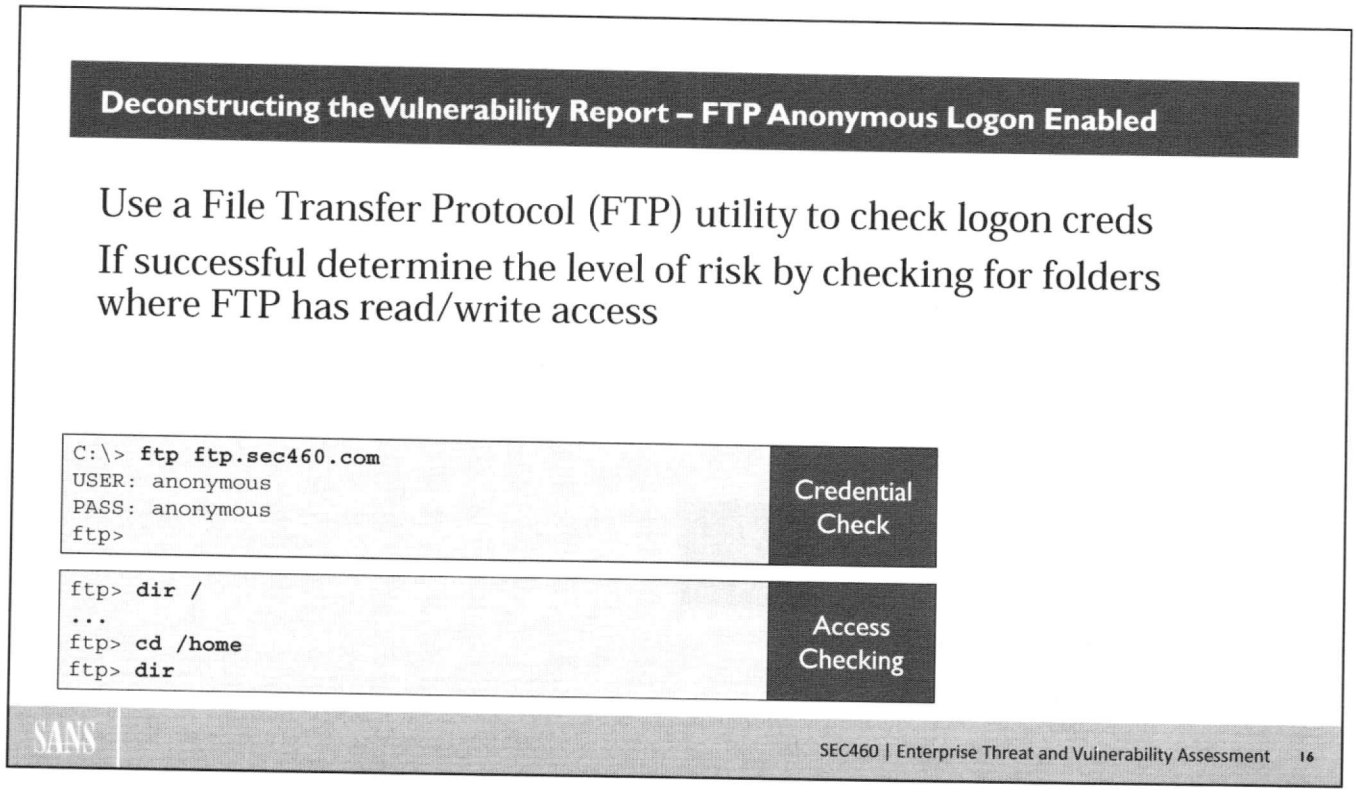
Replication Testing

In replication or manual testing, we attempt to validate the vulnerability findings and prove the result. Ideally, this test should focus on the **exploitation result** and attempt to **prove** that **exploitation** is **possible.** Often vulnerability discovery tools only correlate system details to vulnerability. We should avoid this approach.



Understanding the Vulnerability Report

In order to manually validate vulnerability report findings, we first must understand the report

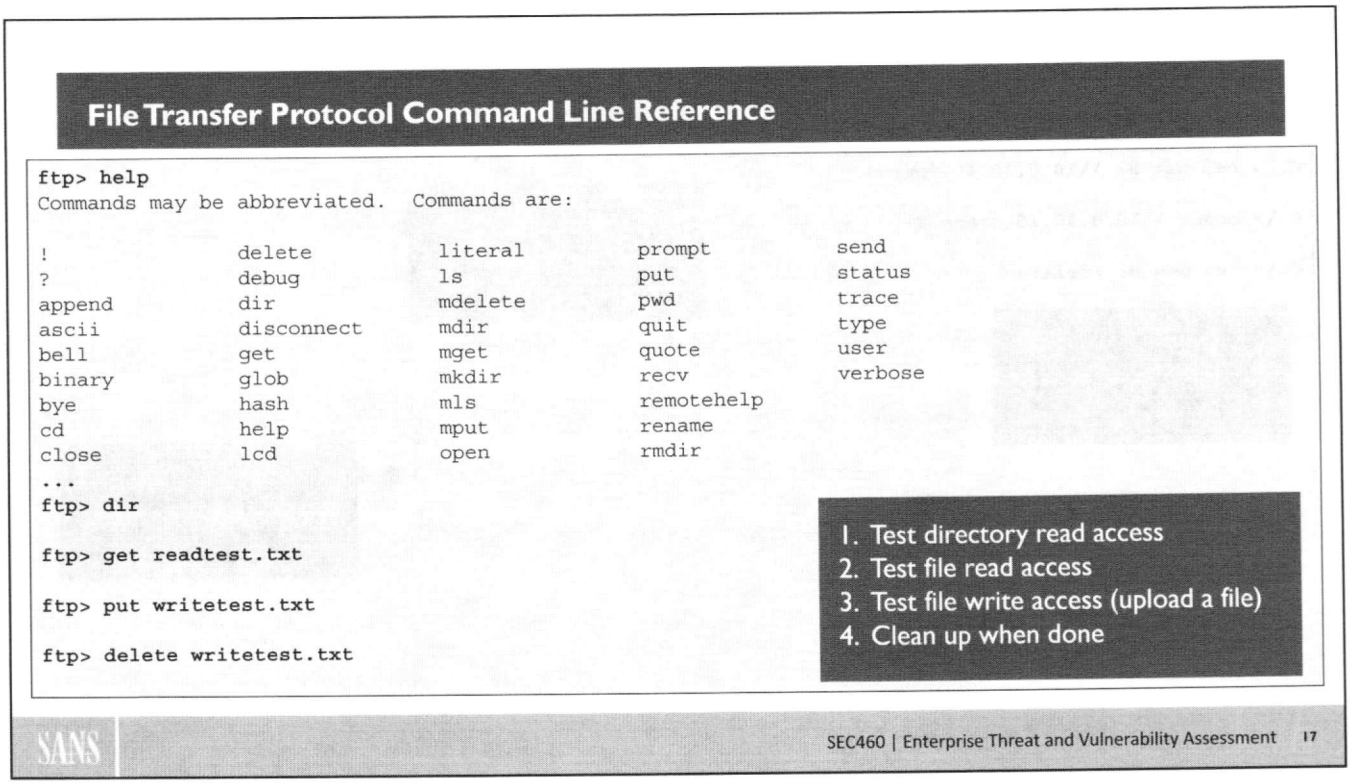


Deconstructing the Vulnerability Report – FTP Anonymous Logon Enabled

The File Transfer Protocol (FTP) is the standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead; it is technologically different.

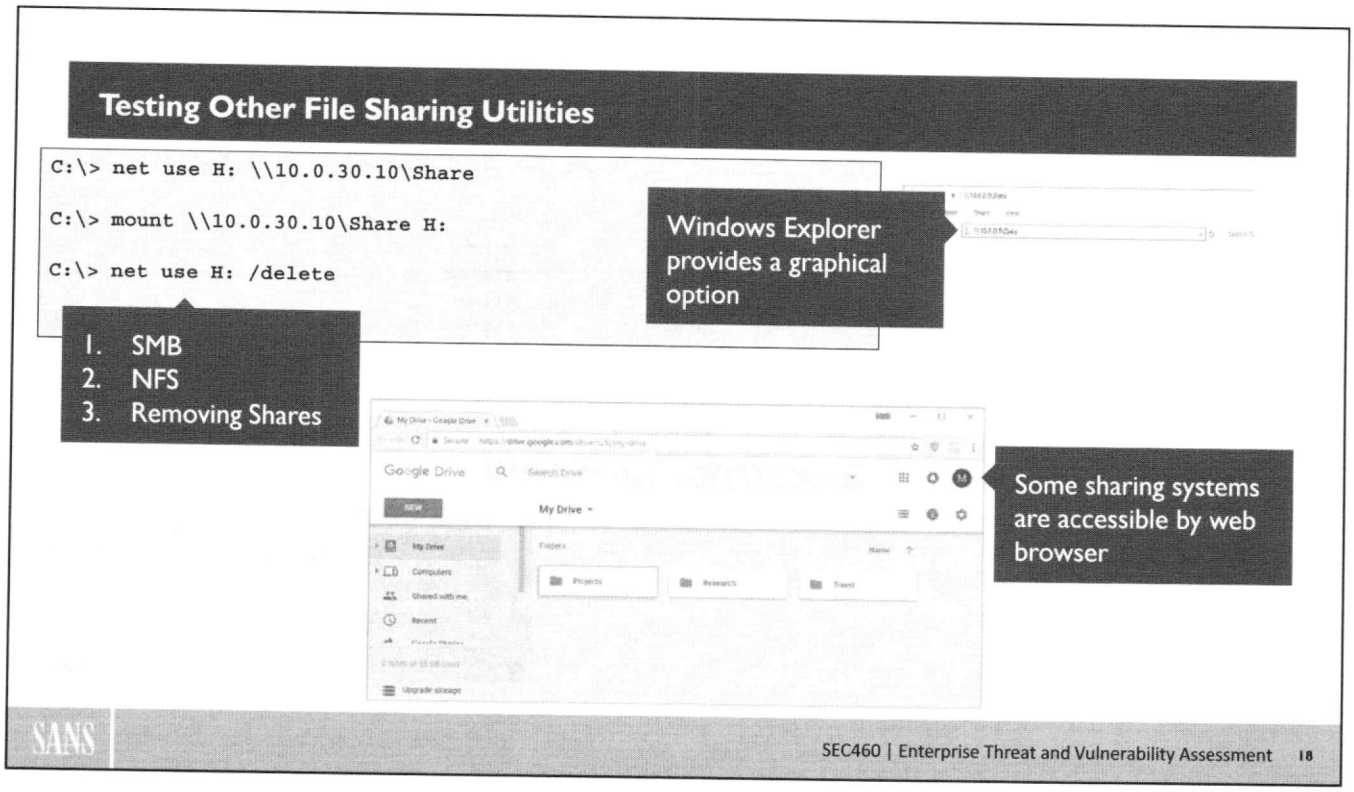
The <anonymousAuthentication> element specifies the settings for anonymous access. This form of authentication allows access to an FTP site without a user account on your server or domain and is most often used for public FTP sites. Anonymous users will typically log in by using a user name of ftp or anonymous, and most users will use their e-mail address as a password, although this is not required.

The configuration of systems allowing anonymous FTP should be checked carefully, as improperly configured FTP servers are frequently attacked. If you are not using this service, it is recommended to disable it or at least deny anonymous logins. Nessus rates this risk factor to be medium.



File Transfer Protocol Command Line Reference

The ftp command uses the File Transfer Protocol (FTP) to transfer files between the local host and a remote host or between two remote hosts. The FTP protocol allows data transfer between hosts that use dissimilar file systems. Although the protocol provides a high degree of flexibility in transferring data, it does not attempt to preserve file attributes (such as the protection mode or modification times of a file) that are specific to a particular file system. Moreover, the FTP protocol makes few assumptions about the overall structure of a file system and does not provide or allow such functions as recursively copying subdirectories.



Testing Other File Sharing Utilities

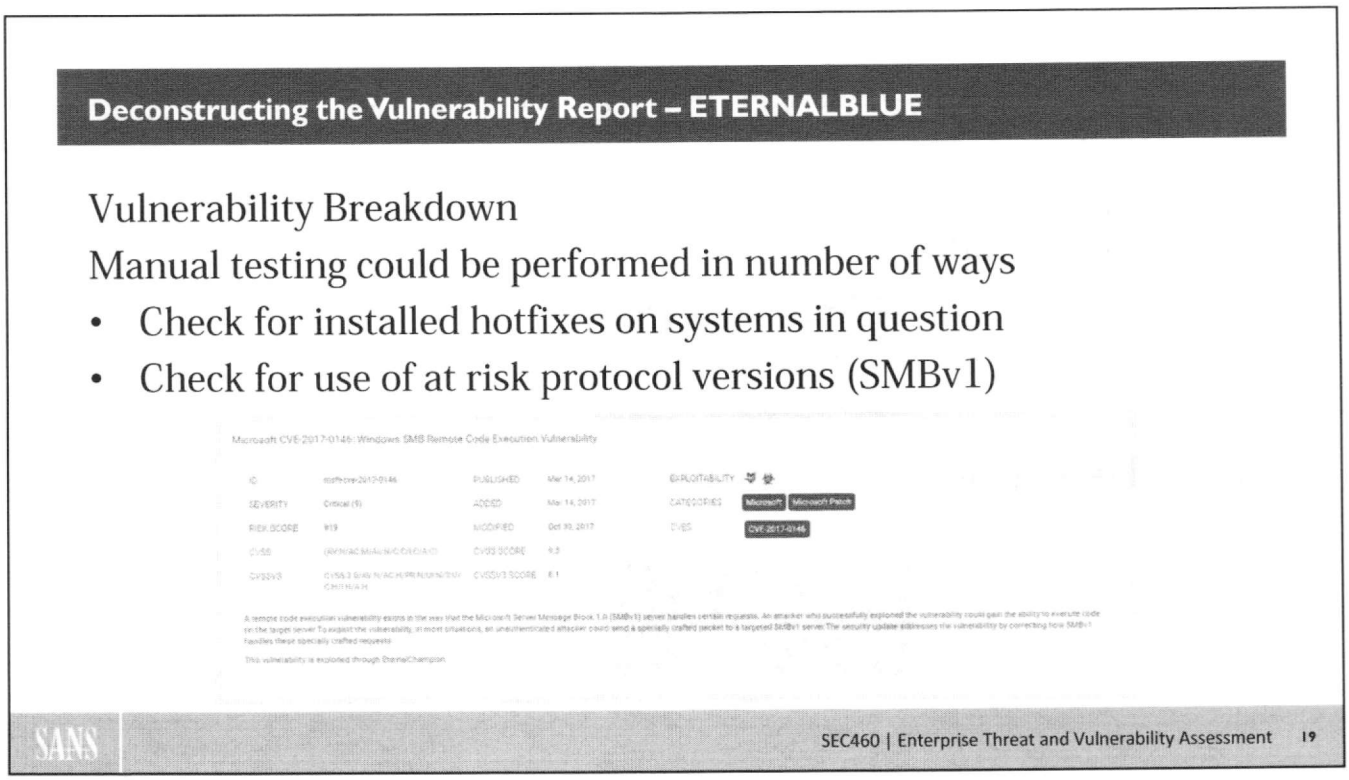
The general test processes are unchanged no matter what file sharing utility is in use. Namely, connect, read files, write files, delete files (cleaning up on the way out). Common utilities we have at our disposal include:

net use – The Windows net command supports mounting of both SMB (Microsoft) shares

mount – Network File System (NFS) shares can be mounted using the Services for Unix-based Applications Feature in Windows. Enabling this activates the native **mount** command

Windows Explorer – The Windows Explorer can be used to navigate network shares similarly to the net command

Web Browser – Many modern sharing systems are cloud resident and based around the user's web browser



Deconstructing the Vulnerability Report – ETERNALBLUE

For years, Microsoft has been recommending that the vulnerable SMBv1 protocol be disabled. Two devastating global ransomware outbreaks, WannaCry and Petya, spread quickly because of a vulnerability in one of the internet's most ancient networking protocols, Server Message Block version 1 (aka SMBv1).

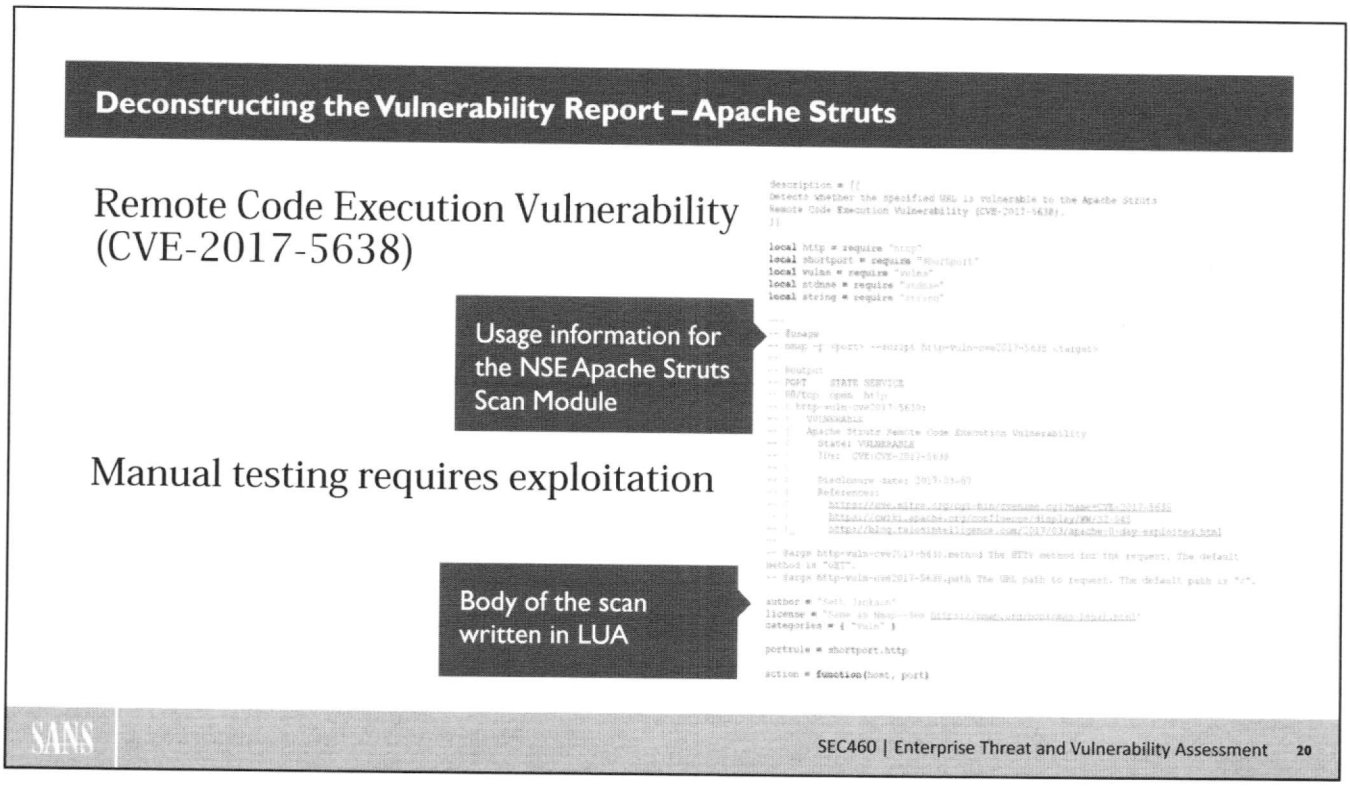
Starting this fall, with the public launch of the next major Windows 10 update — codenamed Redstone 3 -- Microsoft plans to disable SMBv1 in most versions of the Windows operating systems. SMBv1 is a three-decades-old file sharing protocol that Microsoft has continued to ship "enabled by default" with all Windows OS versions. Microsoft officially confirmed that it will not ship SMBv1 with the Fall Creators Update. This change will affect only users performing clean installs and will not be shipped as an update. This means Microsoft decision will not affect existing Windows installations, where SMBv1 might be part of a critical system.

The remote Windows host is affected by multiple vulnerabilities:

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.



Deconstructing the Vulnerability Report – Apache Struts

The Equifax incident came about after attackers exploited a web app vulnerability identified as CVE-2017-5638 targeting Apache Struts. This Apache Struts vulnerability was disclosed and patched in March 2017, and it was given the highest critical rating on the CVSS, because it is a remote code execution flaw that was being actively exploited in the wild. Apache classified the vulnerability in Struts' Jakarta Multipart parser as high risk, warning of remote code execution (RCE) attacks. The flaw that exists in Struts 2.3.5 to 2.3.31, and in 2.5 to 2.5.10 mishandles file upload functionality allowing an attacker to gain illicit access to the effected system.

Scanners like Nmap NSE use the Content-Type HTTP header to send a specially crafted packet in order to identify exploitable systems. For Example:

Content-Type: %{#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse'].addHeader('X-Test-Struts',3195*2088)}.multipart/form-data

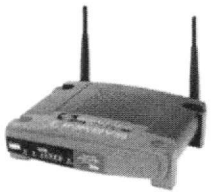
The request asks the webserver to multiply two numbers and can be used to request the web server to perform any other operation. In the example above the two numbers are 3195 and 5088. If the scanner received the correct answer from the webserver, i.e. 16256160 in this example it is concluded that the server is vulnerable, and the multiplication answer is in the HTTP response header.

Brainstorming Vulnerability Opportunities

Manual validation techniques can enable vulnerability discovery for targets that may not show up in scan results

Custom web appliances, internet of things devices, and SOHO routers are frequently vulnerable to authentication bypass attacks.

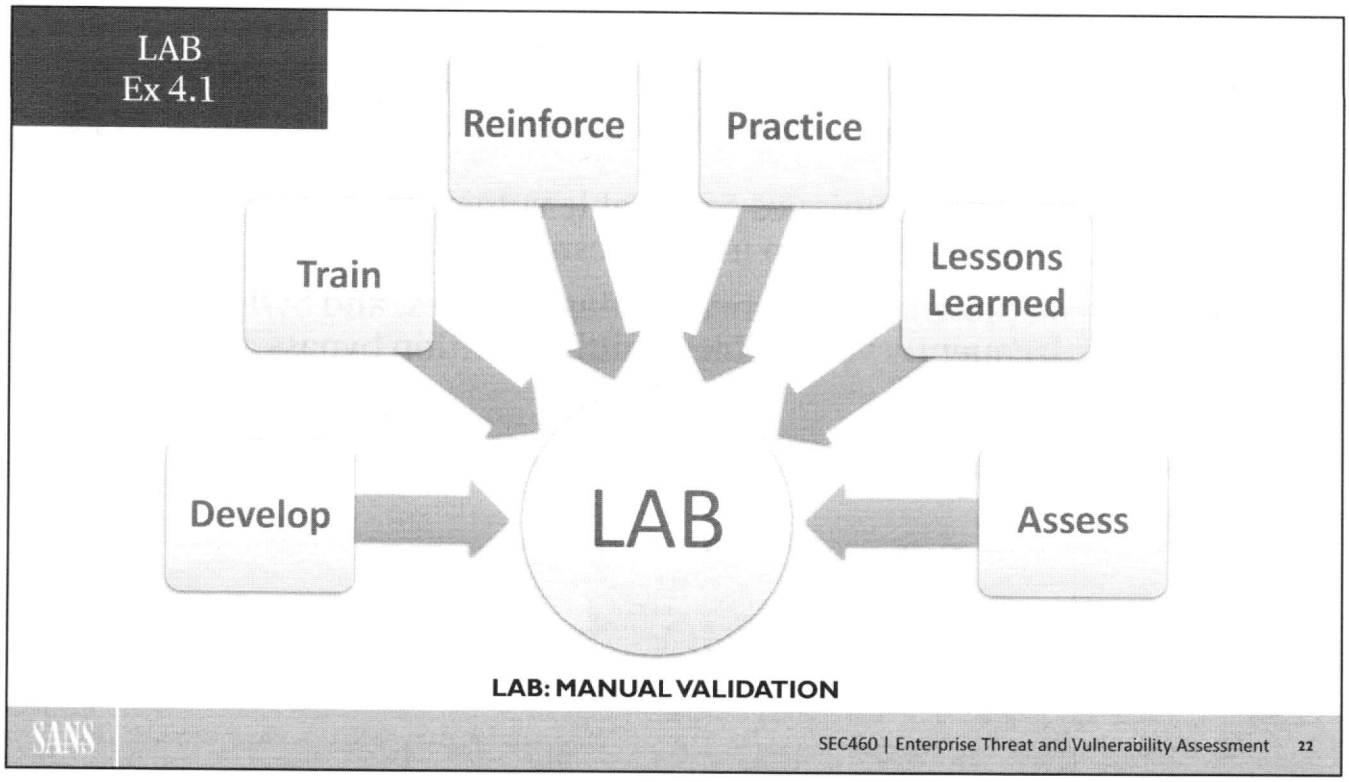
- Try guessing URLS
- Use the documentation to see if authentication checks are validated



Brainstorming Vulnerability Opportunities

An earlier ASUS firmware update addressed a number of vulnerabilities in 30 models of its popular RT routers. The flaws were privately disclosed by researchers at Baltimore consultancy Nightwatch Cybersecurity. The vulnerabilities were found in a native web interface on the devices and allow an attacker on the same local network to change router settings, steal Wi-Fi passwords or leak system information. ASUS addressed all but one of the disclosed vulnerabilities, an issue found in two JSONP endpoints that leak some information about the router without the need for the attacker to be logged in. "Fool a user that is on a network using an Asus router into visiting a malicious page; the JavaScript code on that page that can do the rest," Nightwatch's Yakov Shafranovich said.

The software used by many wireless IP cameras manufactured by Foscam Digital Technologies have a vulnerability that allows remote users to access their video streams and take snapshots without proper authentication. Foscam MJPEG cameras support as many as eight separate user accounts with different privileges: Administrator, Operator and Visitor. The user administration interface has eight user ID fields, but only one of them is configured by default with user name "admin" and privilege Administrator. The rest are blanked out and have the Visitor privilege assigned by default. If any of the eight user slots are left empty—with no username and password configured—it's possible to access the camera by simply hitting OK on the authentication prompt. This will give the remote user Visitor privileges and allow them to access video streams with or without audio, take snapshots and execute any CGI commands available to the Visitor access level.



LAB: Manual Validation

Please refer to the Wiki for Exercise 4.1.

Course Roadmap

- Day 1: Methodology, Planning, and Threat Modeling
- Day 2: Discovery
- Day 3: Enhanced Vulnerability Scanning and Automation
- **Day 4: Validation, Triage, and Mass Data Management**
- Day 5: Collaboration, Remediation, and Reporting
- Day 6: Capstone Exercise

SEC460.4

Vulnerability Validation
Manual Validation
- **Lab: Manual Validation**

Authenticated Scanning
- **Lab: Authenticated Scanning**

PowerShell WinRM Enhanced Engagements
- **Lab: PowerShell and WinRM Enhanced**

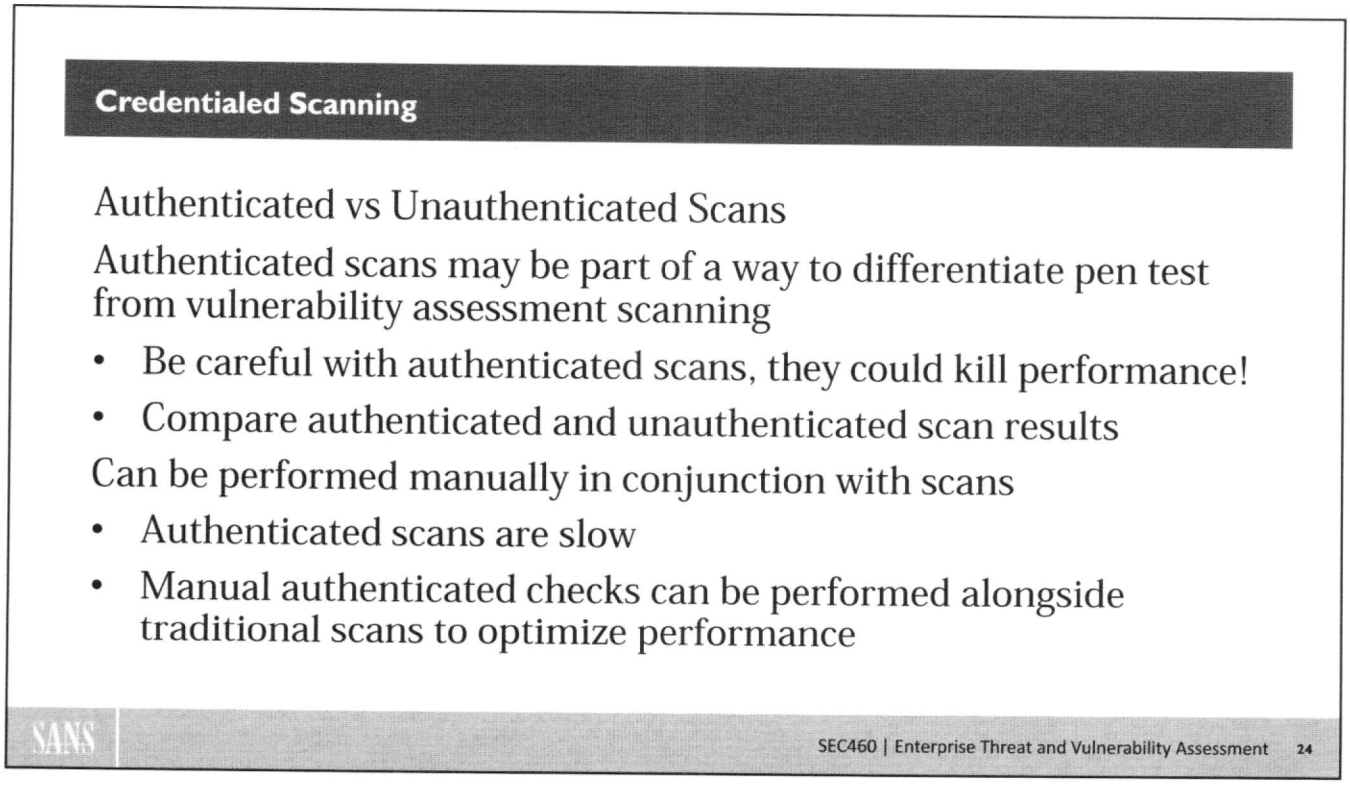
Data Management
Overcoming Data Management Pitfalls
- **Lab: Data Management Mayhem**

Enterprise Knowledge Management
- **Lab: Data Management and Collaboration**

Collaboration and Purple Teaming
- **Lab: Testing Egress Controls**

Triage
- **Lab: Triage**

This page intentionally left blank.



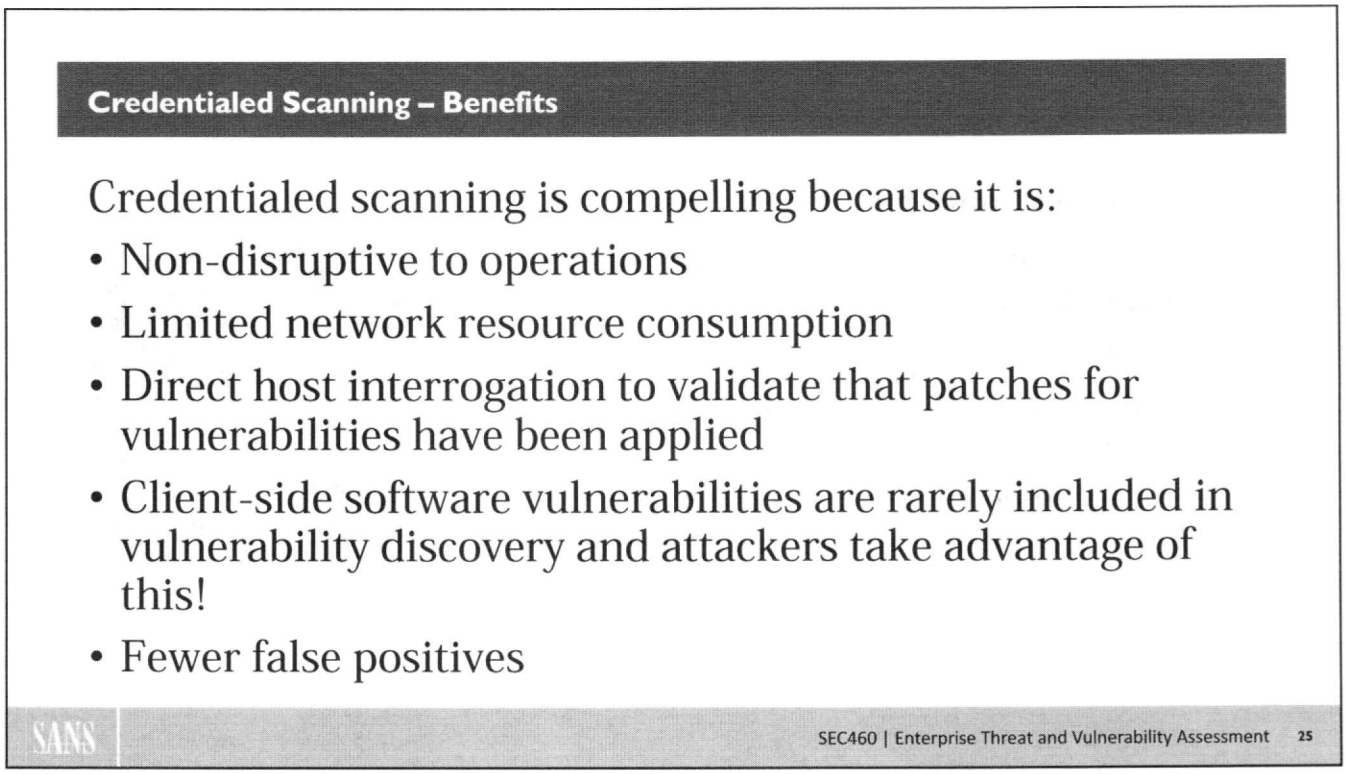
Credentialed Scanning

Credentialed scans are scans in which the scanning computer has an account on the computer being scanned that allows the scanner to do a more thorough check looking for problems that cannot be seen from the network. Examples of the sorts of checks that a credentialed scan can do includes checks to see if the system is running insecure versions of Adobe Acrobat or Java or if there are poor security permissions governing a service. Information Security and Policy (ISP) runs Nessus scanners that are capable of running these credentialed scans; however, without accounts on the local machines, we are unable to use this functionality. Scanning with credentials has opened a new frontier for security assessment. Here's an analogy: traditional vulnerability scanning is like a mechanic evaluating a car just by looking at the outside and listening to the motor run. It's useful but there is so much more information available by looking under the hood and plugging into the on-board diagnostics.

The notion that you cannot scan control system networks is an outdated excuse for maintaining security status quo. Can scanning cause fragile protocol stacks and services on many control system devices and applications to crash? Absolutely, we see it all the time. Can you scan intelligently, get valuable information, and not affect the production process? Yes.

Just like the mechanic plugging into the on-board diagnostics, credentialed scanning can give a much more accurate and thorough picture. Part of vulnerability scanning is identifying missing patches that leave a machine open to compromise. The netstat port scanning makes a good case here too. Ever try to identify open UDP ports? It can be a little tricky between the nature of the protocol itself and the rate-limiting most OSes impose on ICMP response messages. Credentialed scanning offers a much more accurate report of open ports.

Credentialed scanning, and more specifically, the Policy Compliance plugins, allow customized auditing of operating systems, applications, databases, file content — nearly all aspects of configuration that impacts security. Nessus offers baseline files for a variety of OSes, applications, standards, and policies.



Credentialed Scanning – Benefits

If a department had a compromise, I would do my best to help them figure out what happened and take measures to prevent it from happening again. A comprehensive assessment would next be performed to gain a better understanding of the security shortcomings and appropriate remediation measures. These types of assessments can be a daunting task for any security professional. It is important to scan for vulnerabilities such as missing patches or buffer overflows, but assessments need to go deeper. Attackers will do whatever it takes to get in! Often, that involves taking advantage of misconfigurations affecting legitimate authenticated users as opposed to zero-day exploits

Credentialed scanning with Nexpose provides a compelling option because it is:

- Non-disruptive to operations
- Limited network resource consumption
- Direct host interrogation to validate that patches for vulnerabilities have been applied
- Fewer false positives

Client-side software vulnerabilities are rarely included in vulnerability discovery and attackers take advantage of this! By looking at the software installed and its version, Nexpose will find client-side software vulnerabilities that are otherwise missed in a traditional network-based audit. While so-called "0-day" exploits get a lot of attention in the press, the dirty little secret of penetration testers (and most likely attackers) is that you don't need "0-day" exploits to compromise systems. Most successful penetration tests and breaches by attackers are accomplished by exploiting vulnerabilities for which the vendor has already released a patch, but the target organization has not yet applied. You may have a "world class" patch management system, but an attacker needs only one vulnerability on just one system in order to gain a foothold into your systems and network. You need a process of checks and balances to ensure that patches are being applied properly to all of your systems.

Credentialed Scanning – Pitfalls

Your scanner could be a target for exploitation!

- Scanners are often given elevated access permissions
- Attackers can impersonate or compromise security appliances to escalate privileges during a compromise

Many appliance vendors discount this risk and provide dangerous configuration procedures

Credentialed Scanning – Pitfalls

Many appliance vendors discount this risk and provide dangerous configuration procedures. This author impersonates security appliances during penetration tests on a regular basis. This exploitation generally results in Domain Admin level compromise.

Services are executables that are often run without user interaction and launched automatically when an operating system starts up, which is why services and service accounts are often overlooked as a unique security risk in a business network. Even when the security risks are understood, service account management can be a rather complex ordeal, considering that a simple password change may require several other changes to prevent outages. In addition, the use of domain accounts to run services is still a common practice because it has been easier to manage services across the domain instead of at individual servers, despite the security risks associated with this practice. Services store the user account and password information that they use in the registry, whether they use local or domain accounts. Therefore, when a single computer is compromised this information can be used to escalate privileges for the attacker if those services use domain accounts. If a service uses an administrative level domain account, such a scenario could pose a threat to the entire network.

As with the management of administrator and critical accounts, there are three fundamental issues that are key to establishing a successful plan that can increase the security of services in a midsize business environment. It is important that the following three issues be addressed during development phases and incorporated into security policy procedures:

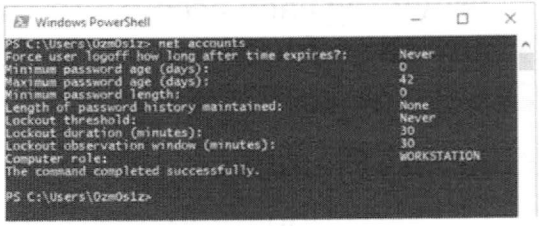
- Understanding and documenting the environment
- Using the principle of least privilege
- Using the principle of least service

One must strike a balance between time, effort and expense. On the DMZ, I think it prudent to marry unauthenticated external scanning with authenticated internal scanning. If the bandwidth of the vulnerability remediation teams is sufficient, why not do both un/authenticates scans internally as well?

Application vs. Network Credentials

What kinds of credentials may be needed or requested to facilitate the engagement?

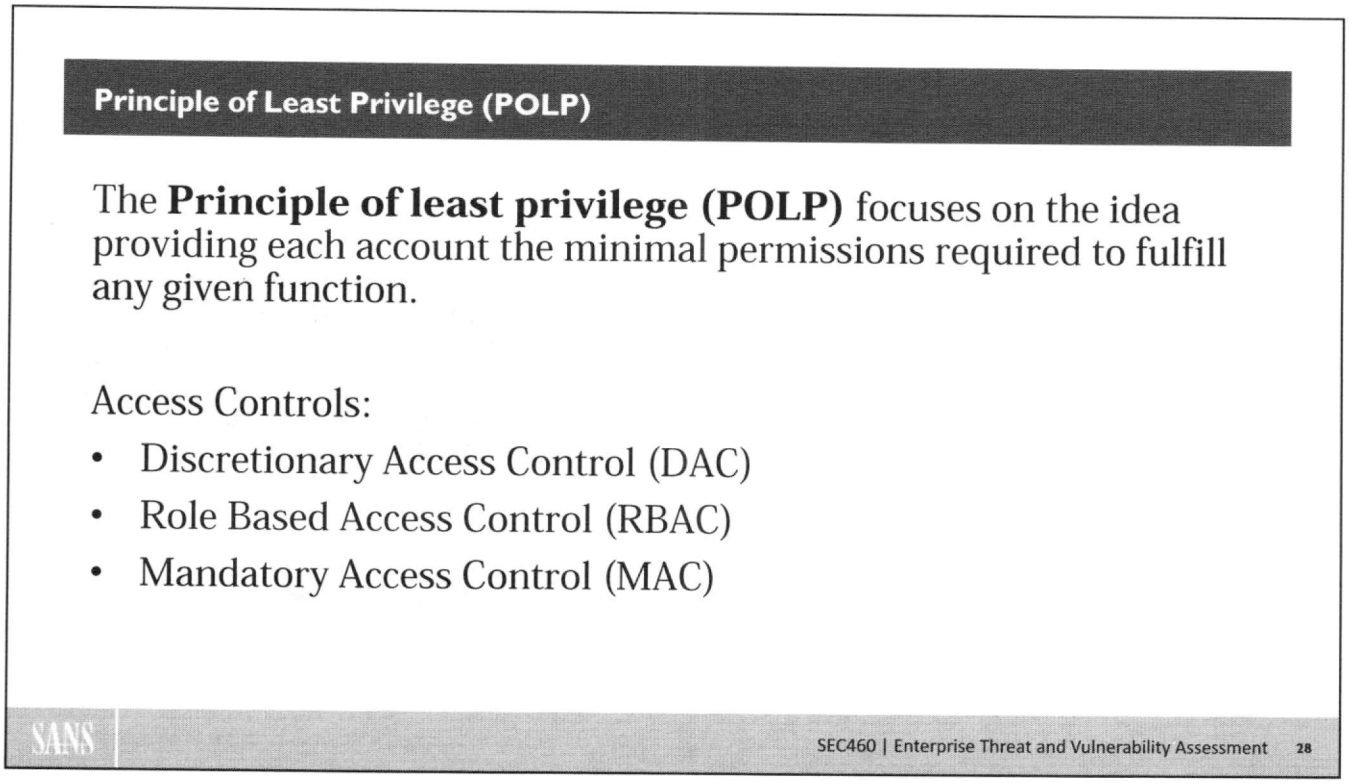
- Network Credentials
  - Local Administrator
  - Domain Service Account Credentials
- Application Credentials
  - Much like systems, applications have an extended exploitation foot print once accessed. For example:
    - Website behind the authentication portal
    - FTP Server after logon



SANS SEC460 | Enterprise Threat and Vulnerability Assessment 27

Application vs. Network Credentials

In many situations, greater value can be had by including security tests behind an authentication gateway. This can apply to a network from the domain user context or local administrator. A frequently overlooked opportunity for the same test potential lives in applications. Particularly, in applications that process information of a sensitive nature. These systems often protect this data (or even simple access) by using an authentication portal. What happens if one of the legitimate users is hacked? We should include tests in our scope that evaluate this potential source for risk.



Principle of Least Privilege (POLP)

The principle of least privilege (also known as the principle of minimal privilege or the principle of least authority) requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.

The principle means giving a user account only those privileges which are essential to perform its intended function. For example, a user account for the sole purpose of creating backups does not need to install software: hence, it has rights only to run backup and backup-related applications. Any other privileges, such as installing new software, are blocked. When applied to users, the terms least user access or least-privileged user account (LUA) are also used, referring to the concept that all user accounts at all times should run with as few privileges as possible, and also launch applications with as few privileges as possible.

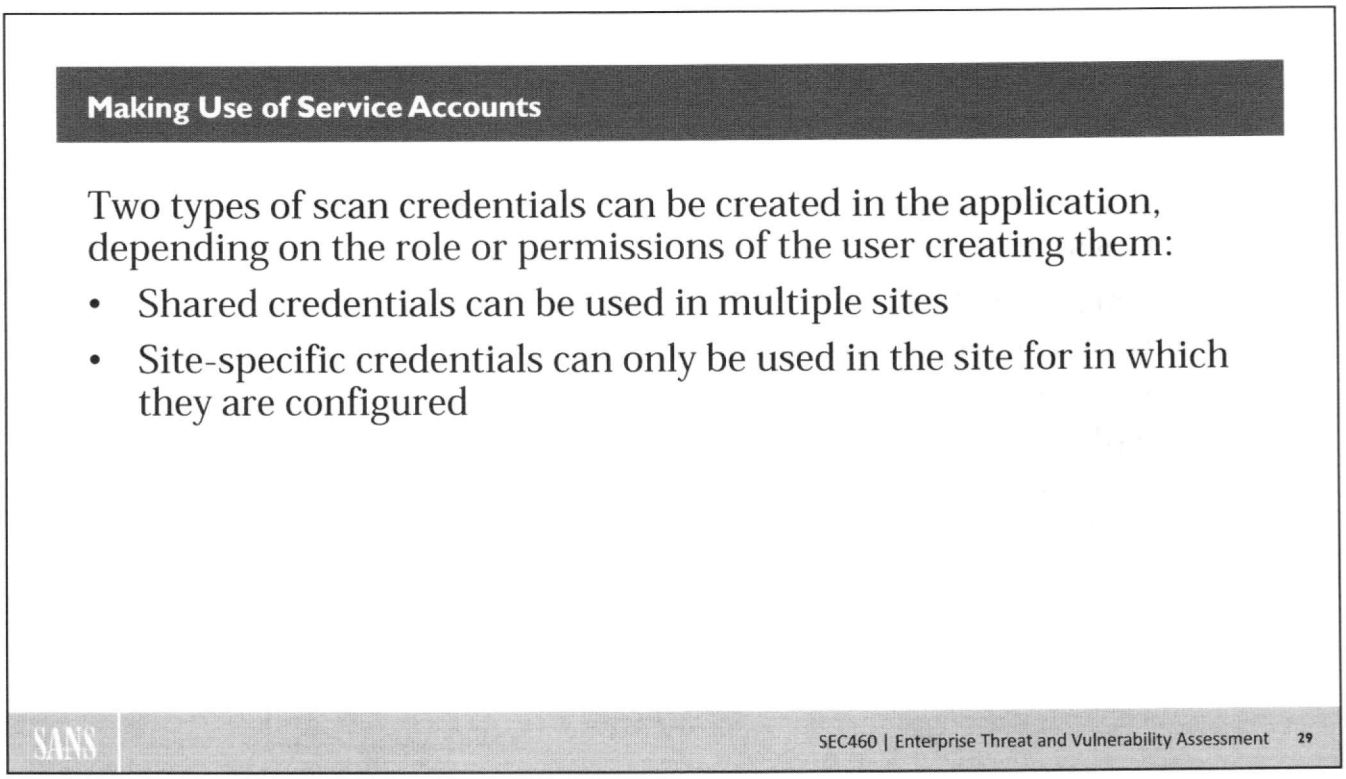
When code is limited in the system-wide actions it may perform, vulnerabilities in one application cannot be used to exploit the rest of the machine. For example, Microsoft states, "Running in standard user mode gives customers increased protection against inadvertent system-level damage caused by "shatter attacks" and malware, such as root kits, spyware, and undetectable viruses".

Discretionary Access Control (DAC) – a means of restricting access to objects based on the identity of subjects and/or groups to which they belong

Role Based Access Control (RBAC) – an approach to restricting system access to authorized users

Mandatory Access Control (MAC) – a type of access control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target

RBAC can be used as a foundation to implement both DAC and MAC.

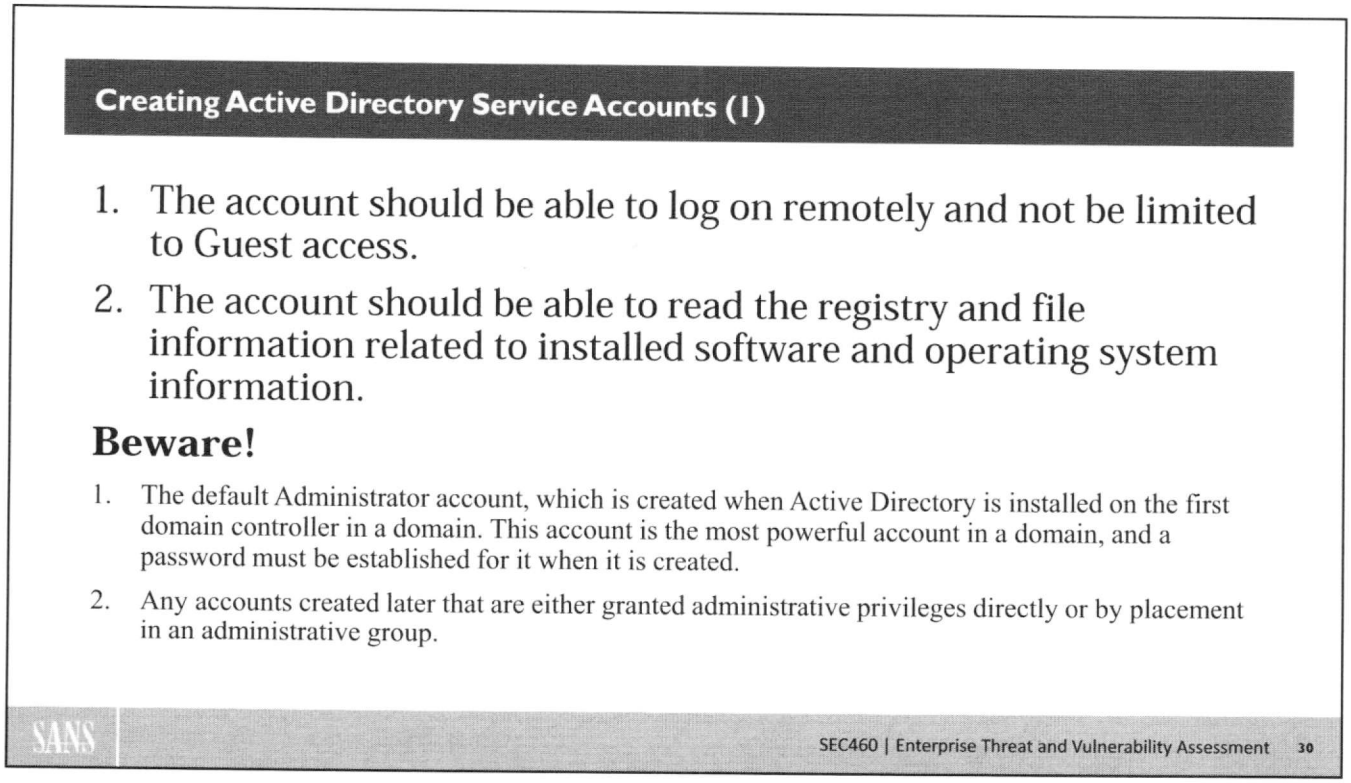


Making Use of Service Accounts

Scanning with credentials allows you to gather information about your network and assets that you could not otherwise access. You can inspect assets for a wider range of vulnerabilities or security policy violations. Additionally, authenticated scans can check for software applications and packages and verify patches. When you scan a site with credentials, target assets in that site authenticate the Scan Engine as they would an authorized user.

You can create and manage scan credentials that can be used on multiple sites. Using shared credentials can save time if you need to perform authenticated scans on a high number of assets in multiple sites that require the same credentials. It is also helpful if these credentials change often. For example, your organization's security policy may require a set of credentials to change every 90 days. You can edit that set in one place every 90 days and apply the changes to every site where those credentials are used. This eliminates the need to change the credentials in every site every 90 days.

To configure shared credentials, you must have a Global Administrator role or a custom role with Manage Site permissions.



Creating Active Directory Service Accounts (1)
Abuse of privileged accounts through compromised credentials is proving to be an increasingly popular tactic for hackers and malicious insiders. When it comes to vulnerability scanning, credentialed scans are more effective because they have a greater reach into an organization's network.

When scanning Windows assets, it is recommended that you use domain or local administrator accounts in order to get the most accurate assessment. Administrator accounts have the right level of access, including registry permissions, file-system permissions, and either the ability to connect remotely using Common Internet File System (CIFS) or Windows Management Instrumentation (WMI) read permissions. In general, the higher the level of permissions for the account used for scanning, the more exhaustive the results will be. If you do not have access, or want to limit the use of domain or local administrator accounts within the application, then you can use an account that has the following permissions:

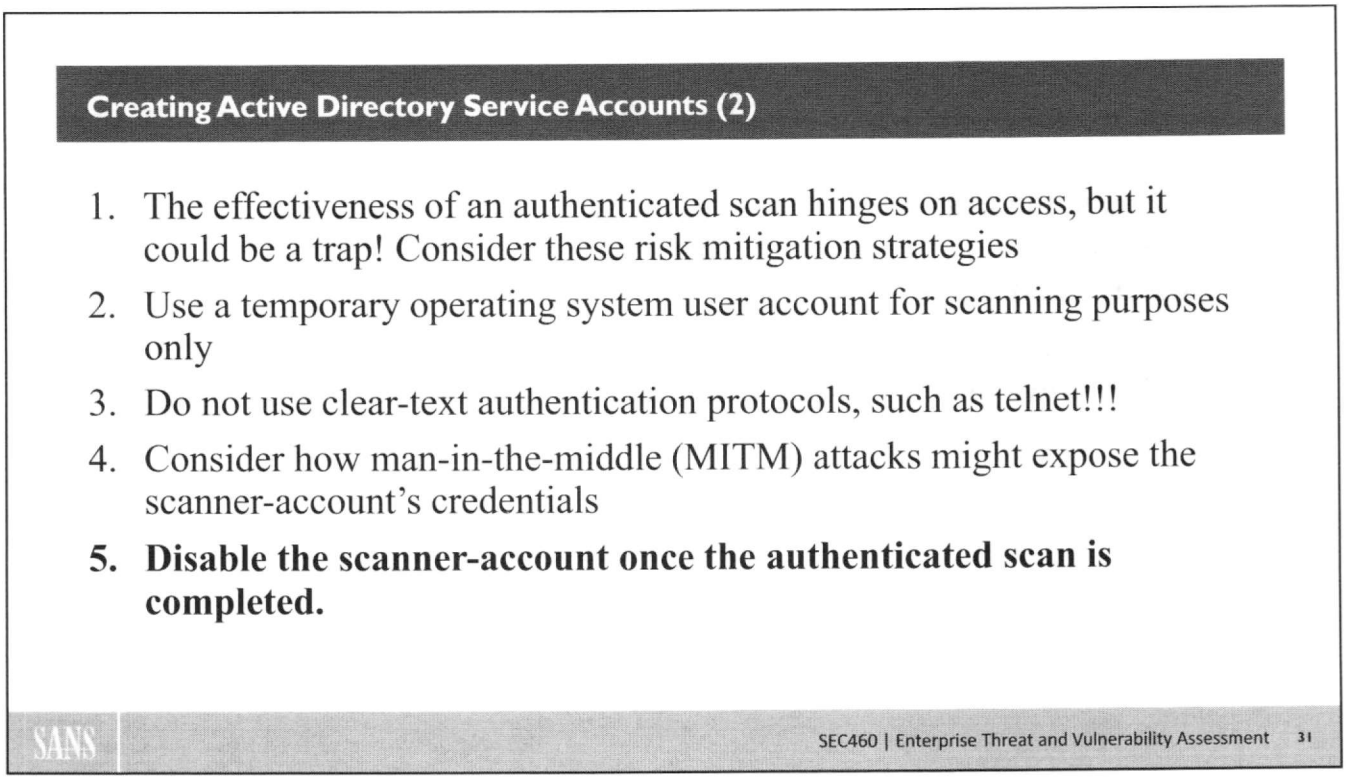
1. The account should be able to log on remotely and not be limited to Guest access.
2. The account should be able to read the registry and file information related to installed software and operating system information.

The administrative level accounts in an Active Directory network include:

1. The default Administrator account, which is created when Active Directory is installed on the first domain controller in a domain. This account is the most powerful account in a domain, and a password must be established for it when it is created.
2. Any accounts created later that are either granted administrative privileges directly or by placement in an administrative group.

There are two different types of administrative privileges in a Windows Server 2003 Active Directory environment: service administrators and data administrators.

1. Service administrator accounts govern the maintenance and delivery of directory services, which includes the management of domain controllers and Active Directory.
2. Data administrator accounts govern the data that is stored in the directory service, on domain member servers, and workstations in the domain.

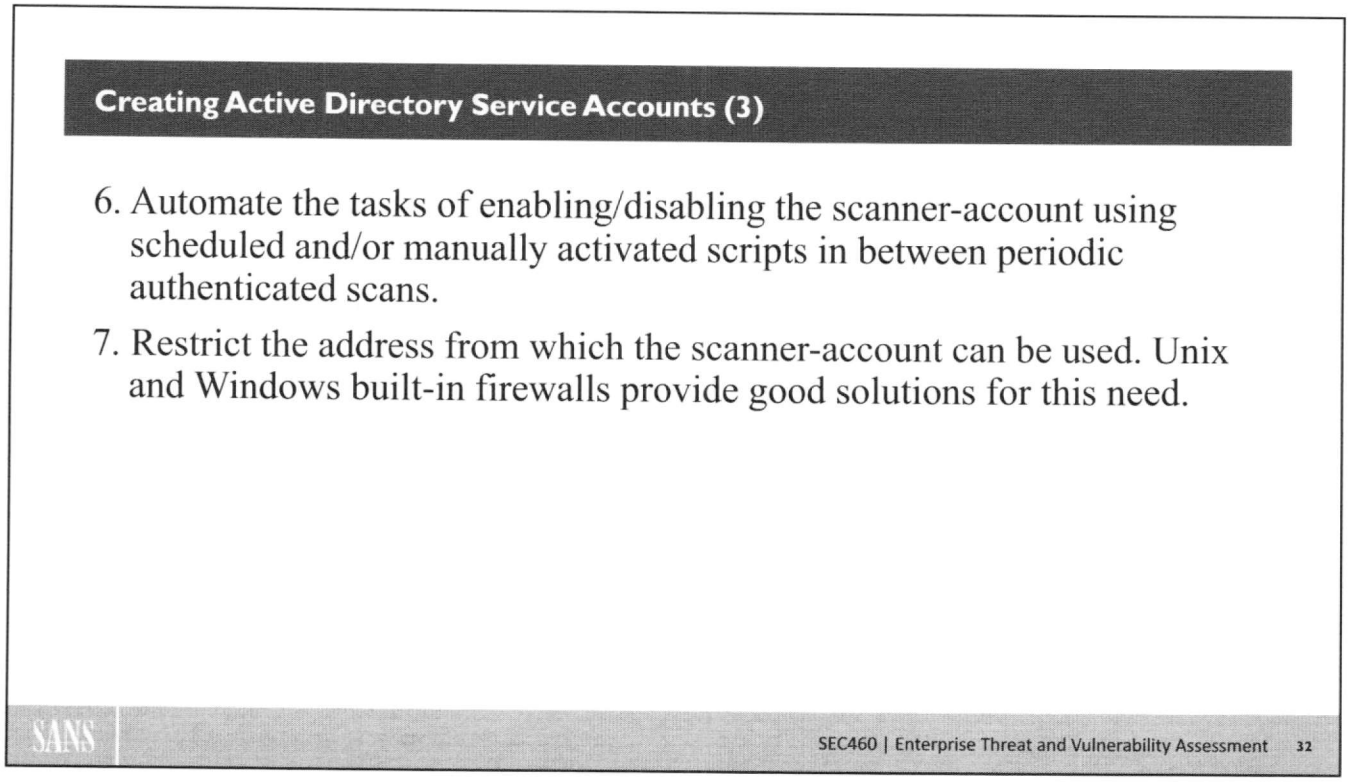


Creating Active Directory Service Accounts (2)

Authenticated scan is an essential tool to obtain accurate vulnerability information on covered devices by authenticating to scanned devices to obtain detailed and accurate information about the operating system and installed software, including configuration issues and missing security patches. The additional details provided by an authenticated scan allows resource proprietors and resource custodians to better mitigate risks on covered data and reduce the likelihood of successful attacks against covered devices. To ensure timely discovery of vulnerabilities on covered devices, **authenticated scans should be executed at least once a month on covered devices**, which include sysadmin and core devices.

The effectiveness of an authenticated scan often hinges on access to administrative credentials on covered devices. This requires adequate planning to addresses risks associated with handling and storing administrative credentials. The following practices should be carefully considered when implementing an authenticated scan program to mitigate such risks:

1. Rather than using an existing user account, create a temporary operating system user account dedicated to executing authenticated scans to allow for more granular control. The temporary user account, which we will call scanner-account, must have administrative access to all covered devices to be scanned. For Unix based devices, scanner-account may need to be setup separately on each device to be scanned.
2. Confirm that the scanner-account is able to authenticate to all the covered devices as expected.
3. Do not use clear-text authentication protocols, such as telnet.
4. Consider man-on-the middle attacks that might expose the scanner-account's credentials. For instance, an attacker might set up an internal SSH server to which the scanner will authenticate and give up the username and password.
5. **Disable the scanner-account once the authenticated scan is completed.** Keeping the scanner-account enabled only for the duration of the periodic authenticated scan will reduce the likelihood that scanner-account will be exploited for malicious purposes.



Creating Active Directory Service Accounts (3)

6. Automate the tasks of enabling/disabling the scanner-account via scheduled scripts in between periodic authenticated scans.
7. Restrict the host/IP address from which the scanner-account can be used. For example, when scanning Unix devices, only allow the scanner-account to login from the scanner's IP address. (Scanner being the server running the vulnerability scanner software.)

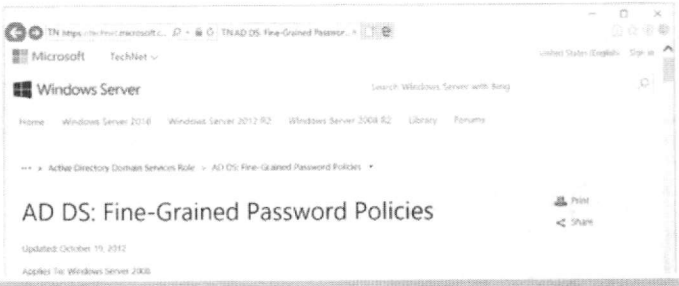
In Nexpose, configure SSH keys for authentication:

On every target system to be scanned using local security checks, create a new user account dedicated to Nessus. This user account must have exactly the same name on all systems. For this document, we will call the user "Nexpose", but you can use any name. Once the account is created for the user, make sure that the account has no valid password set. On Linux systems, new user accounts are locked by default, unless an initial password was explicitly set. If you are using an account where a password had been set, use the "passwd –l" command to lock the account. You must also create the directory under this new account's home directory to hold the public key. For this exercise, the directory will be /nexpose//dir// An example for Linux systems is provided below:

Securing Active Directory Service Accounts (4)

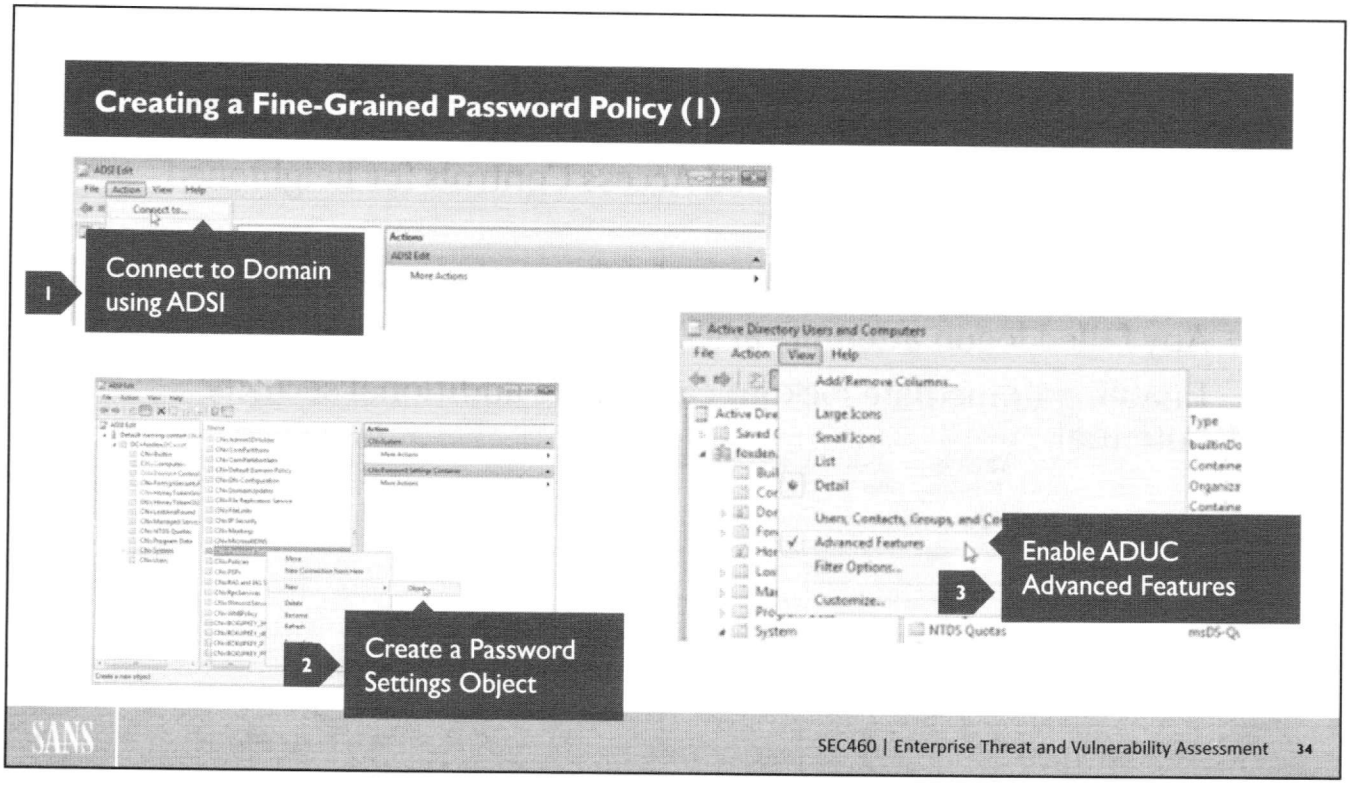
(Optional) Setup Fine-Grained Access Controls for heightened security/control

- The scanning system will never fat finger the password
- Any failed logon attempts are therefore NOT normal
- Enabling immediate lockout can enable additional security potential



Creating Active Directory Service Accounts (4)

The premise of this detection mechanism is to create a fake user account in Active Directory with a lockout policy of one. The next step is to seed the network with files containing the associated username with an incorrect password. This file should be permissioned such that a nominal user cannot access the file to gain this authentication information. This means that when a logon attempt to this account does occur it must by its very nature be malicious. In order to detect these logons, we simply need to monitor the associated account to see if it becomes locked and retrieve the associated event logs to obtain source information. First, we begin by creating our honeytoken account under active directory. The name for this account should be something innocuous that appears to be typical of your organization's environment. For this demonstration our account name will be HoneyAccount.



Creating a Fine-Grained Password Policy (1)

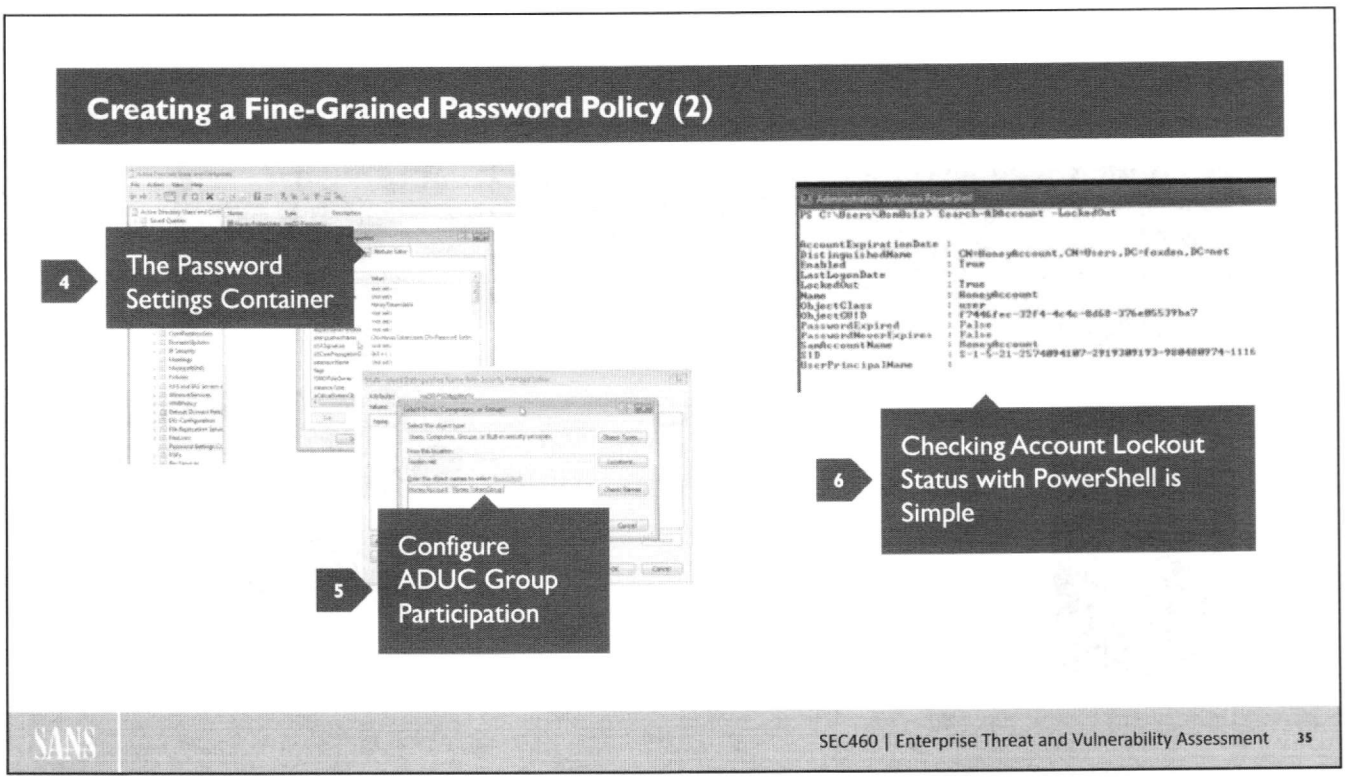
From here, the account lockout policy is typically configured by setting up the Group Policy Object (GPO) located at: \Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy. However, a limitation in Windows Active Directory is the inability to create group or user specific password policies without allocating them an entire domain. To get around this, Microsoft implemented AD DS Fine-Grained Password and Account Lockout Policy (Microsoft, 2012). These changes allow for the direct creation of a Password Settings Object (PSO) in order to explicitly assign account settings within a given domain. Note that these settings are not visible under net accounts. To create a PSO we use the Active Directory Services Interfaces (ADSI) Editor. The appropriate Microsoft Management Console (MMC) snap-in or a Windows Server can be used to access this toolkit.

From within the ADSI Editor connect to the appropriate domain as shown above.

Next, we navigate through CN=DomainName -> CN=System

Now, we right click on CN=Password Settings Container -> New -> Object. And follow the wizard. We will be using Microsoft default settings with the exception of Maximum Password Age and Lockout Threshold.

The final step is to assign our newly created PSO to a specific user/group and monitor that group with PowerShell. To do this we need to enable advanced features under ADUC.



Creating a Fine-Grained Password Policy (2)

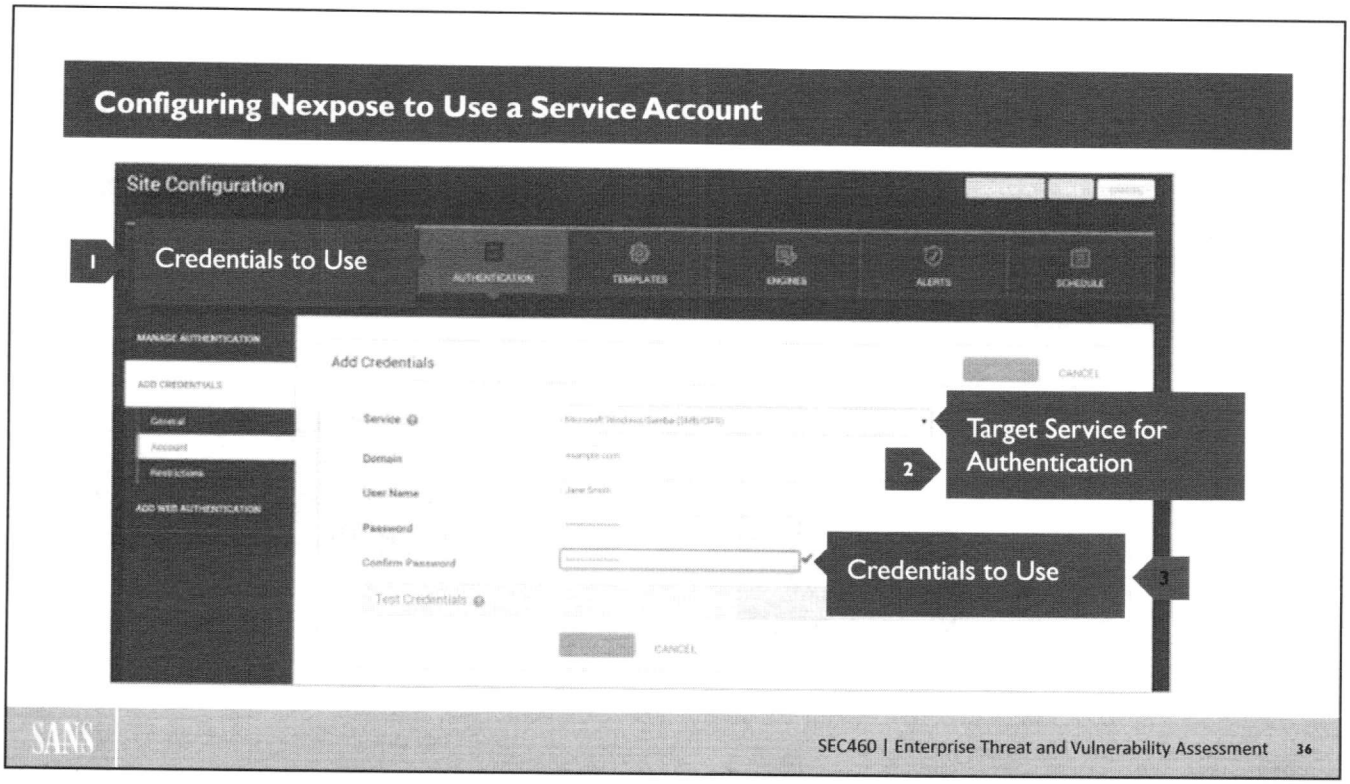
Next, we have to navigate to our PSO. It can be found under Domain -> System -> Password Settings Container.

We now double click on the PSO and look under the Attribute Editor tab, then navigate to: msDS-PSOAppliesTo and set the variable to the honeytoken account/group.

The account lockout policy has been set. The only objective remaining is to monitor the account's lockout status regularly to detect adversary activity. As is often the case with PowerShell, a built-in function takes what could have been an arduous task and makes it exceedingly easy:

PS C:\> **Search-ADAccount –LockedOut**

As you can see from the figure above Search-ADAccount –LockedOut grants network security personnel an easy means to determine when an adversary has attempted to gain access with a honey account.



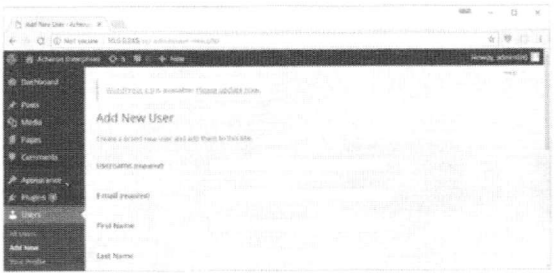
Configuring Nexpose to Use a Service Accounts

https://help.rapid7.com/nexpose/en-us/Files/Site_specfic_credentials.html

Creating Application Testing Accounts

May need full access in order to test full set of features, use caution

- If the scanner stumbles upon a vulnerability and retrieves PCI compliance required data, what then?



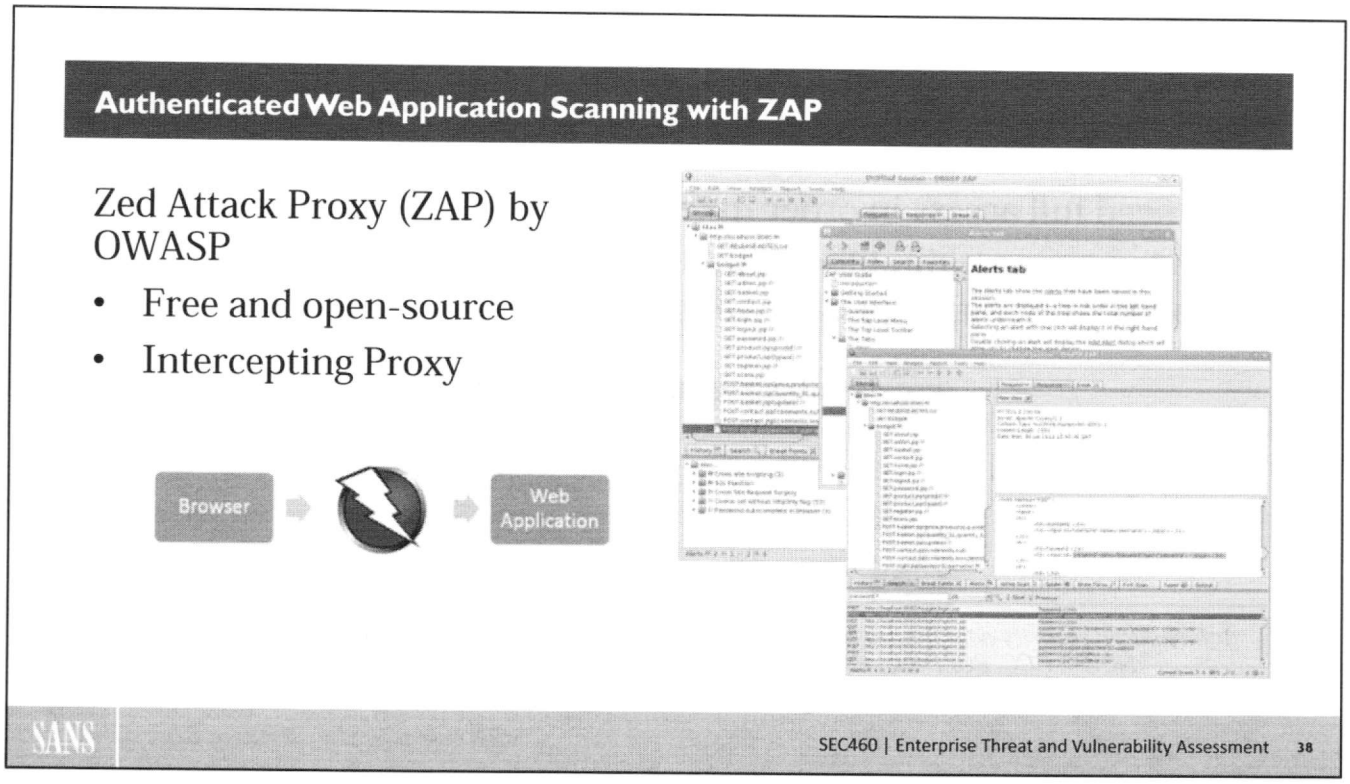
Information security compliance regulations and guidelines (FDIC, FFIEC, GLBA, HIPAA, HITECH, NCUA, OCC, PCI DSS, etc.) require an organization to conduct independent testing

Creating Application Testing Accounts

Web based Payroll systems, Shopping Malls, Banking, Stock Trade application are not only being used by organizations but are also being sold as products today. This means that online applications have gained the trust of customers and users regarding their vital feature named as SECURITY. No doubt, the security factor is of primary value for desktop applications too. However, when we talk about the web, the importance of security increases exponentially. If an online system cannot protect the transaction data, no one will ever think of using it. Security is neither a word in search of its definition yet, nor is it a subtle concept.

Information security compliance regulations and guidelines (FDIC, FFIEC, GLBA, HIPAA, HITECH, NCUA, OCC, PCI DSS, etc.) require an organization to conduct independent testing of the information security program to identify vulnerabilities that could result in unauthorized disclosure, misuse, alteration, or destruction of confidential information, including Non-Public Personal Information (NPPI). In order to ensure the security of an organization's external network, best practices state that each organization should perform an external penetration test in addition to regular security assessments. This includes any web-facing application that is exposed to risk.

Maintaining payment security is required for all entities that store, process or transmit cardholder data. Guidance for maintaining payment security is provided in PCI security standards. These set the technical and operational requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.



Authenticated Web Application Scanning with ZAP

"At its core, ZAP is what is known as an "intercepting proxy." It stands between the tester's browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination. In essence, ZAP can be used as a "man in the middle," but also can be used as a stand-alone application, and as a daemon process. "

The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers*. It can help you automatically find security vulnerabilities in your web applications while you are developing and testing your applications. It's also a great tool for experienced pen testers to use for manual security testing.

Since ZAP is set up to act as a proxy between your browser and the web application, using SSL (HTTPS) will cause the certificate validation to fail and the connection to be terminated. This is because ZAP encrypts, and decrypts traffic sent to the web application using the original web application certificate. This is done so that ZAP can access the plain text in the requests and responses. To prevent this failure from happening, ZAP automatically creates an SSL certificate for each host you access, signed by ZAP's own Certificate Authority (CA) certificate. To have your browser trust these SSL certificates, you need to first import and trust the ZAP Root CA certificate. Once it is trusted, the other ZAP SSL certificates signed by it will be trusted as well.

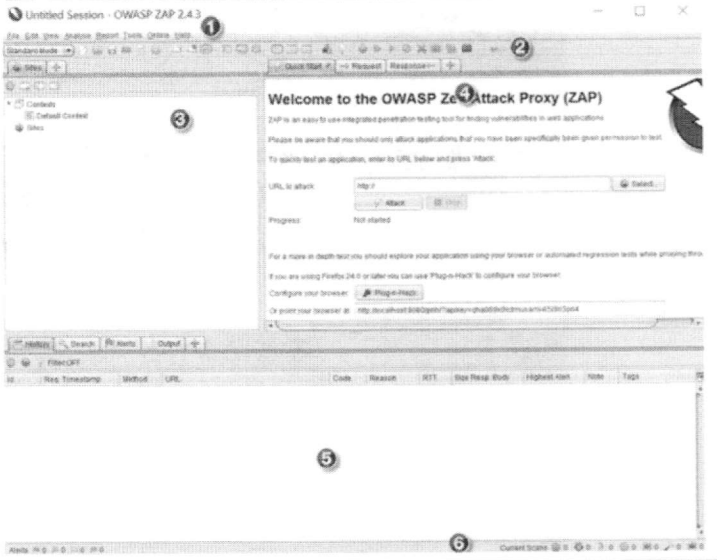
The passive scanning and automated attack functionality is a great way to begin a vulnerability assessment of your web application, but it has some limitations. Among these are:

- Any pages protected by a login page are not discoverable during a passive scan because, unless you've configured ZAP's authentication functionality, ZAP will not handle the required authentication.
- Any pages that are not findable with ZAP's default spider are not testable during a passive scan. ZAP does provide additional options for discovery and coverage outside of passive scanning.
- You don't have a lot of control over the sequence of exploration in a passive scan or the types of attacks carried out in an automated attack. ZAP does provide many additional options for exploration and attacks outside of passive scanning.

The Zed Attack Proxy

The ZAP UI is composed of the following elements:

1. **Menu Bar** – Provides access to many of the automated and manual tools.
2. **Toolbar** – Includes buttons which provide easy access to most commonly used features.
3. **Tree Window** – Displays the Sites tree and the Scripts tree.
4. **Workspace Window** – Displays requests, responses, and scripts and allows you to edit them.
5. **Information Window** – Displays details of the automated and manual tools.
6. **Footer** – Displays a summary of the alerts found and the status of the main automated tools.



The Zed Attack Proxy - Authenticated Web Application Scanning with ZAP

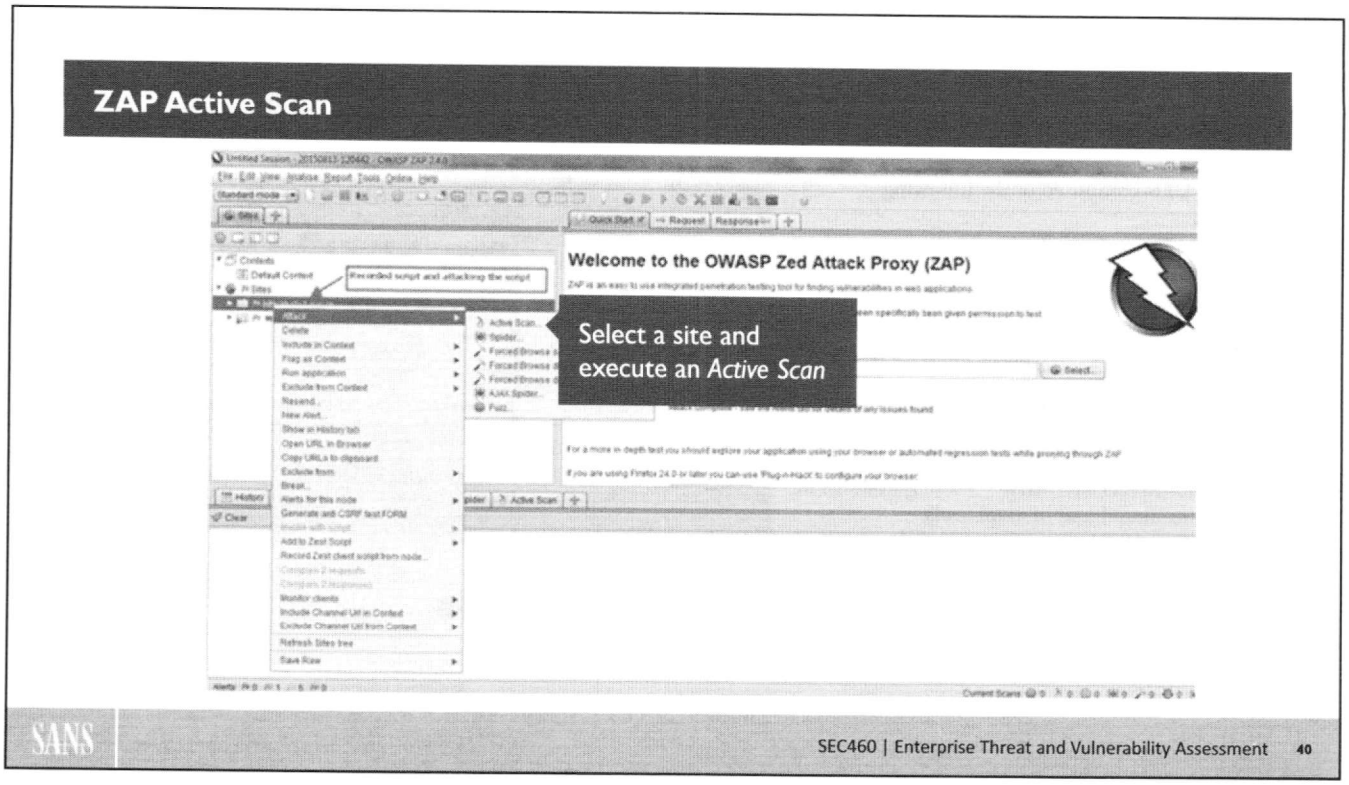
Zap runs on proxy, to set up the proxy in ZAP:

- Close all active Firefox browser sessions
  ZAP tool -> Tools Menu -> Options -> Local Proxy -> Change Address = 127.0.0.1 Port = 8080.
  Mozilla browser -> Tools Menu -> Options -> Advanced tab -> Network -> Settings -> Select Manual Proxy configuration:- HTTP Proxy = 127.0.0.1 Port = 8080.

- Now try to connect to your application using your browser. If you can't connect to it then check your proxy settings again. You will need to check your browser's proxy settings, and ZAP's proxy settings. It's also worth checking that the application that you are trying to test is running!

- When you have successfully connected to your application you will see one or more lines in ZAP's Sites and History tabs. Note that most of ZAP's tabs provide additional functionality that could be accessed via 'right click' menus.

- Right click on the HTML -> Attack -> Active scan. ZAP will perform active scan on all the pages and display the results.



ZAP Active Scan

So far ZAP has only carried out passive scans of your web application. Passive scanning does not change responses in any way and is considered safe. Scanning is also performed in a background thread to not slow down exploration. Passive scanning is good at finding some vulnerabilities and as a way to get a feel for the basic security state of a web application and locate where more investigation may be warranted.

Active scanning, however, attempts to find other vulnerabilities by using known attacks against the selected targets. Active scanning is a real attack on those targets and can put the targets at risk, so do not use active scanning against targets you do not have permission
to test.

To start an active scan:

1. In the Tree View, in the Sites tab, select the sites you want to perform an active scan on.
2. Right-click the selected sites and select Active Scan.

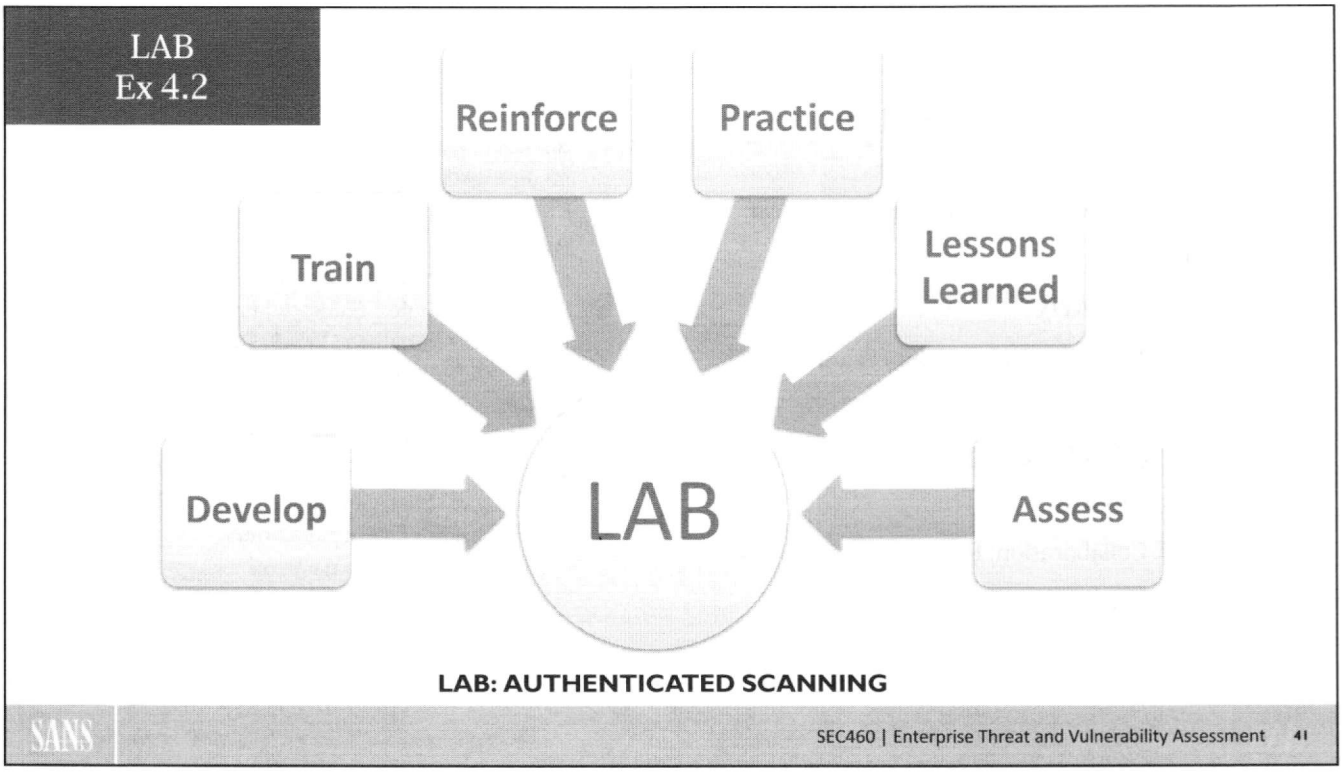
Or

1. In the Information Window, select the Active Scan tab.
2. Click New Scan.

To review and modify your settings, then begin an active scan:

1. In the Menu Bar, click Tools -> Active Scan.
2. Review the settings and make any changes you wish to.
3. Click Start Scan to start the Active Scan with these settings.

You can review the results of your active scan the same way you reviewed the results of your passive scan, as shown in Interpret Your Test Results.



LAB: Authenticated Scanning

Please refer to the Wiki for Exercise 4.2.

Course Roadmap

- Day 1: Methodology, Planning, and Threat Modeling
- Day 2: Discovery
- Day 3: Enhanced Vulnerability Scanning and Automation
- **Day 4: Validation, Triage, and Mass Data Management**
- Day 5: Collaboration, Remediation, and Reporting
- Day 6: Capstone Exercise

SEC460.4

Vulnerability Validation
Manual Validation
- **Lab: Manual Validation**

Authenticated Scanning
- **Lab: Authenticated Scanning**

PowerShell WinRM Enhanced Engagements
- **Lab: PowerShell and WinRM Enhanced**

Data Management
Overcoming Data Management Pitfalls
- **Lab: Data Management Mayhem**

Enterprise Knowledge Management
- **Lab: Data Management and Collaboration**

Collaboration and Purple Teaming
- **Lab: Testing Egress Controls**

Triage
- **Lab: Triage**

This page intentionally left blank.

PowerShell WinRM Enhanced Engagements

PowerShell can automate away tedium

- Checking for patches

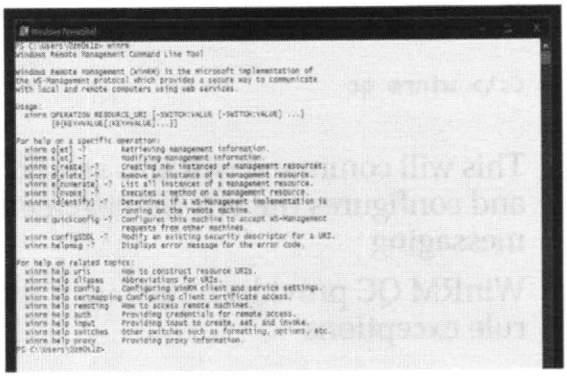
```
Get-HotFix -Description "Security*" -ComputerName
"Server01", "Server02" -Cred "Domain\admin"
```

- Check for file (existence or not (passwords.txt)

```
get-childitem *.*
```

Windows Remote Management enables us to take action on a massive scale just as easily as command singles

- WS-Man service



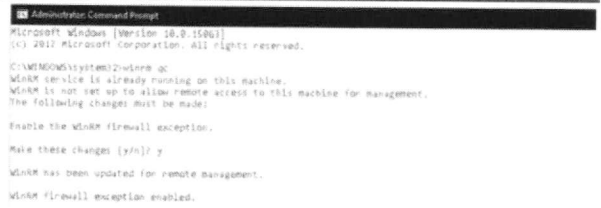
PowerShell WinRM Enhanced Engagements

The Windows Remote Management (a.k.a. WinRM) interface is a component of the Windows Hardware Management toolkit that allows remote management access to computer via the network. It's used frequently as a conduit to allow remote management of computer via PowerShell. As a result, WinRM is enabled by default on Windows Server 2012 to enable the Server Manager tool but it is not enabled for Windows client OS's by default. These features include a service that implements the WS-Management protocol, hardware diagnosis and control through baseboard management controllers (BMCs), and a COM API and scripting objects that allow you to write applications that communicate remotely through the WS-Management protocol. For more information about the public specification for WS-Management protocol, see Web Services for Management (WS–Management).

PowerShell WinRM Enhanced Engagements

Query/Start the WinRM Service

```
C:\> winrm qc
```



This will command will also set the WinRM service startup type to automatic and configures the WS-Management protocol listener to accept inbound messaging

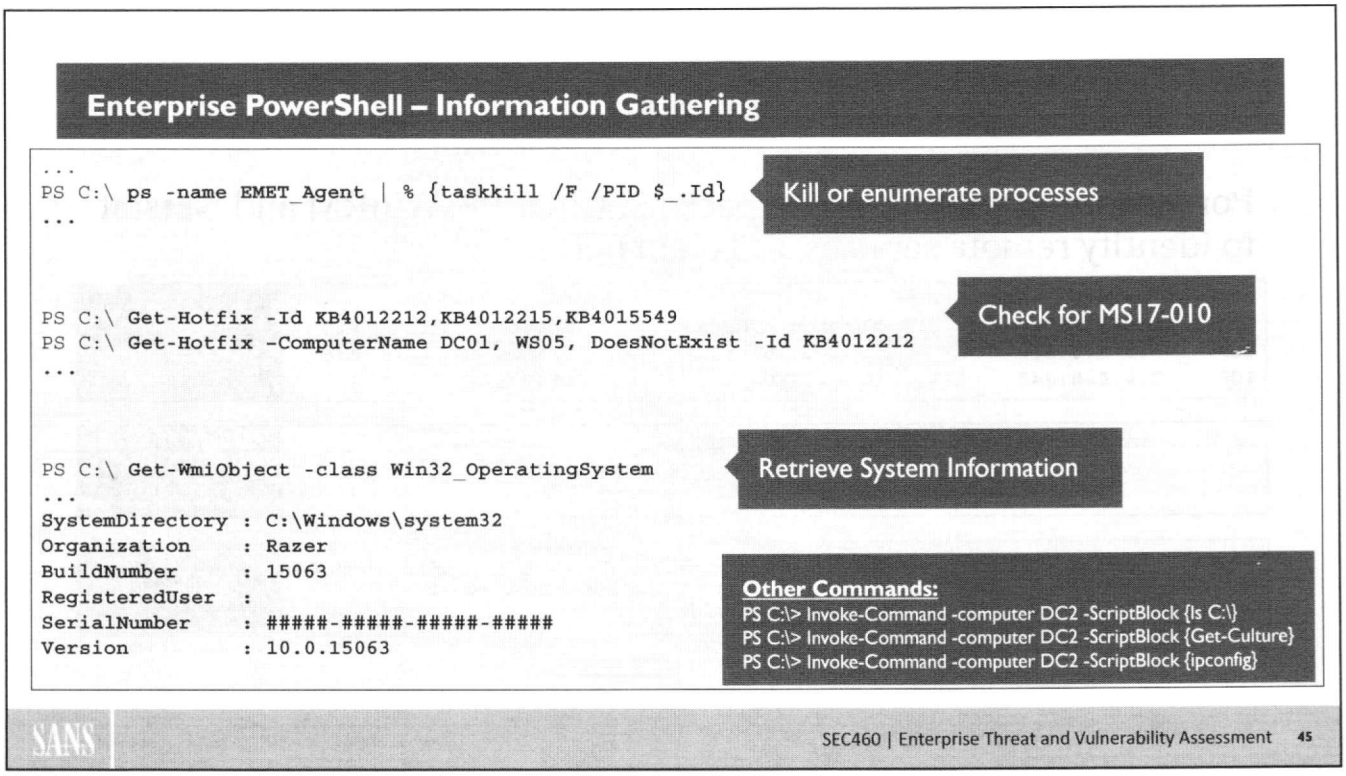
WinRM QC provides a simplistic auto configuration method down to firewall rule exceptions

PowerShell WinRM Enhanced Engagements

The first step is to Query/Start the WinRM Service

```
C:\> winrm qc
```

This will command will also set the WinRM service startup type to automatic and configures the WS-Management protocol listener to accept inbound messaging. WinRM QC provides a simplistic auto configuration method down to firewall rule exceptions



Enterprise PowerShell – Information Gathering

The **Get-Hotfix** cmdlet gets hotfixes (also called updates) that have been installed on either the local computer (or on specified remote computers) by Windows Update, Microsoft Update, or Windows Server Update Services; the cmdlet also gets hotfixes or updates that have been installed manually by users.

Example 1: Get all hotfixes on the local computer

PS C:\> Get-HotFix

Example 2: Get all hotfixes on multiple computers that start with a search string

PS C:\> Get-HotFix -Description "Security*" -ComputerName "Server01", "Server02" -Cred "Server01\admin01"

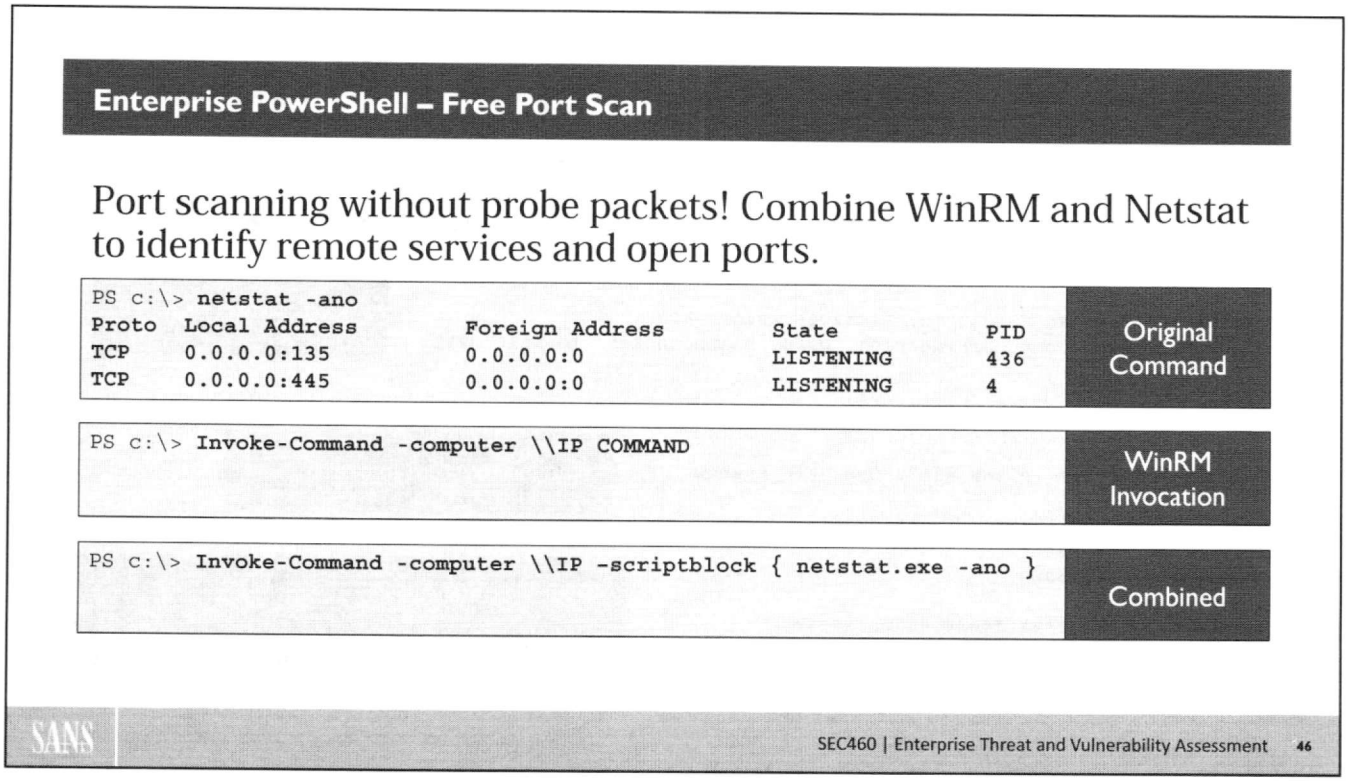
Example 3: Create a text file that contain the computer names that are missing a security update

PS C:\> $A = Get-Content "servers.txt"

PS C:\> $A | ForEach { if (!(Get-HotFix -Id "KB957095" -ComputerName $_)) { Add-Content $_ -Path "Missing-kb953631.txt" }}

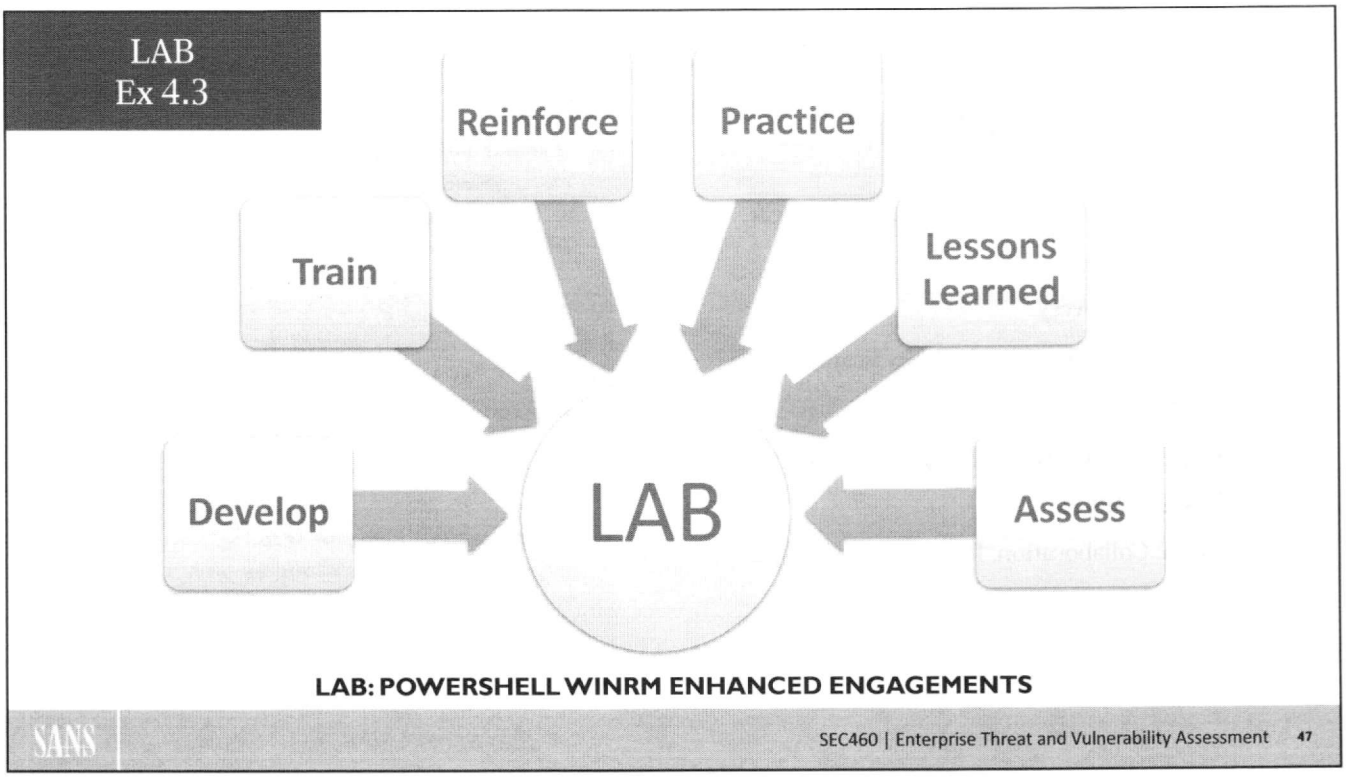
Example 4: Get the most recent hotfix on the local computer

PS C:\> (Get-HotFix | sort installedon)[-1]



Enterprise PowerShell – Free Port Scan

We can leverage PowerShell and WinRM to create all kinds of networking havoc! Port scanning without probe packets, for example! Combine WinRM and Netstat to identify remote services and open ports.



LAB: PowerShell WinRM Enhanced Engagements

Please refer to the Wiki for Exercise 4.3.

Course Roadmap

- Day 1: Methodology, Planning, and Threat Modeling
- Day 2: Discovery
- Day 3: Enhanced Vulnerability Scanning and Automation
- **Day 4: Validation, Triage, and Mass Data Management**
- Day 5: Collaboration, Remediation, and Reporting
- Day 6: Capstone Exercise

SEC460.4

Vulnerability Validation
Manual Validation
- **Lab: Manual Validation**

Authenticated Scanning
- **Lab: Authenticated Scanning**

PowerShell WinRM Enhanced Engagements
- **Lab: PowerShell and WinRM Enhanced**

Data Management
Overcoming Data Management Pitfalls
- **Lab: Data Management Mayhem**

Enterprise Knowledge Management
- **Lab: Data Management and Collaboration**

Collaboration and Purple Teaming
- **Lab: Testing Egress Controls**

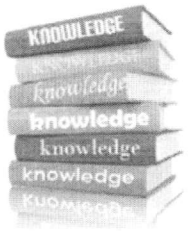
Triage
- **Lab: Triage**

This page intentionally left blank.

Data Management and the Enterprise Knowledge-Base

The Enterprise Security Knowledge Base includes:

- Baselines of the performing organization's standards, processes, procedures, policies and documentation around the project. It also includes the configuration management databases
- Historical information like lessons learned
- The knowledge-base should be a **Living** document



Goals of Enterprise Vulnerability Scanning

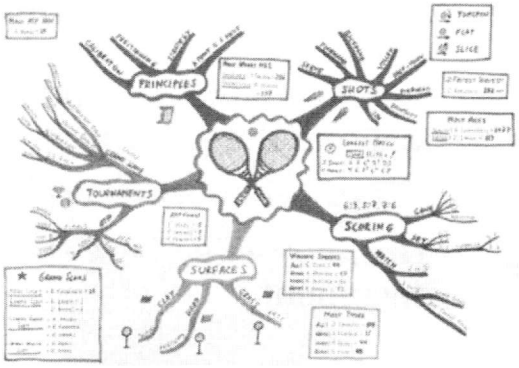
The Enterprise Security Knowledge Base is made up of baselines of the performing organization's standards, processes, procedures, policies and documentation around the project. It also includes the configuration management databases, and historical information like lessons learned. The knowledge-base should be a **Living** document.

Mind Maps and Vulnerability Data

Mind Mapping is a technique to assist learning. It improves:

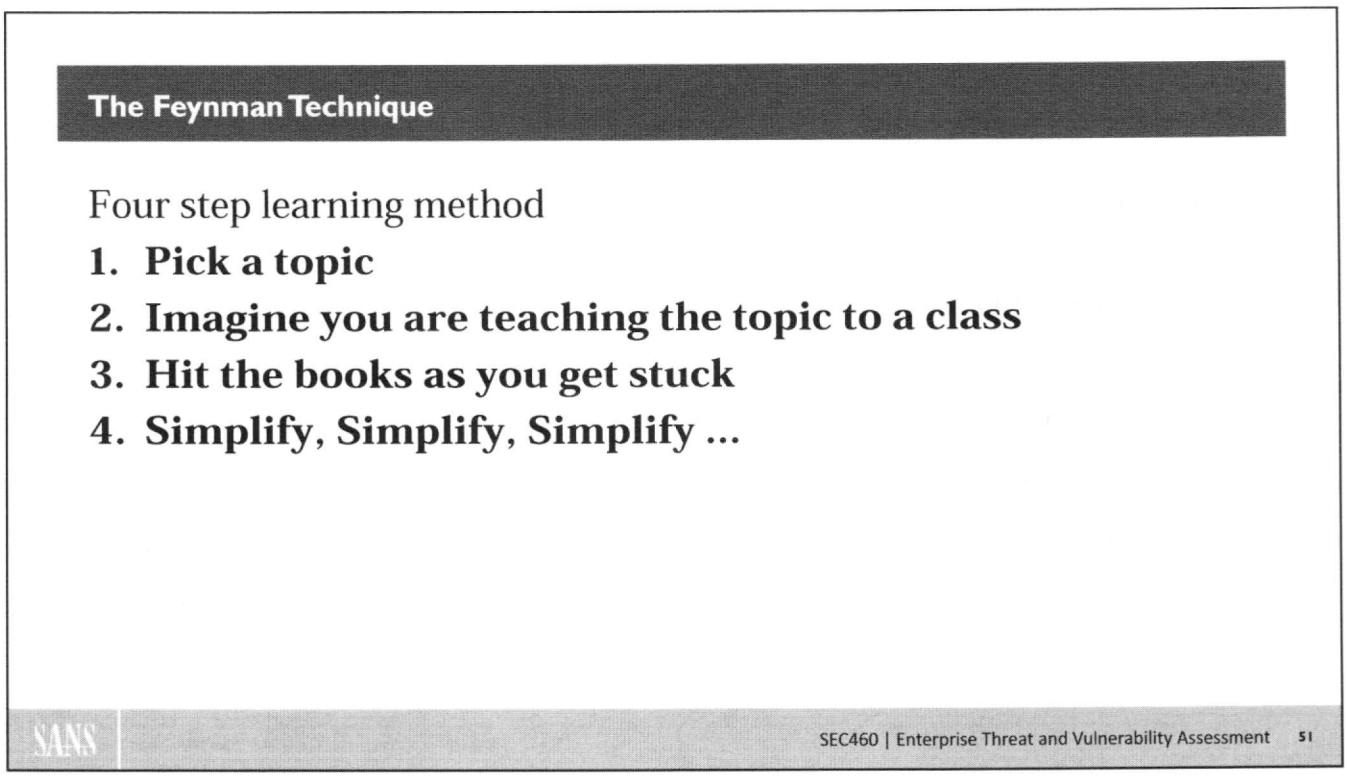
- Information retention
- Enhances creative problem solving

Framed around a central topic
Much like Center of Gravity (COG) analysis



Mind Maps and Vulnerability Data

Mind Mapping is a technique to assist learning. It is particularly useful when making decisions on a complex data set. Each individual node should be deconstructed to represent an easy to understand component. This allows us to rapidly zero-in on key nexuses of information that may otherwise be overlooked. Intelligence organizations follow similar methodologies using a technique called Center of Gravity (COG) Analysis. This allows organizations like the FBI to deconstruct vast criminal networks and military services to identify and interdict high value targets.



The Feynman Technique

Four step learning method

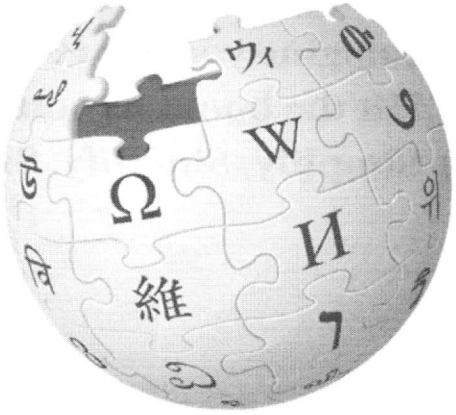
1. **Pick a topic**
2. **Imagine you are teaching the topic to a class**
3. **Hit the books as you get stuck**
4. **Simplify and use analogies** – Can you teach it using stories and examples?

Keeping Track of Critical Information

Many testers use a Wiki to manage organizational practice and knowledge.

Many kinds of wiki-like options:

- Wiki.js
- Confluence
- Media Wiki
- And More!



Keeping Track of Critical Information

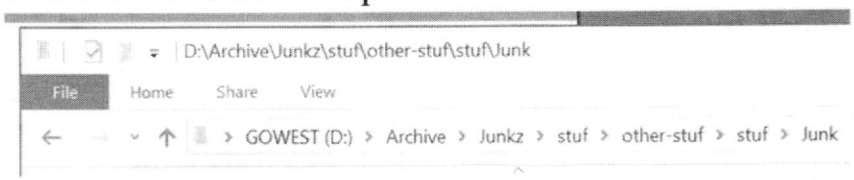
Many testers use a Wiki to manage organizational practice and knowledge.

Many kinds of wiki-like options:

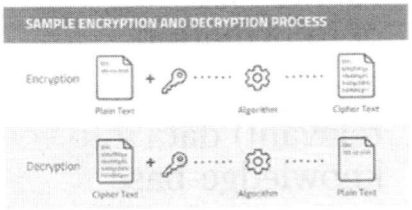
- Wiki.js
- Confluence
- Media Wiki
- And More!

Secure Management and Storage of Critical Information

Some information is sensitive. Managing data handling and encryption is a critical first step!



- How is data handled?
  - During transmission
  - How about at rest
- What kind of risks arise?



Secure Management and Storage of Critical Information

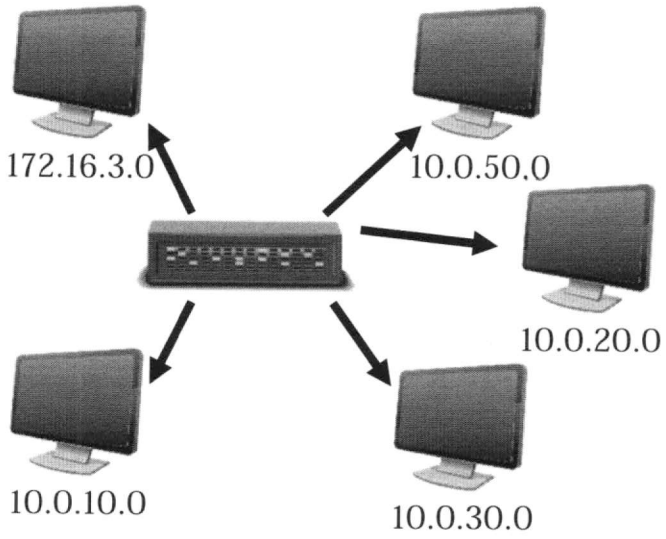
Some information is sensitive. Managing data handling and encryption is a critical first step! How is data handled during transmission? How about at rest? What kind of risks arise as a result of the organization's data management processes?

Topology Mapping and Tracking

Network layout and topology is an information type that is highly relevant to security professionals

It may already exist

- Identify existing sources of information
- Incorporate external (but relevant) data into your knowledge-base



Topology Mapping and Tracking

Network layout and topology is an information type that is highly relevant to security professionals and it may already exist! When developing an enterprise knowledgebase, it is important to identify and incorporate existing repositories of knowledge, and this goes both ways. When improving on a data set that is also used by a peer, it is important to keep open lines of communication and data sharing.

Course Roadmap

- Day 1: Methodology, Planning, and Threat Modeling
- Day 2: Discovery
- Day 3: Enhanced Vulnerability Scanning and Automation
- **Day 4: Validation, Triage, and Mass Data Management**
- Day 5: Collaboration, Remediation, and Reporting
- Day 6: Capstone Exercise

SEC460.4

Vulnerability Validation
Manual Validation
- **Lab: Manual Validation**

Authenticated Scanning
- **Lab: Authenticated Scanning**

PowerShell WinRM Enhanced Engagements
- **Lab: PowerShell and WinRM Enhanced**

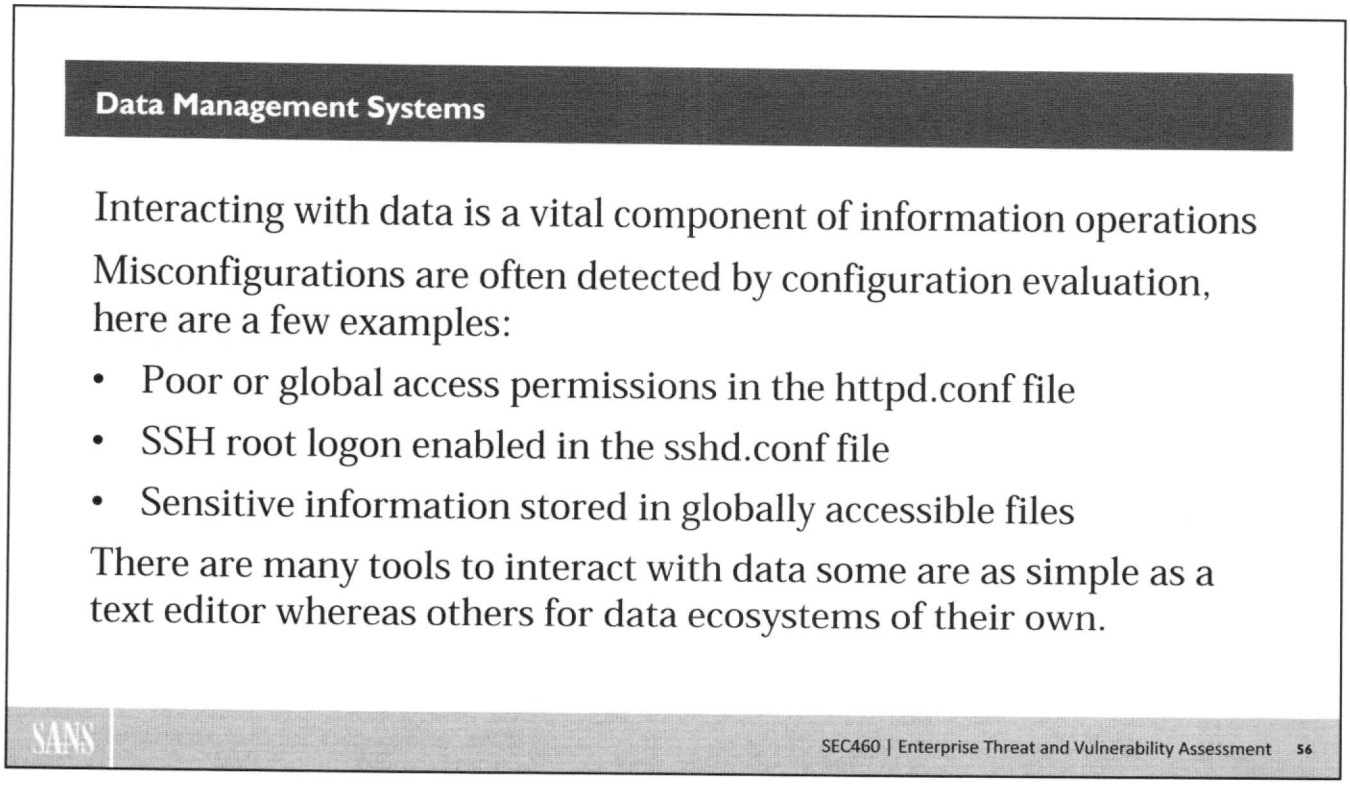
Data Management
Overcoming Data Management Pitfalls
- **Lab: Data Management Mayhem**

Enterprise Knowledge Management
- **Lab: Data Management and Collaboration**

Collaboration and Purple Teaming
- **Lab: Testing Egress Controls**

Triage
- **Lab: Triage**

This page intentionally left blank.



Overcoming Data Management Pitfalls

All that said. That are still critical, strategic hurdles to overcome when approaching large datasets. What do you do when there is a TON of data? Having trouble with tools using proprietary output formats? Too much data. WAY TOO MUCH?

A data management tool or sometimes even a project or task management tool could be a major boon to operations. It is best; however, to lead with simplistic and work up to more complex data management appliances gradually. Some examples of simple tools that can aid our data handling capabilities are text editors. Wikis and Spreadsheets are also easily adapted into existing processes. When scale (of the team not the dataset!) becomes an issue, larger data driven systems like MySQL may be more appropriate.

Overcoming Data Management Pitfalls

There are critical, strategic hurdles to overcome when approaching large datasets

- Mass Data
- Fighting your tools
- Information vs Noise

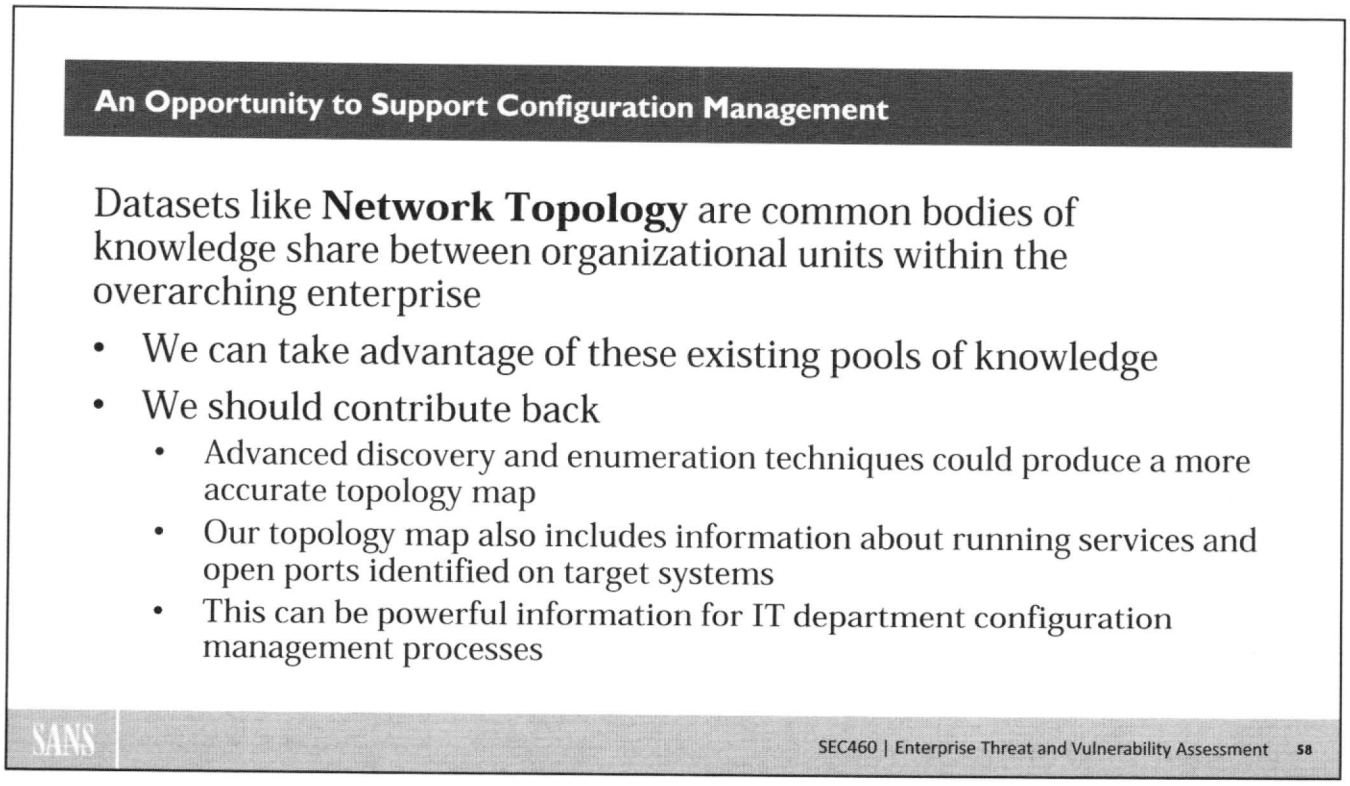
Some examples of tools that can aid our data handling capabilities include:

Text Editors

- Notepad
- Notepad++
- Atom
- Sublime Text
- VI / VIM
- Nano

Wikis, Confluence, Spreadsheets, Databases (Access, MySQL, etc.), and many more

This page intentionally left blank.



An Opportunity to Support Configuration Management

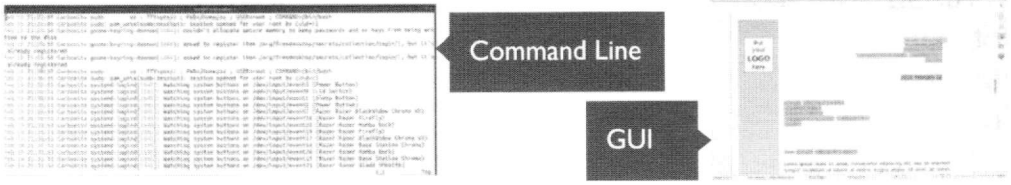
Datasets like **Network Topology** are common bodies of knowledge share between organizational units within the overarching enterprise. We can take advantage of these existing pools of knowledge, but we should also contribute back where possible.

Modes of Data Interaction

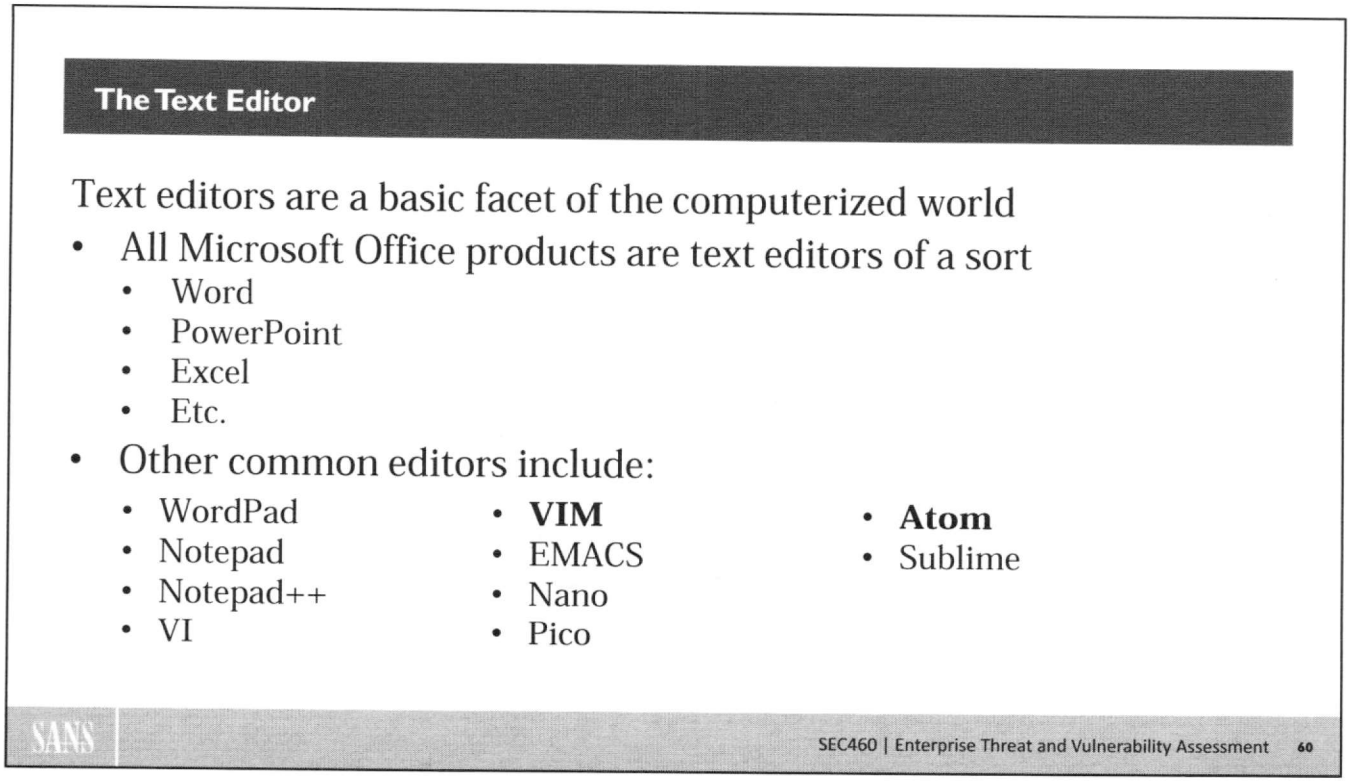
There are generally two categories of interaction with system data

- Graphical
- Command Line

While we might attempt to download files and open them in a graphical user interface, this becomes impractical at scale. We *must* be comfortable with both.



This page intentionally left blank.



The Text Editor

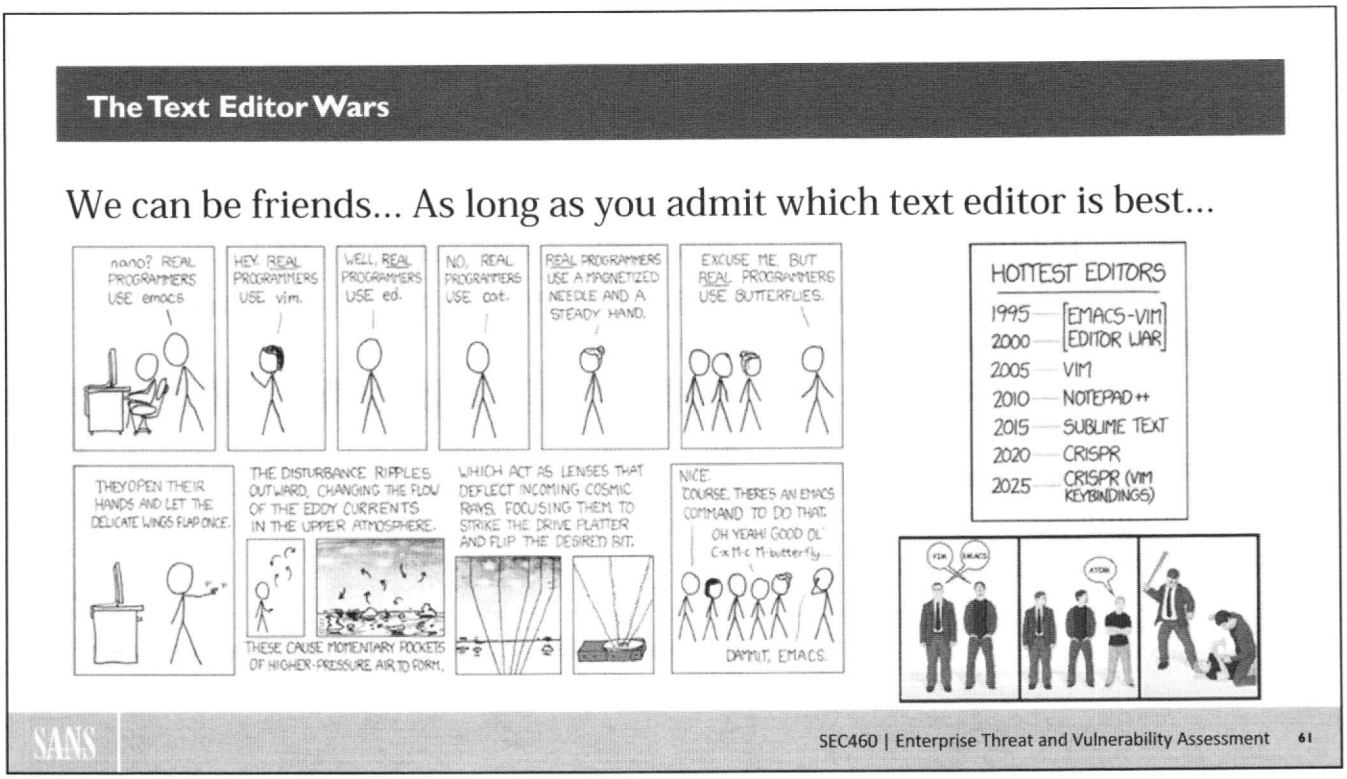
Text editors are a basic facet of the computerized world. All Microsoft Office products, for example, are text editors of a sort.

- Word
- PowerPoint
- Excel

Other common editors include:

- WordPad
- Notepad
- Notepad++
- VI
- **VIM**
- EMACS
- Nano
- Pico
- **Atom**
- Sublime

Next, we will breakdown the editors listed in bold and unlock a number of hidden features that can accelerate any existing workflow without causing any major deviation.



The Text Editor Wars

It's VIM. Obviously.

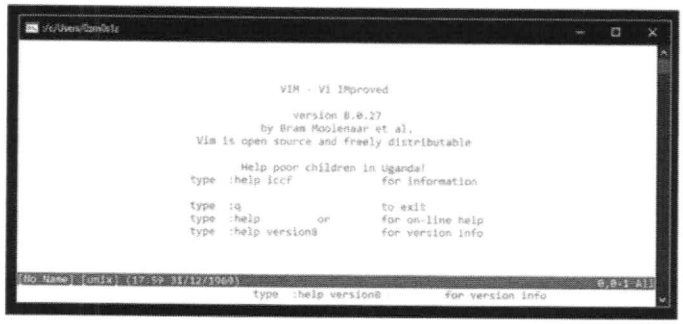
The Vi Improved Text Editor

VI is a Unix text editor created by Bill Joy in 1976.

VIM or (Vi IMproved) by Bram Moolenaar was released in 1991.

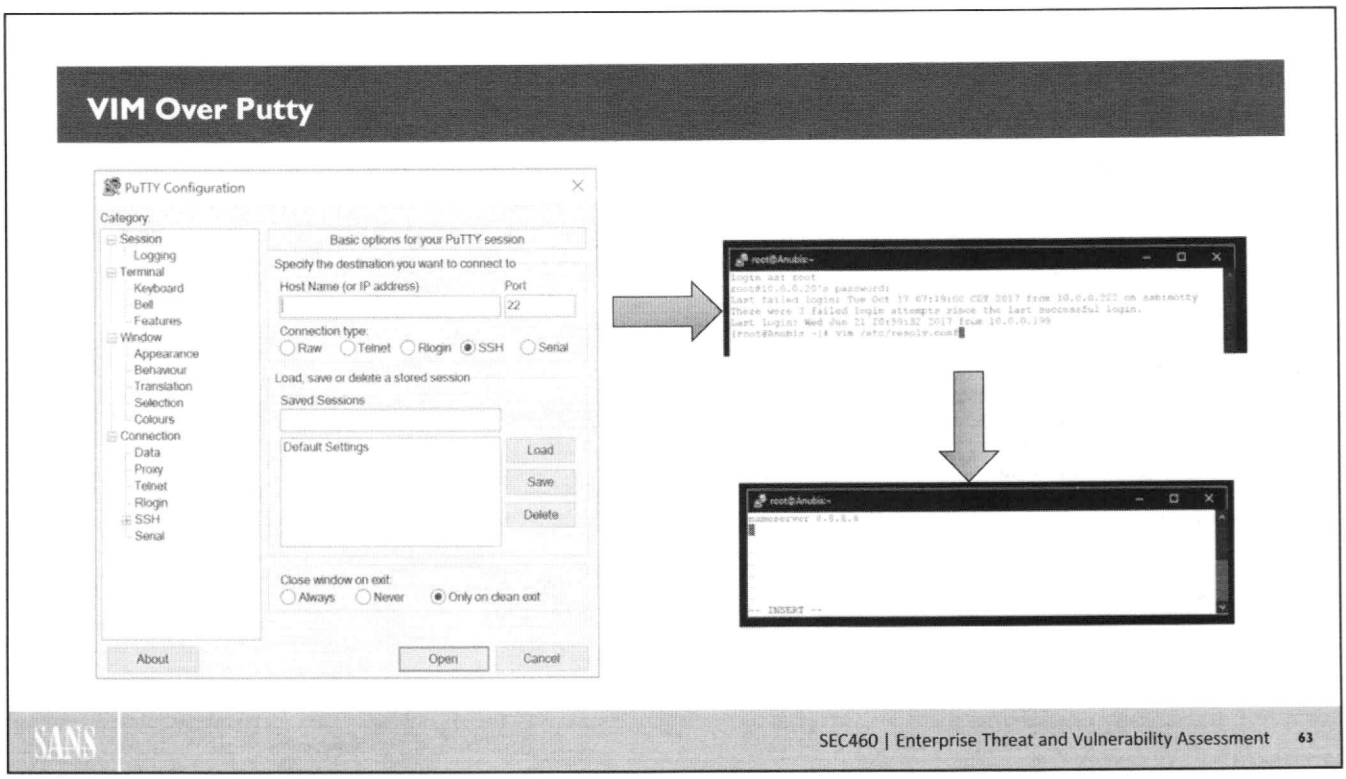
- VIM is an extended version of vi that includes additional quality of life and functionality improvements
  - VIM allows navigation using arrow keys
  - Vimscript is a native scripting language
  - VIM is cross-platform

```
# vi <filename>
# vim <filename>
```



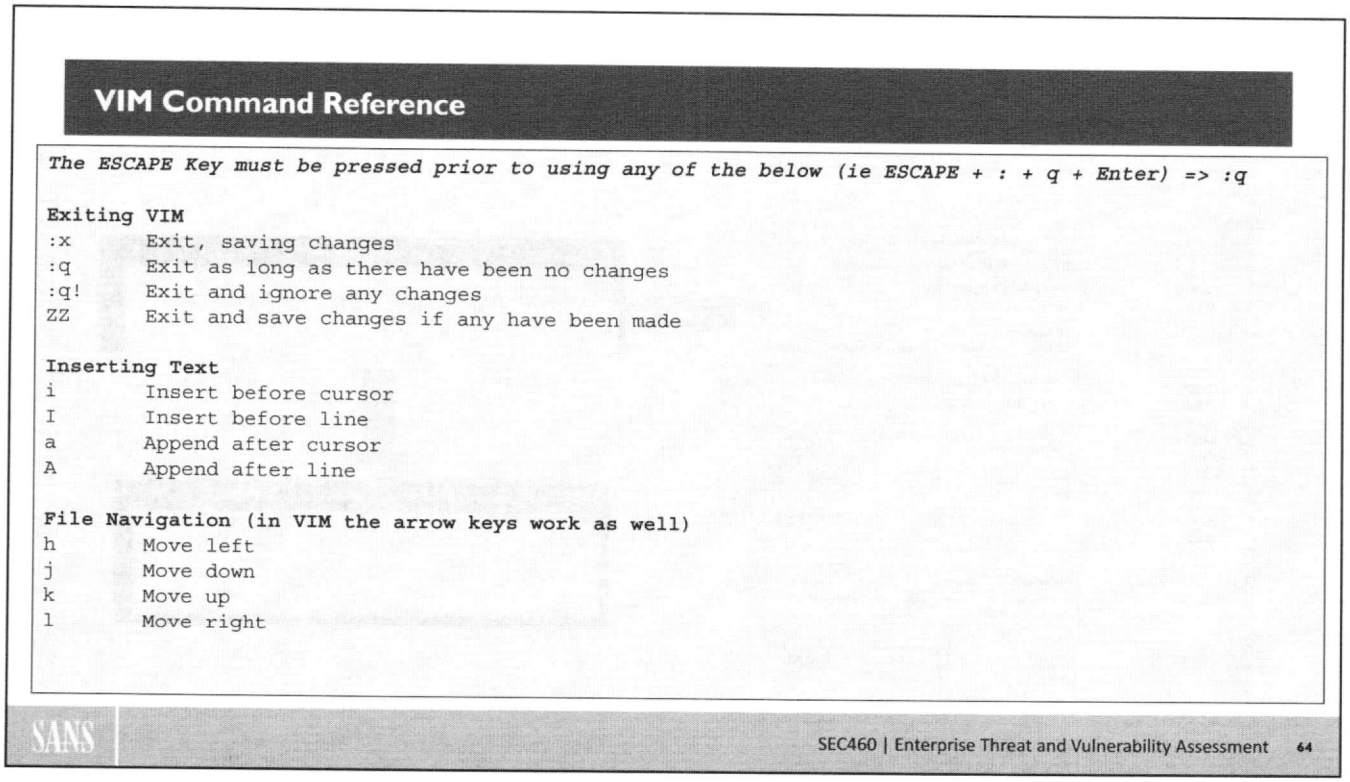
The Vi IMproved Text Editor

VI is a Unix text editor created by Bill Joy in 1976. VIM or (Vi IMproved) by Bram Moolenaar is an extended version of vi that includes additional quality of life and functionality improvements. It was released in 1991.



VIM Over Putty

We will be interacting with VIM in an upcoming lab using the Putty interface to connect to a remote Linux system.



VIM Command Reference

Exiting VIM

:x	Exit, saving changes
:q	Exit as long as there have been no changes
:q!	Exit and ignore any changes
ZZ	Exit and save changes if any have been made

Inserting Text

i	Insert before cursor
I	Insert before line
a	Append after cursor
A	Append after line

File Navigation (in VIM the arrow keys work as well)

h	Move left
j	Move down
k	Move up
l	Move right

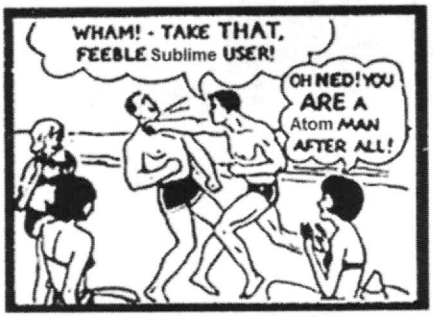
File Editing

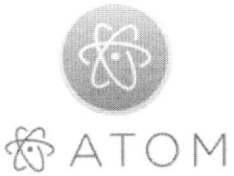
U	undo
y	yank (copy) highlight the desired lines using the navigation keys
P	paste

The Atom Text Editor (1)

Atom much like Sublime and Notepad++ is a powerful, "hackable" text editor.

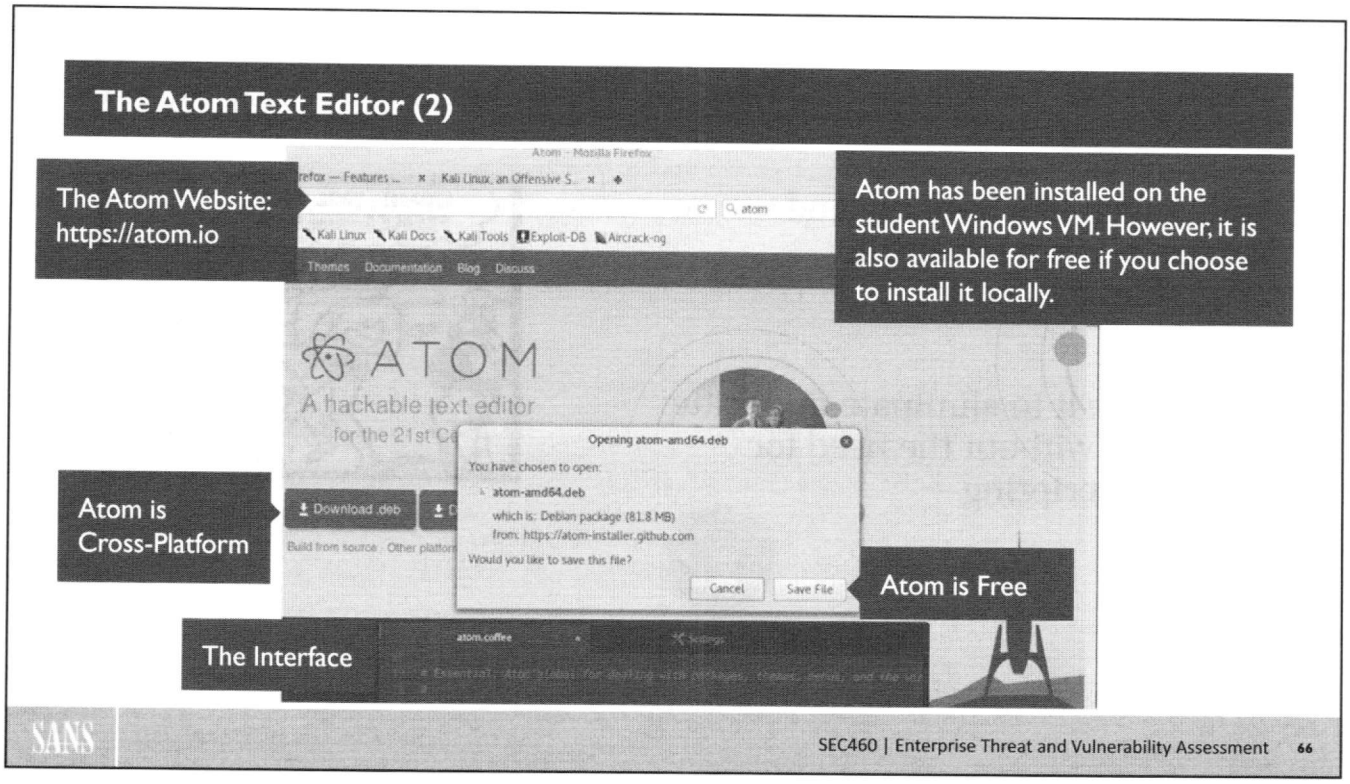
We can use it to eliminate duplicate workflows without the need for excessive scripting





The Atom Text Editor (1)

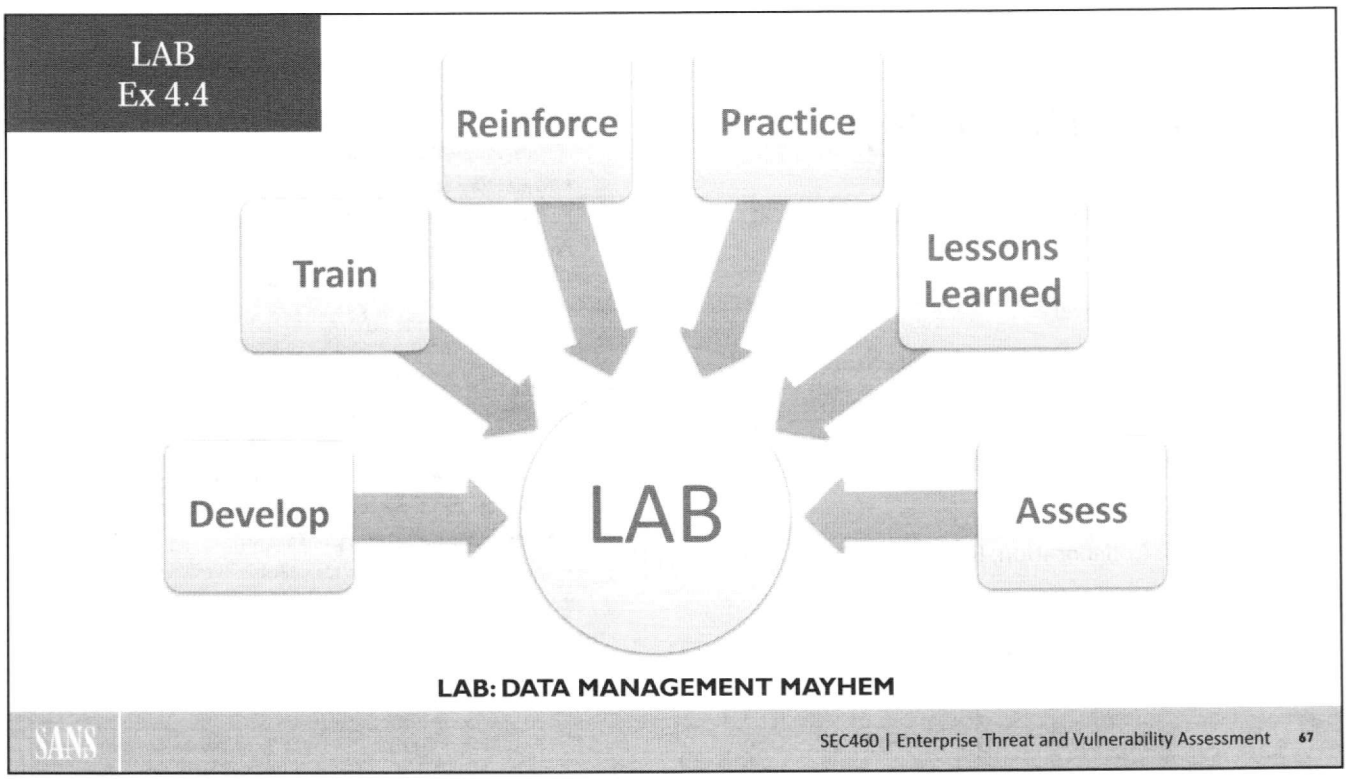
Atom much like Sublime and Notepad++ is a powerful, "hackable" text editor. We can use it to eliminate duplicate workflows without the need for excessive scripting.



The Atom Text Editor (2)

Atom is freely available from the project website: atom.io

The tool is the ultimate in cross-platform compatibility as it is written in HTML and JavaScript using the Electron development framework. Don't like a feature? You can modify it using simple web markup syntax. Awesome! Let's try it out!



LAB: Data Management Mayhem

Please refer to the Wiki for Exercise 4.4.

Course Roadmap

- Day 1: Methodology, Planning, and Threat Modeling
- Day 2: Discovery
- Day 3: Enhanced Vulnerability Scanning and Automation
- **Day 4: Validation, Triage, and Mass Data Management**
- Day 5: Collaboration, Remediation, and Reporting
- Day 6: Capstone Exercise

SEC460.4

Vulnerability Validation
Manual Validation
- **Lab: Manual Validation**

Authenticated Scanning
- **Lab: Authenticated Scanning**

PowerShell WinRM Enhanced Engagements
- **Lab: PowerShell and WinRM Enhanced**

Data Management
Overcoming Data Management Pitfalls
- **Lab: Data Management Mayhem**

Enterprise Knowledge Management
- **Lab: Data Management and Collaboration**

Collaboration and Purple Teaming
- **Lab: Testing Egress Controls**

Triage
- **Lab: Triage**

This page intentionally left blank.

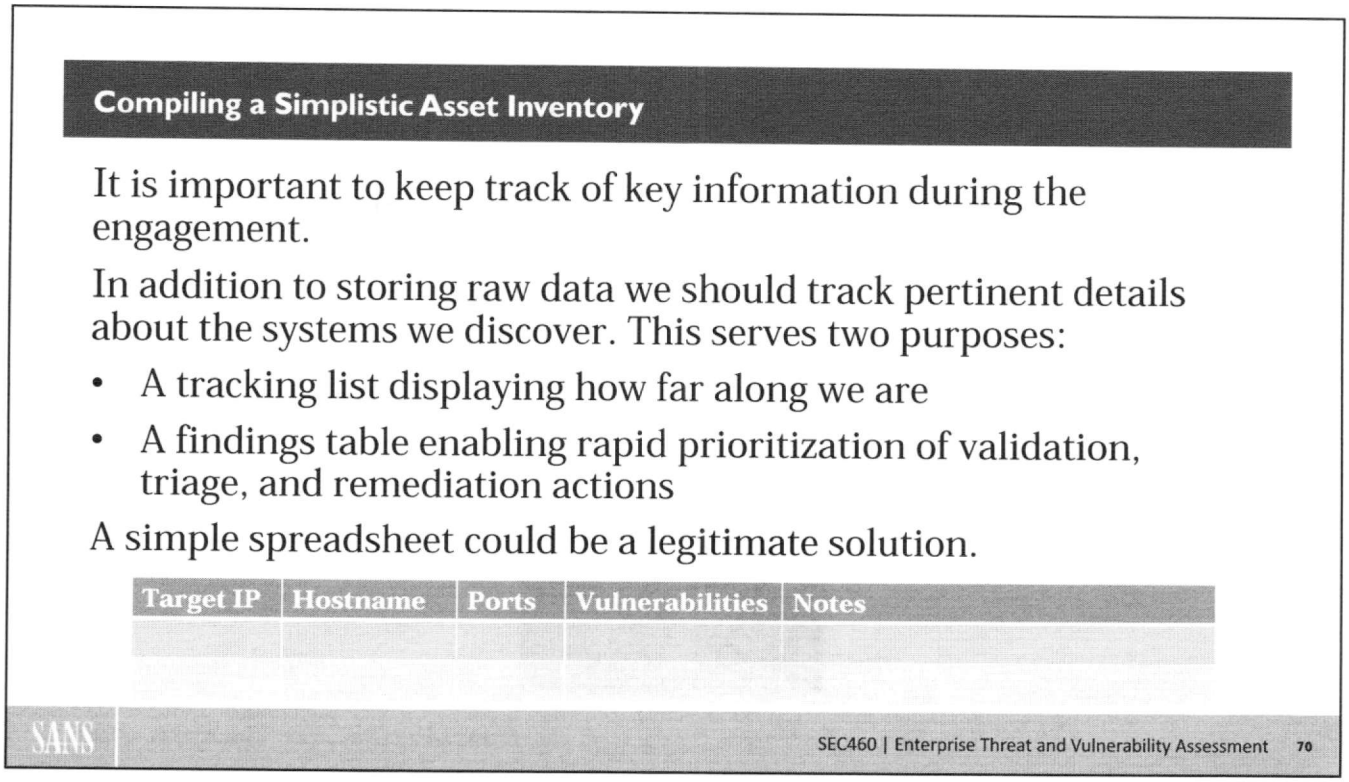
Asset Inventory

The asset inventory is an authoritative list of information systems within the purview of a given organization.

- Well-maintained inventories help to eliminate excess noise by emphasizing pertinent data
- Generally indexed according to an easily searchable schema
- All information in a focused asset inventory should be actionable

Asset Inventory

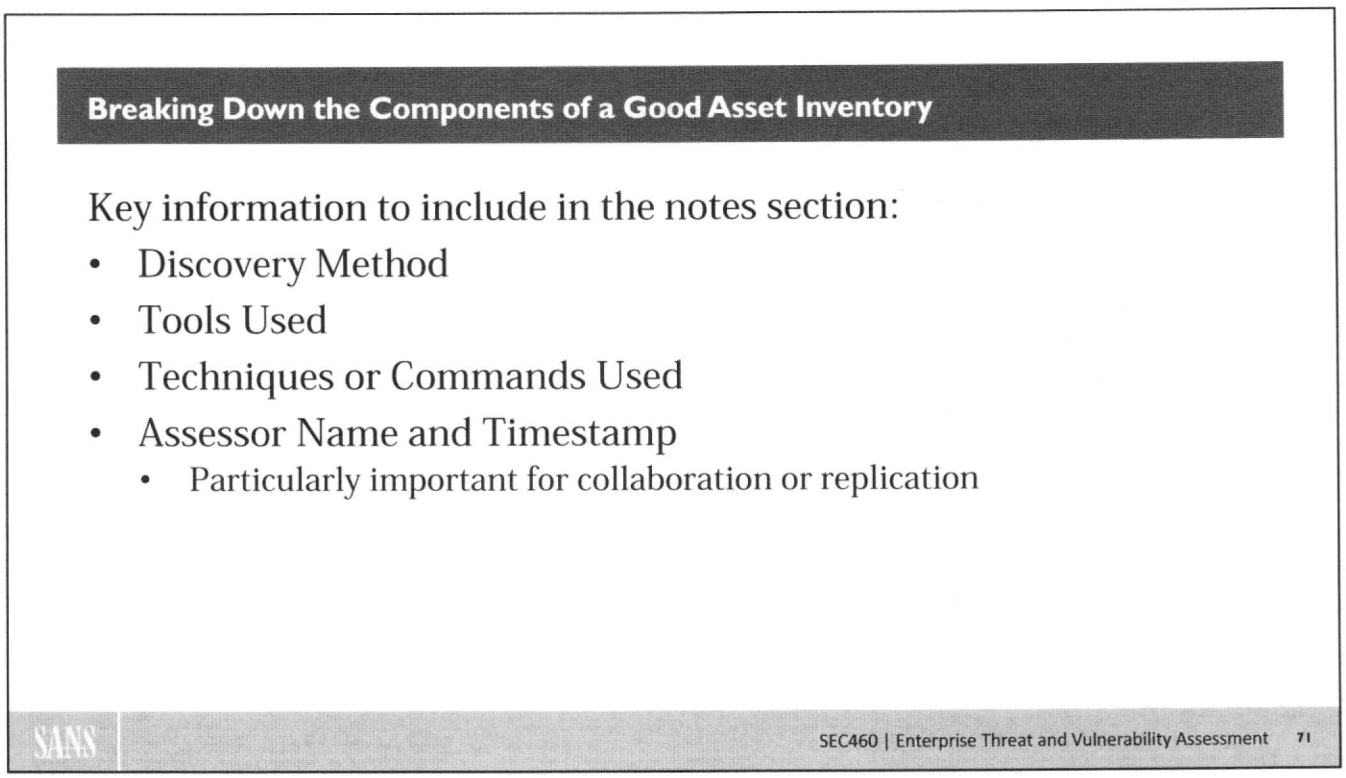
It is important to keep track of key information during the engagement. Asset inventories, generally implemented by spreadsheet, are common in many fields. In information technology they come in particularly handy do to the broad gamut of systems involved in the facilitation of networked environments. Specifically, an asset inventory is an authoritative list of information systems within the purview of a given organization.



Compiling a Simplistic Asset Inventory

The reason inventories trend towards infinitely growing lists or spreadsheets is because they are simple and easy to understand. Typically, in data management, a simple solution that is workable by all parties far exceeds more complex systems. Not everything must be perfect and the quest for a perfect inventory is unending. Do what works now and move to more robust systems when you know specifically what value exists to be tapped.

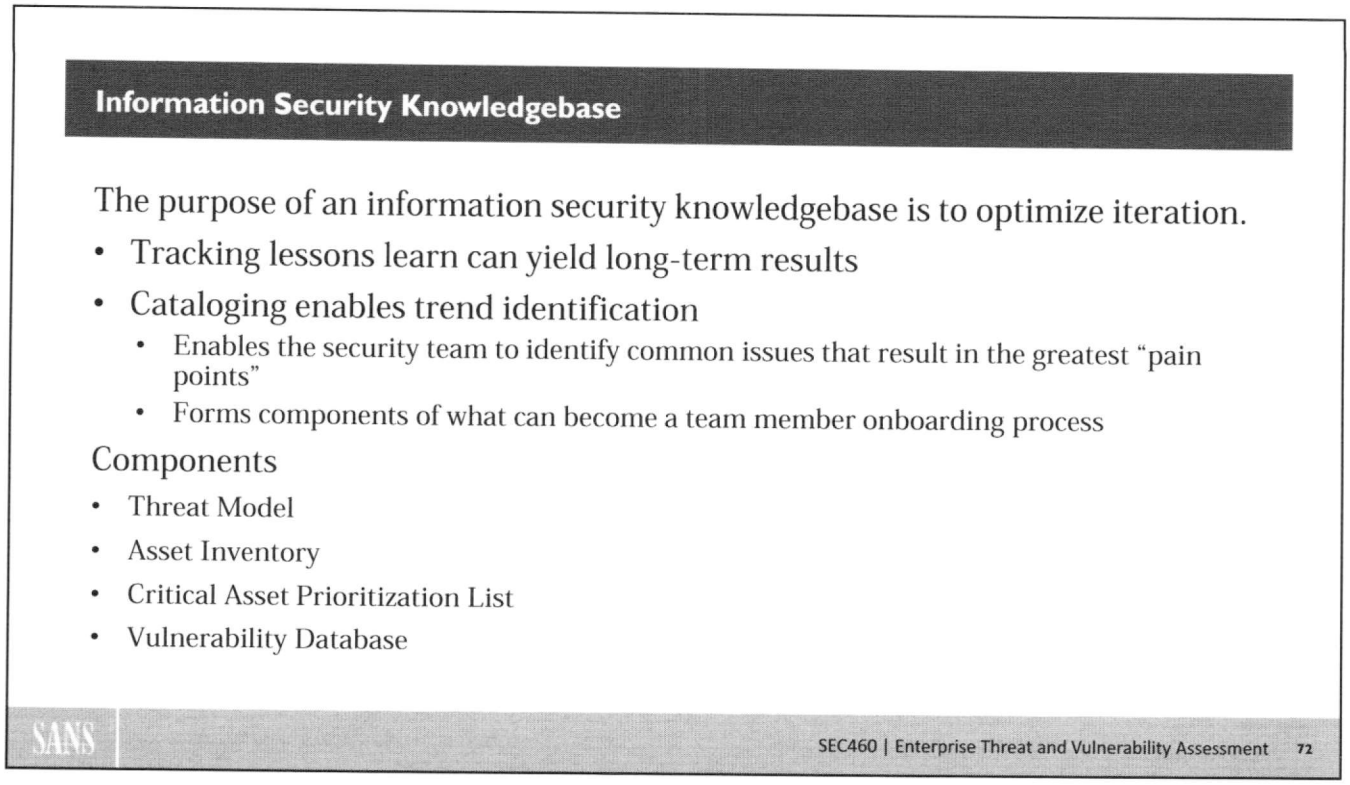
The first step to any list is the first line. Good inventories grow over time. Great inventories are measured by the magnitude of their vigilance to that effort.



Breaking Down the Components of a Good Asset Inventory

Although building a spreadsheet IS simple, working with enormous datasheets can be nightmarish! The key here is to build up from a solid foundation focusing on **key** information relevant to the purpose of the dataset itself. For the vulnerability assessor key information might include:

- Discovery Method
- Tools Used
- Techniques or Commands Used
- Assessor Name and Timestamp
- And More! Just not too much more…



Information Security Knowledgebase

In contrast to a simple inventory the information security knowledge base incorporates a much deeper and broader body of information. Despite all this they are somehow more focused. A good knowledgebase should be built up around a central purpose. If it begins to decay, shedding its skin for more decadent noisy patterns, it should be abandoned like a sinking ship. A knowledgebase is meant to grow, but never grow out of control. The purpose of an **information security knowledgebase** is to optimize iteration facilitating an endless cycle of growth with compounding interest. This knowledge base can include a subordinate set of data including threat models, the asset inventory, prioritization lists, data management best practices, and even a database of vulnerabilities relevant to the entity to whom the knowledgebase belongs.

Vulnerability Database

The vulnerability database is a centralized repository of vulnerability information for a given organization.

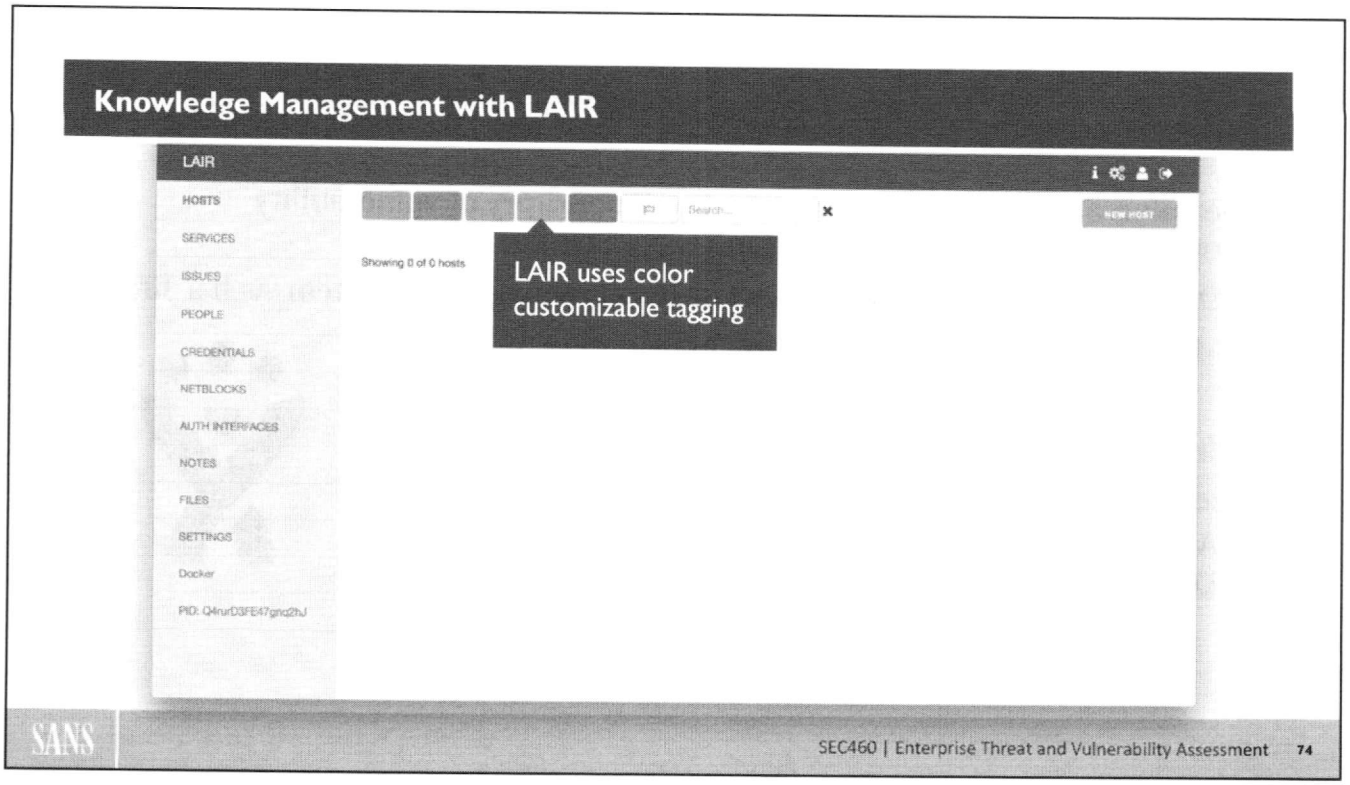
- Often implemented with a project or ticket management system such a Jira
- Many teams begin by centralizing information on a wiki

Vulnerability Data Management Tools provide InfoSec specific solutions:

- Acheron
- Dradis
- MagicTree
- Lair

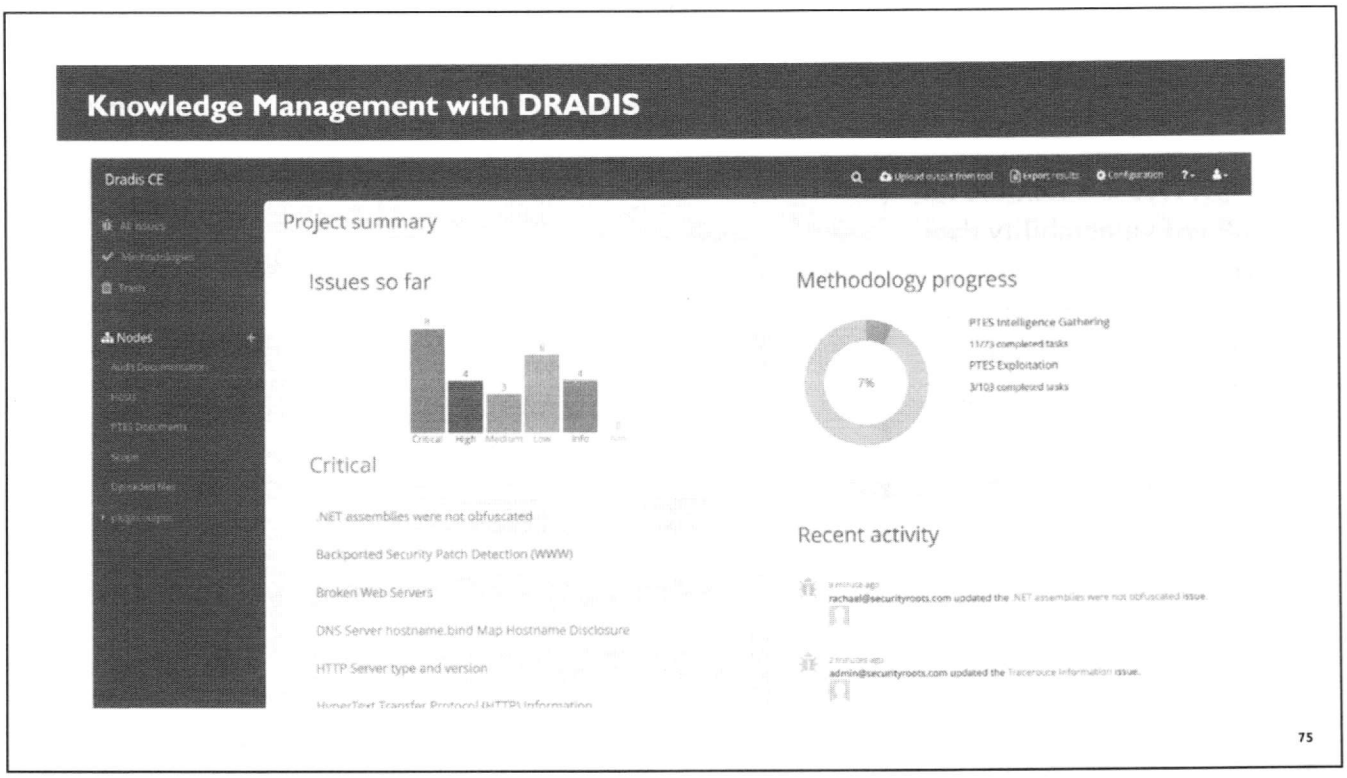
Vulnerability Database

A vulnerability database is a centralized repository of vulnerability information for a given organization. Vulnerability assessors are often an instrumental component of building these repositories, but generally it is the role of the IT Department to handle the aftermath. A schism between these two functions frequently arises out of the management application and process differences. Particularly when ticket management systems are involved. One-way dedicated testers can contribute to cutting down the life expectancy of security flaws affecting the company is by more closely integrating with local IT systems and processes when possible. The first step can be as simple as tagging reports according to the format used by ticketing systems.



Knowledge Management with LAIR

LAIR is based on the idea of collection drones where each type of drone is able to transmute a given set of data. Drones are extensible and developed in the GO programming language. It is a colorful yet robust system to support data management and team collaboration.



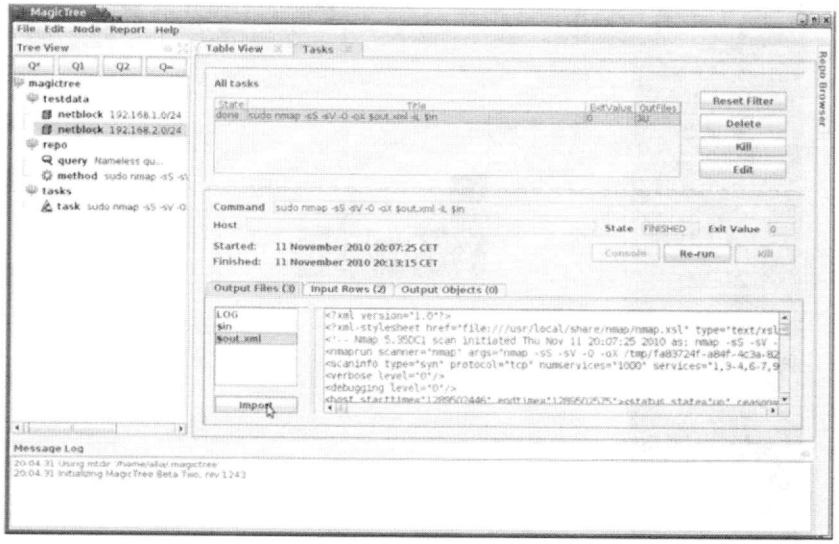
Knowledge Management with DRADIS

Dradis is a Ruby-on-Rails framework focused on empowering vulnerability assessors to collaborate jointly during an engagement. Dradis CE is a platform independent web application.

Knowledge Management with MaGICTree

MagicTree is a flexible full featured vulnerability data management tool.

- Interface similar to old versions of DRADIS
- Usage remains similar
- Free, Open Source



Knowledge Management with MagicTree

MagicTree and Dradis have similar root; however, much of flexibility of Dradis became more rigidly defined as the project searched out commercial opportunities. The result is a more stable but inflexible tool. In contrast, MagicTree retains the open source style (and appearance) it used to share with its cousin.

http://www.gremwell.com

Knowledge Management – Other Tools

Metasploit

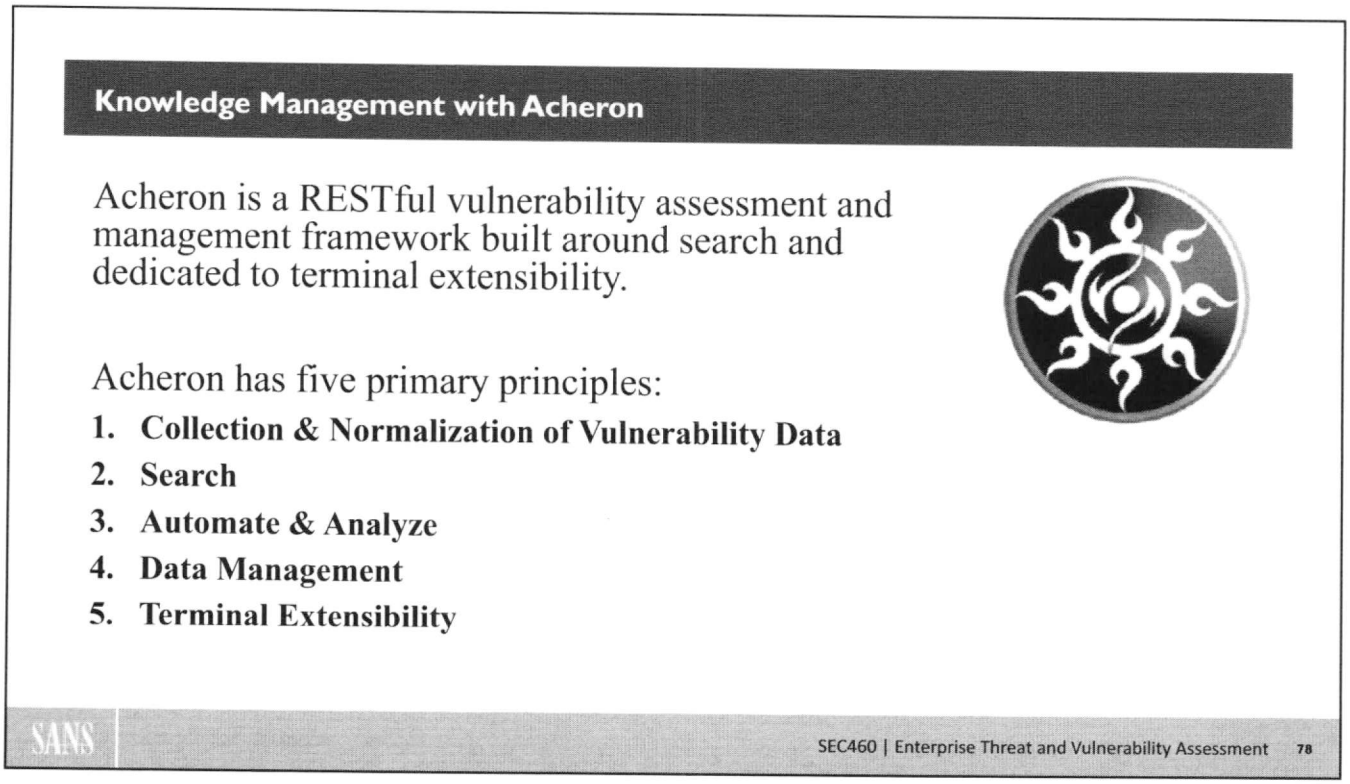
- An Exploitation Framework
- Commercial & Community Versions
- Metasploit Database for Information Handling

Vulnerability Scanners

- Nexpose
- Qualys
- Nessus

Knowledge Management - Other Tools

A host of tools include one form of data management or another. That said, most tools not specializing specifically in the handling and presentation of vulnerability data suffer from major shortcomings in this area. Distinctively, commercial vulnerability scanners and exploitation frameworks tend to fall into this category. Although their internal databases are rife with potential most implementations leave the tester wanting for a horse.



Knowledge Management with Acheron
Acheron is a RESTful vulnerability assessment and management framework built around search and dedicated to terminal extensibility. The framework was designed operating system agnostic and supports all major CPU architectures as well. The tool is built around a phased approach to vulnerability assessment that ensures quality by enforcing simplicity and enhancing productivity through search.

Acheron Performs 5 Primary Functions:

1. Collection & Normalization of Vulnerability Data
- Supports many data types including: Nessus, Acunetix, Grendel, Burp, Nmap, Nikto, Nexpose, Zap, Retina, and More
- Input threat models, intelligence, and risks

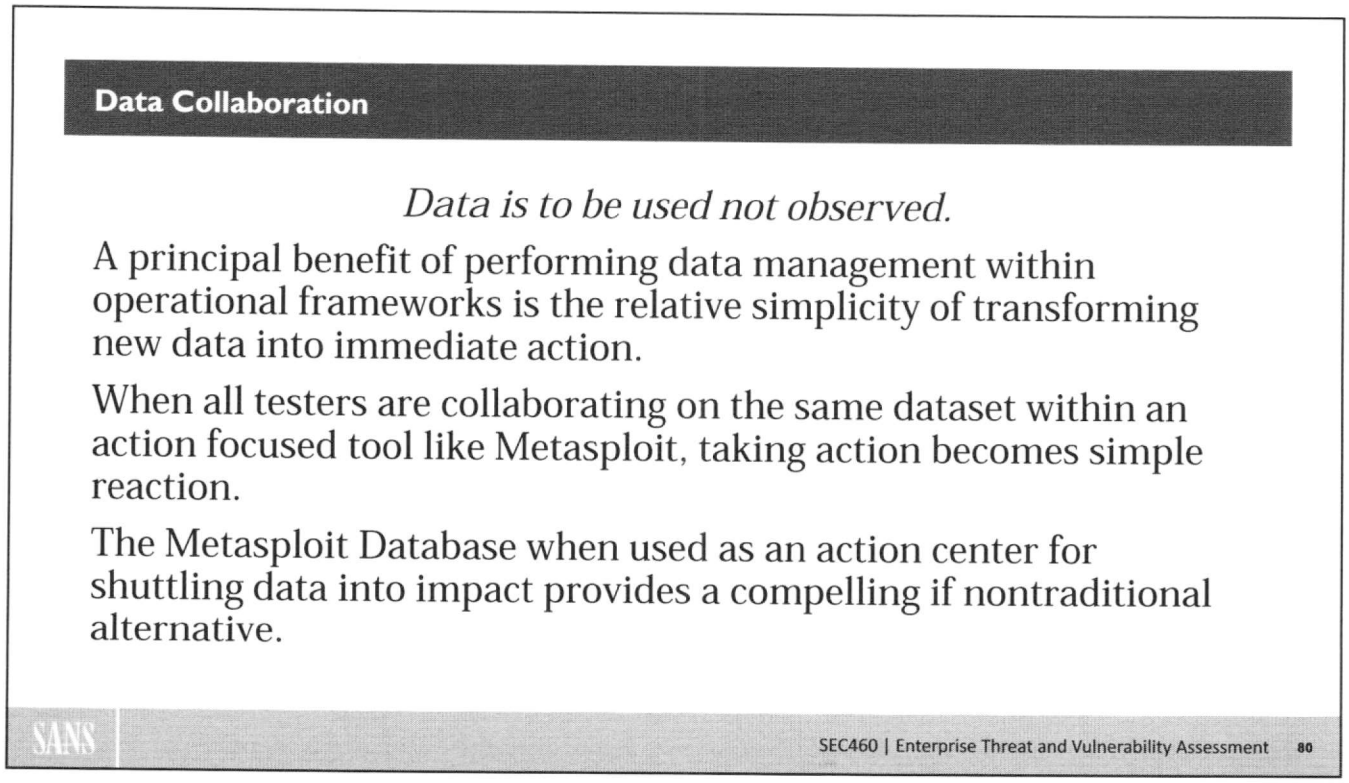
2. Search
- Acheron is built around search in order to inform and enhance rapid data analysis
- Your own personal Google to empower Prioritization, Triage, Remediation, and Reporting

3. Automate & Analyze
- Incorporate authorized system/software inventories and watch them update based on real world data
- Automated correlation of vulnerability data to organization specific threats

4. Data Management
- Track, categorize, and remediate vulnerabilities
- Triage and assign risk ratings

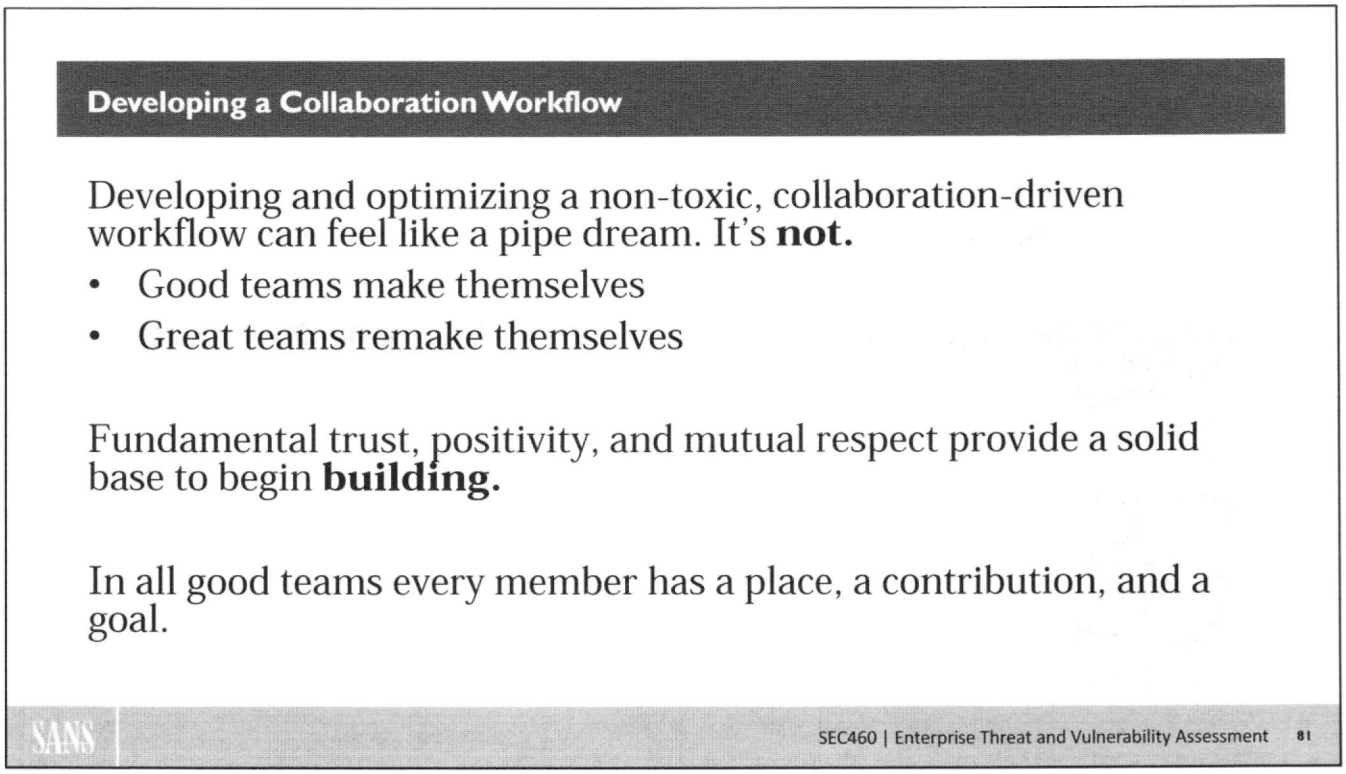
5. Terminal Extensibility
- All data managed by Acheron can be accessed directly from the command line through both Bash and PowerShell
- This enables rapid remediation opportunity and infinite yet simplistic extensibility

Acheron supports many OS and CPU builds via system agnostic design choices; however, it must be built to accommodate each. This (the main project archive) contains binary distributions for all major OS/CPU builds. It also contains all src/dev files. This design was chosen so that anyone can download the main archive and use the tool. For leaner, OS Specific builds, see the Binary Distribution Repository: [dist](https://github.com/Acheron-VAF/Acheron-Dist)



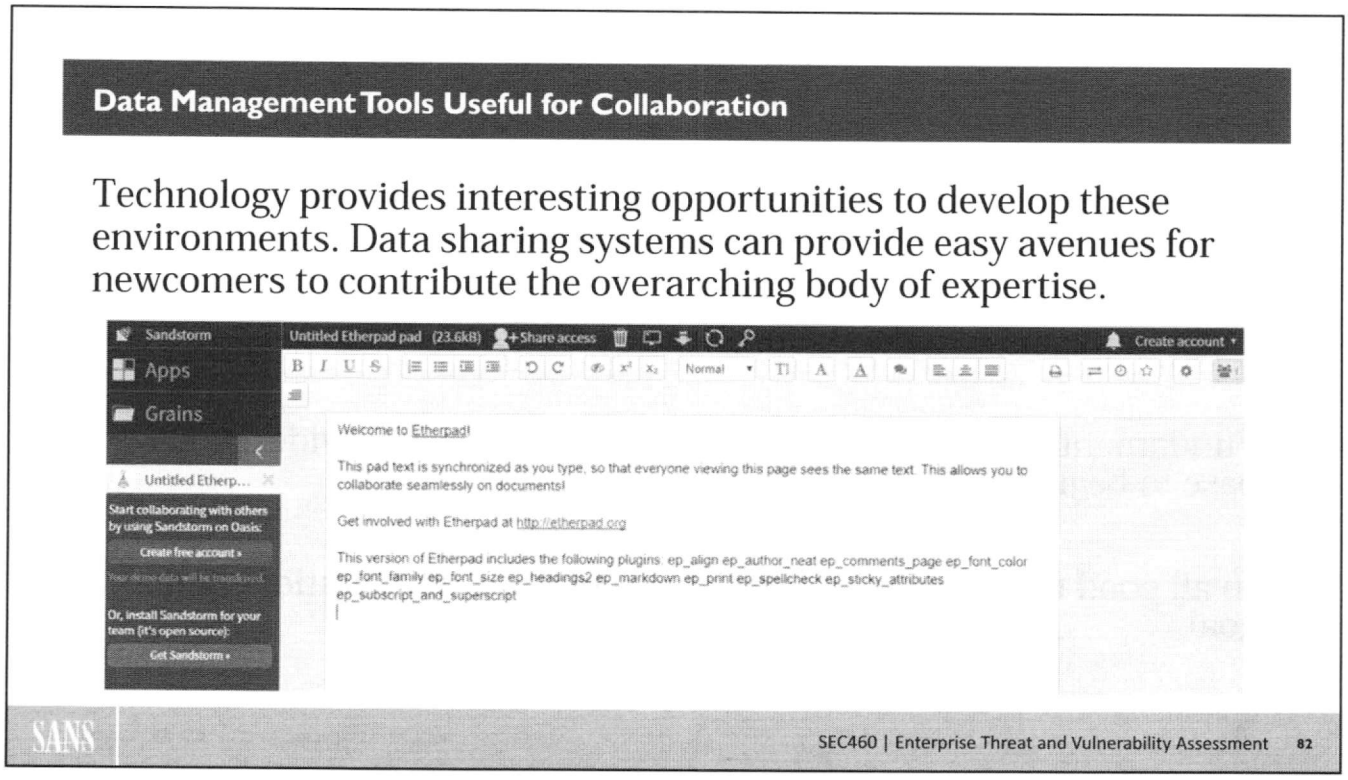
Data Collaboration

Data is to be used not observed. A principal benefit of performing data management within operational frameworks is the relative simplicity of transforming new data into immediate action. When all testers are collaborating on the same dataset within an action focused tool like Metasploit, taking action becomes simple reaction. The Metasploit Database when used as an action center for shuttling data into impact provides a compelling if nontraditional alternative.



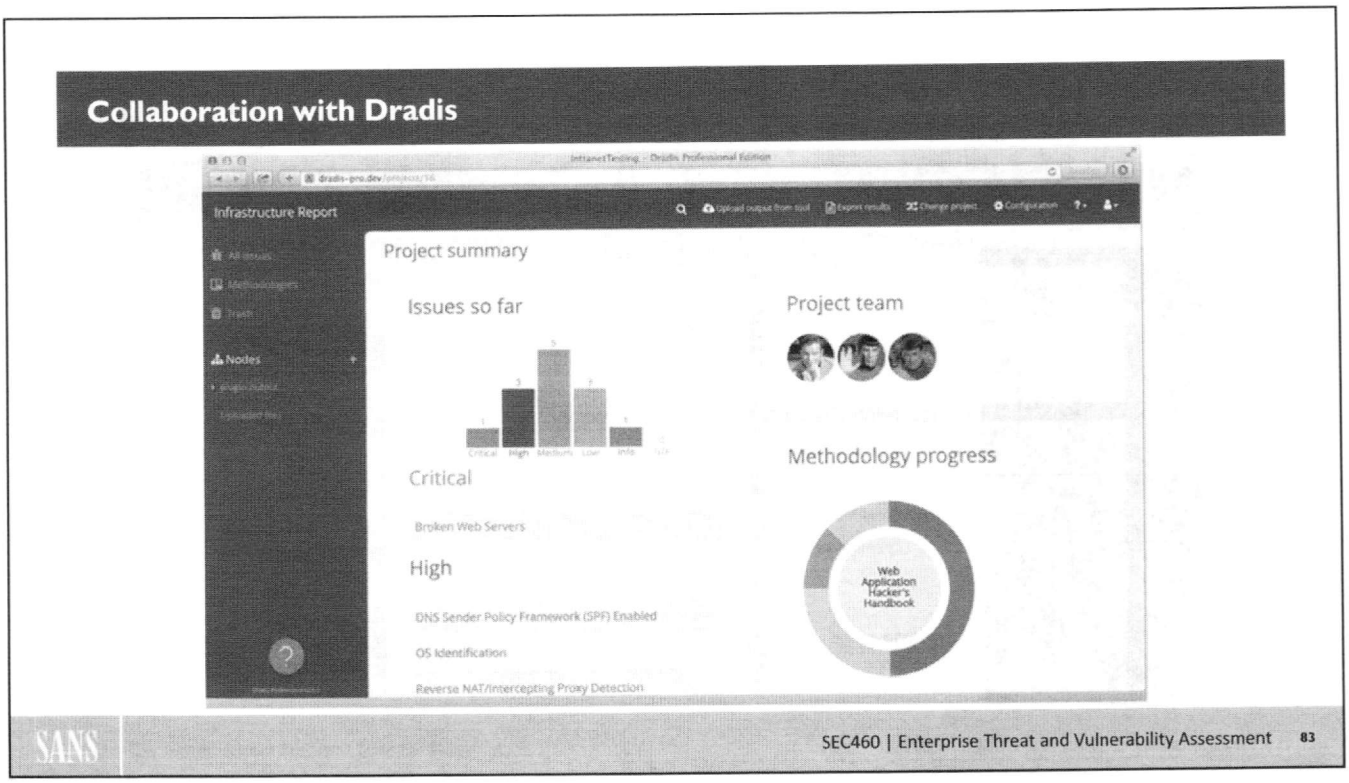
Developing a Collaboration Workflow

Honing a set of good habits and a healthy lifestyle can be challenging, personally. Developing and optimizing a non-toxic, collaboration-driven workflow can feel like a pipe dream. A positive environment focused on individual and team growth can provide a sure path forward. For the team to develop the mutual respect required for this to become relative everyone must contribute.



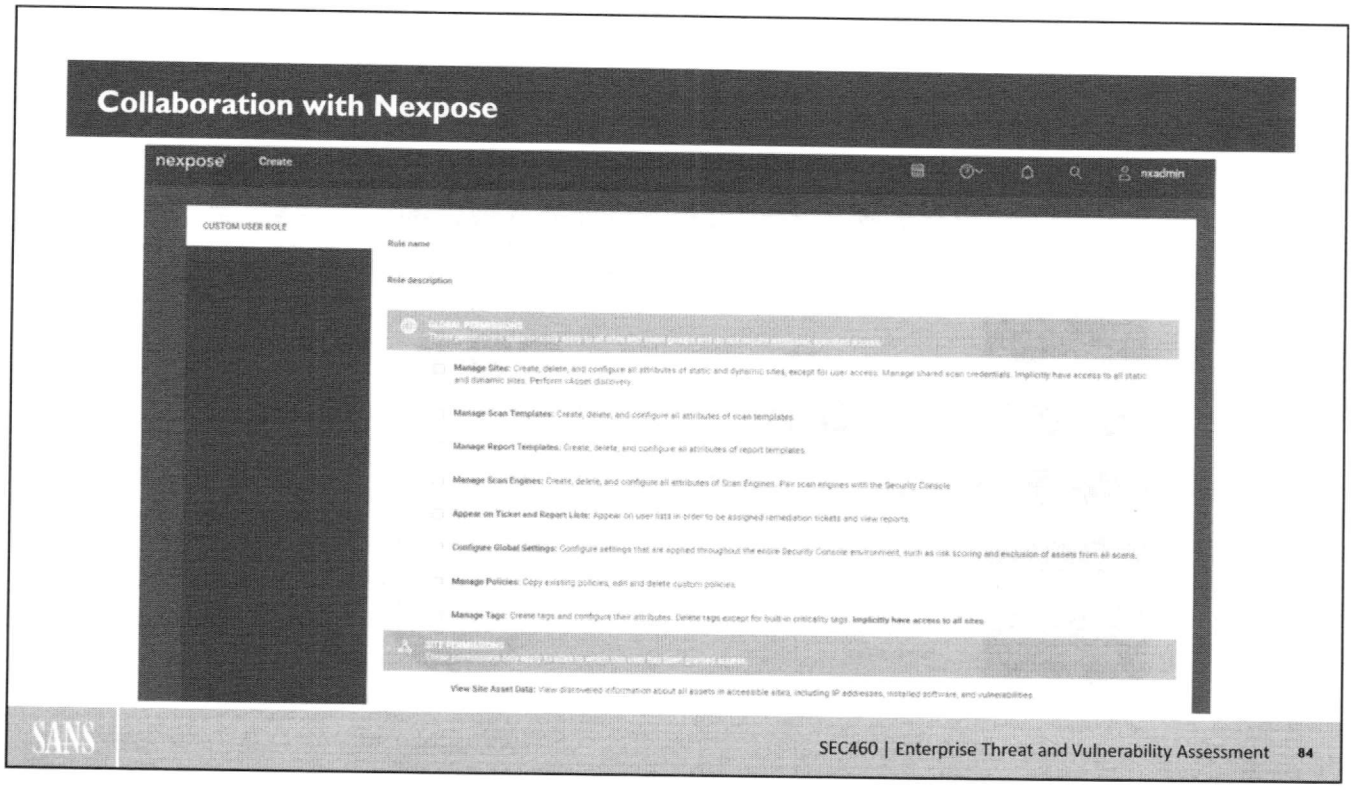
Data Management Tools Useful for Collaboration

Technology provides interesting opportunities to develop these environments. Data sharing systems can provide easy avenues for newcomers to contribute the overarching body of expertise. Document collaboration systems like Etherpad and Google Docs allow for seamless data sharing. People are great at pattern recognition and replication. Even newcomers to information security, when given examples, are happy to contribute in like kind. The open source community is a flourishing example.



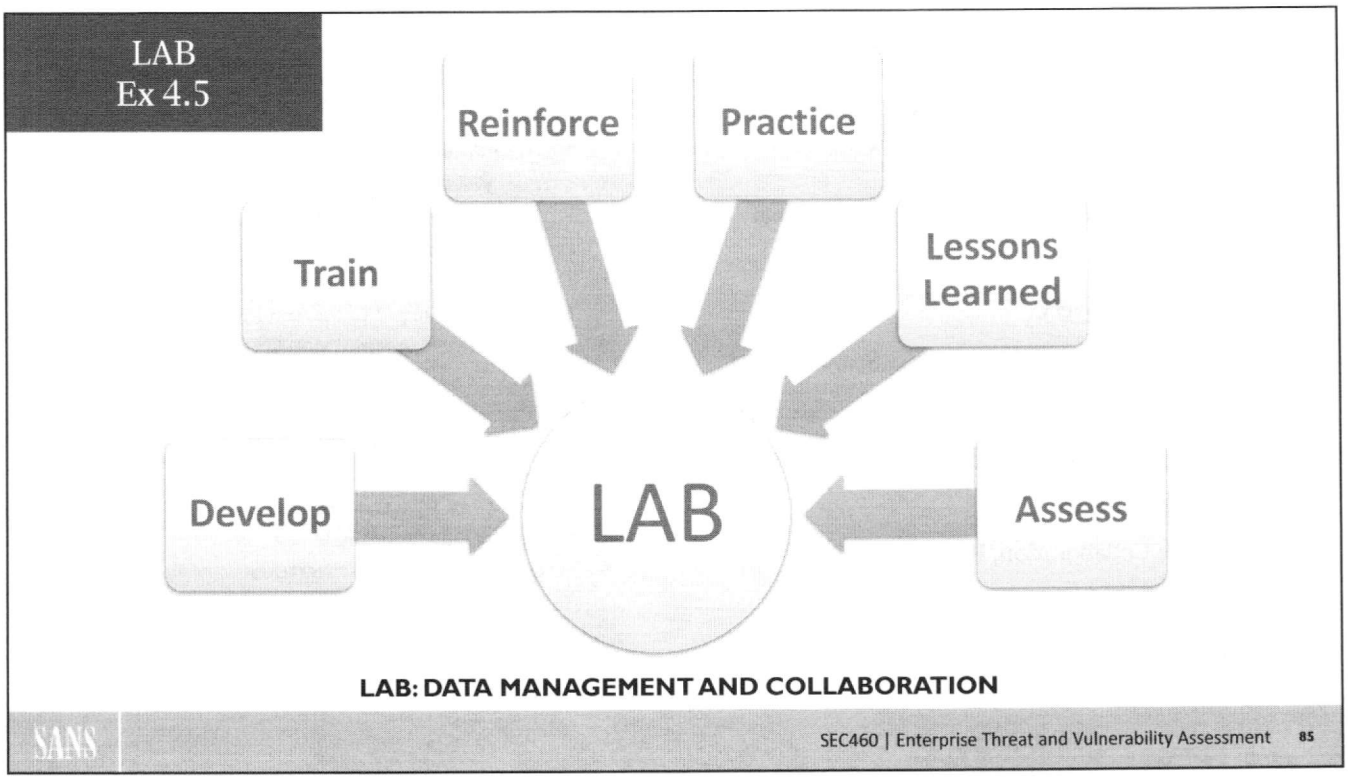
Collaboration with Dradis

Although Dradis has open source roots and remains a vulnerability focused tool that has output type integration, its new professional features also include project management and collaboration features.



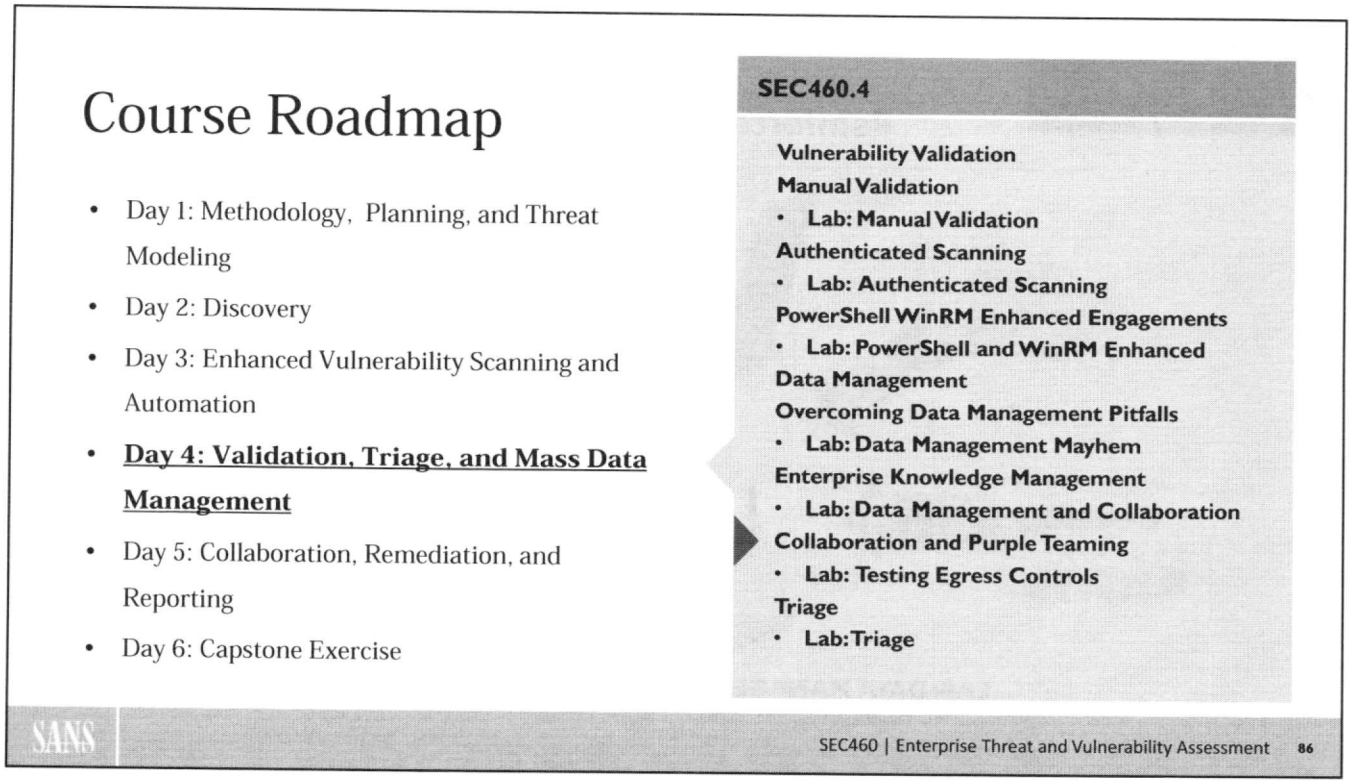
Collaboration with Nexpose

Robust tools like Nexpose can even include user management features and controls to allow for fine-grained team administration.



LAB: Data Management and Collaboration

Please refer to the Wiki for Exercise 4.5.



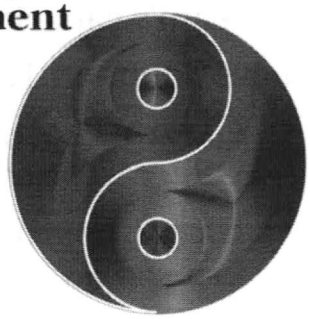
Course Roadmap: Purple Teaming

Red teams improve the blue team, the blue team challenges red. The meddling of these two is the genesis of purple teams. Purple teams exist to straddle both sides of the fence and serve the purpose of continuous improvement and development of both functions.

The Importance of Collaboration

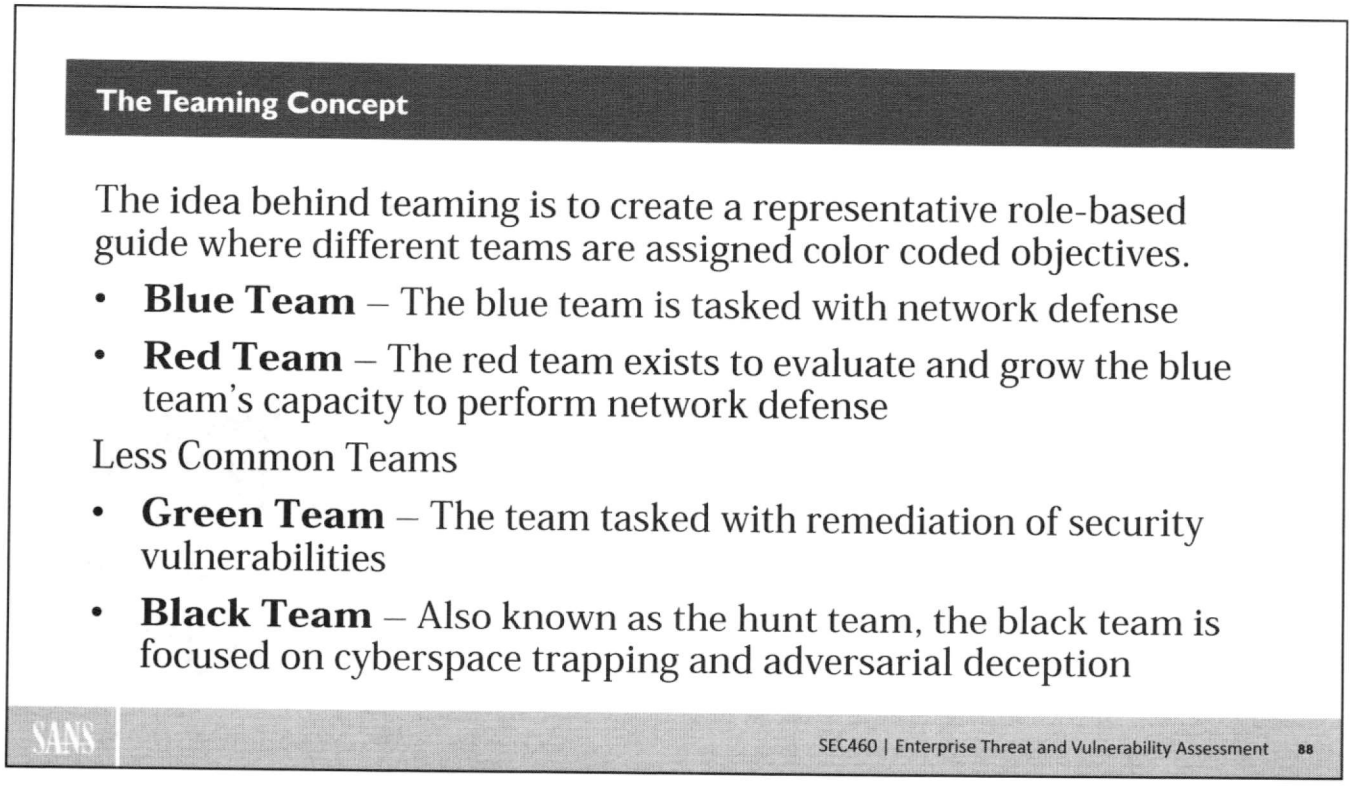
When attack meets defense and learning is achieved the whole is greater than the sum of its parts.

Red Teams attack, **Blue Teams** defend -- but they share a common goal: **Continuous Security Improvement**



The Importance of Collaboration

When attack meets defense and learning is achieved the whole is greater than the sum of its parts. **Red Teams** attack, **Blue Teams** defend -- but they share a common goal: **Continuous Security Improvement**



The Teaming Concept

The idea behind teaming is to create a representative role-based guide where different teams are assigned color coded objectives

- **Blue Team** – The blue team is tasked with network defense
- **Red Team** – The red team exists to evaluate and grow the blue team's capacity to perform network defense

Less Common Teams

- **Green Team** – The team tasked with remediation of security vulnerabilities
- **Black Team** – Also known as the hunt team, the black team is focused cyberspace trapping and adversarial deception

The Teaming Concept

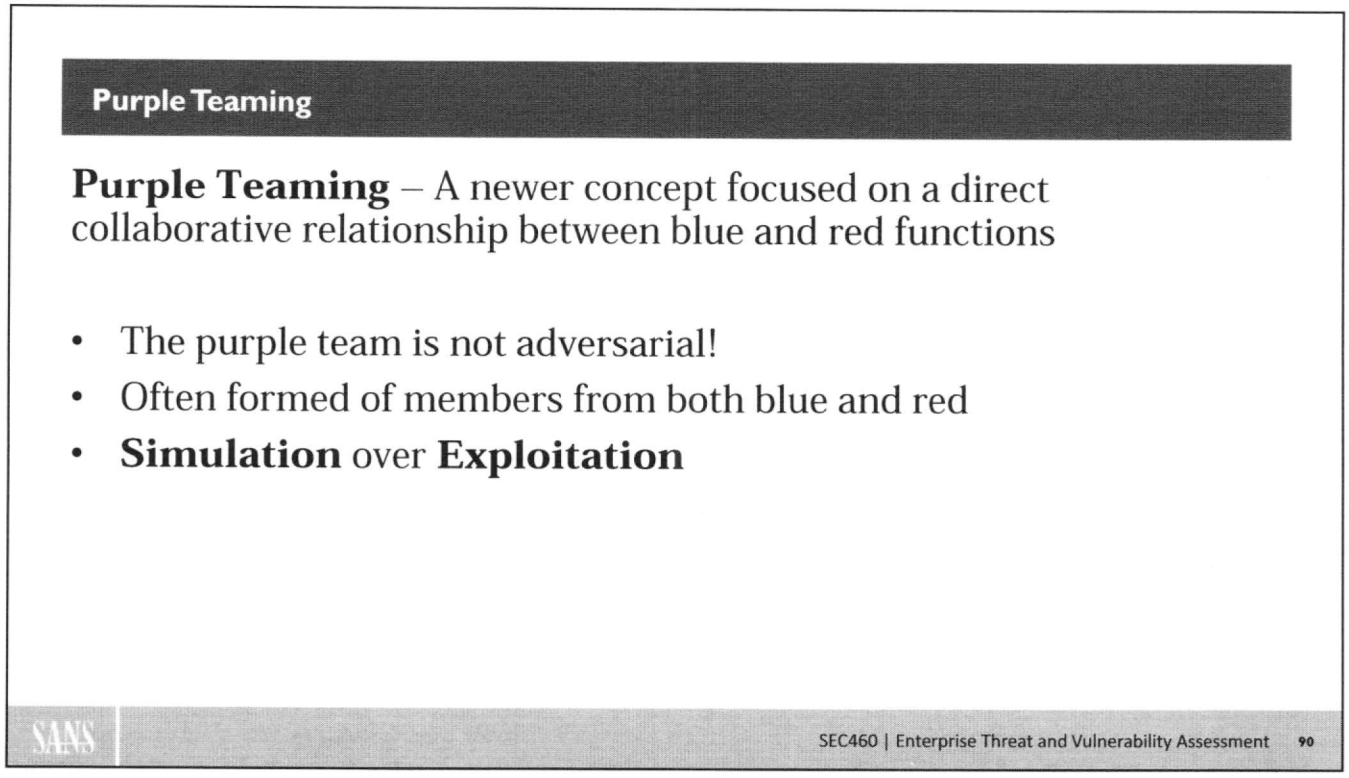
Non-participative groups essential to facilitating the teaming objective are referred to as cells.

- **White Cell** – The white cell's purpose is to enable the teaming event by acting as the intercessor between red and blue teams, validating findings and ensuring system availability
- **Gray Cell** – The gray cell simulates an unwitting user or occasionally an insider threat. Gray cell's role adds realism to the network exercise and facilitates blue team growth by aiding red team exploitation

The Teaming Concept

Non-participative groups essential to facilitating the teaming objective are referred to as cells

- **White Cell** – The white cell's purpose is to enable the teaming event by acting as the intercessor between red and blue teams, validating findings and ensuring system availability
- **Gray Cell** – The gray cell simulates an unwitting user or occasionally an insider threat. Gray cell's role adds realism to the network exercise and facilitates blue team growth by aiding red team exploitation

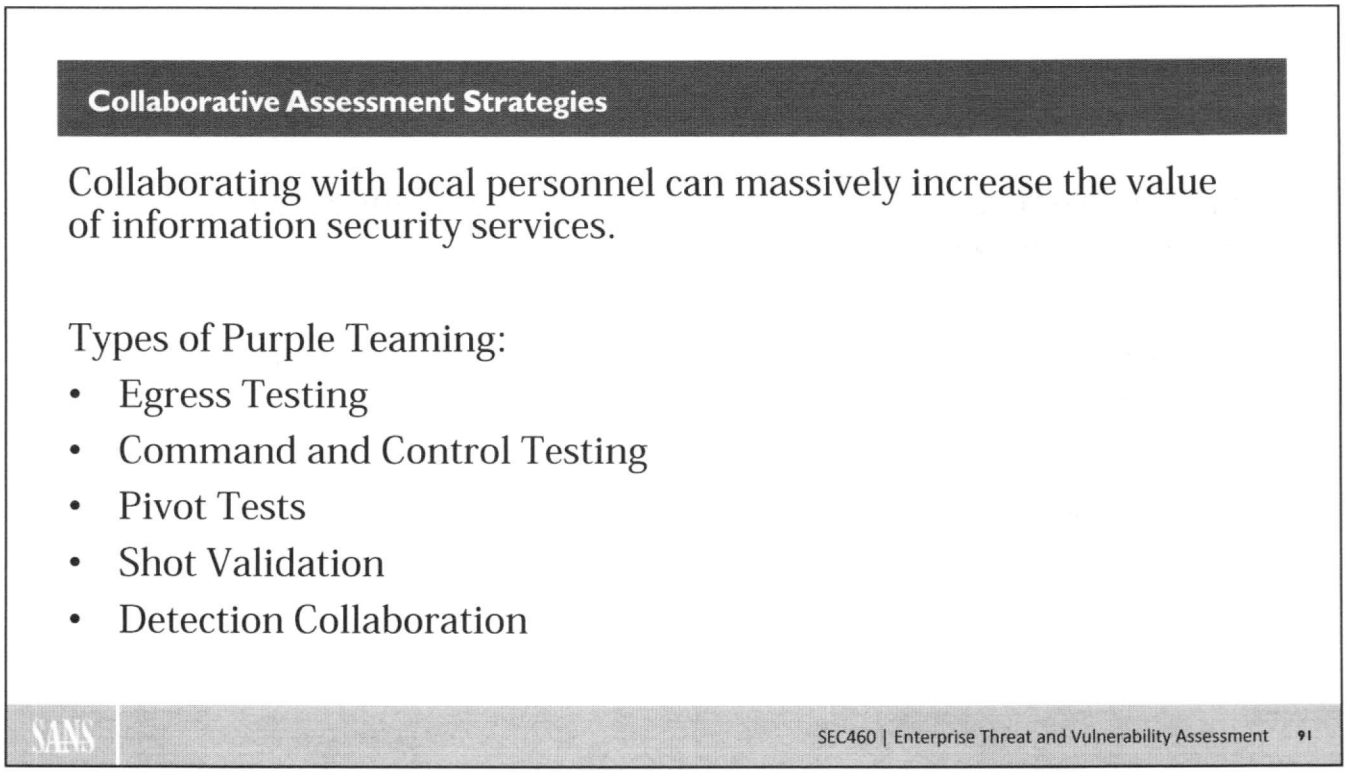


Purple Teaming

A purple team exists to facilitate knowledge transfer between both red and blue functions. The end result is a healthy attack/defense culture focused on iterative growth.

Purple Teaming is a newer concept focused on a direct collaborative relationship between blue and red functions

- The purple team is not adversarial!
- Often formed of members from both blue and red
- **Simulation** over **Exploitation**

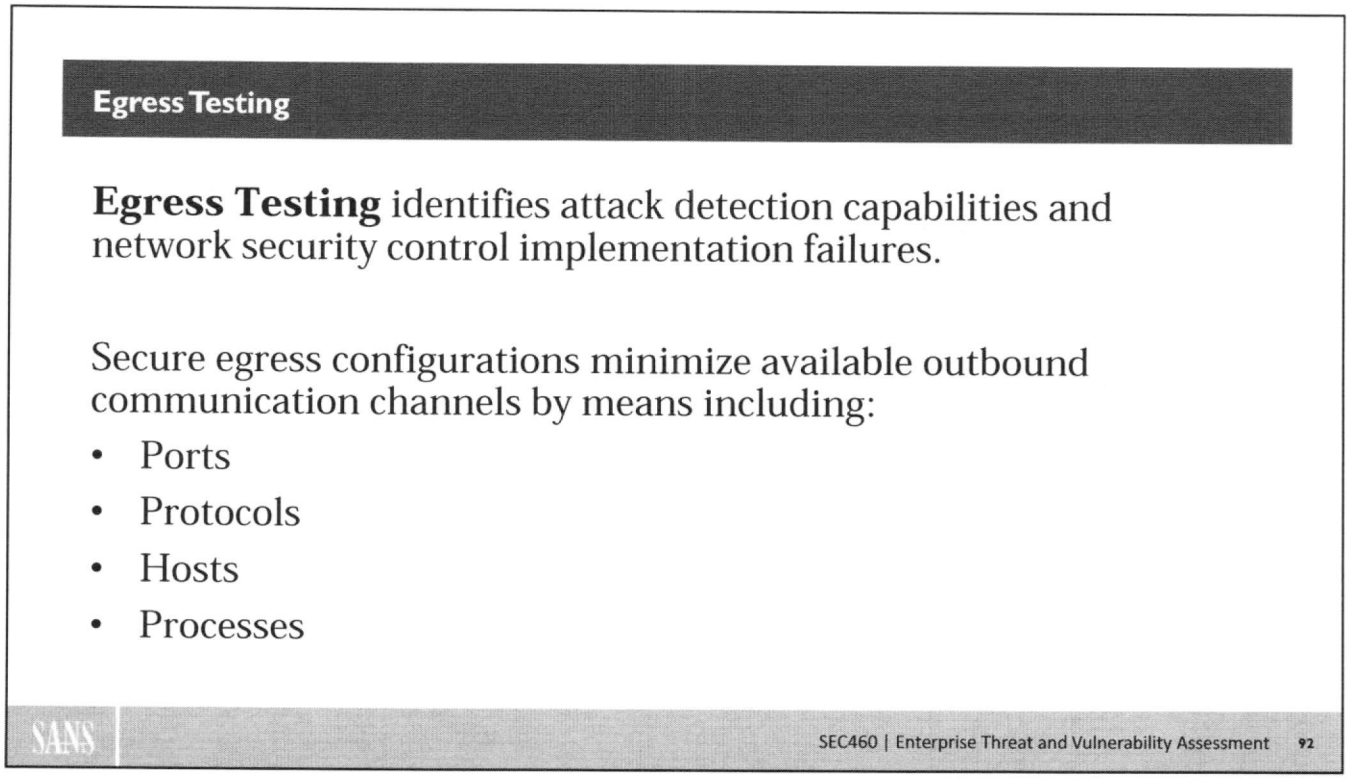


Collaborative Assessment Strategies

Collaborating with local personnel can massively increase the value of information security services

Types of Purple Teaming:

- Egress Testing
- Command and Control Testing
- Pivot Tests
- Shot Validation
- Detection Collaboration

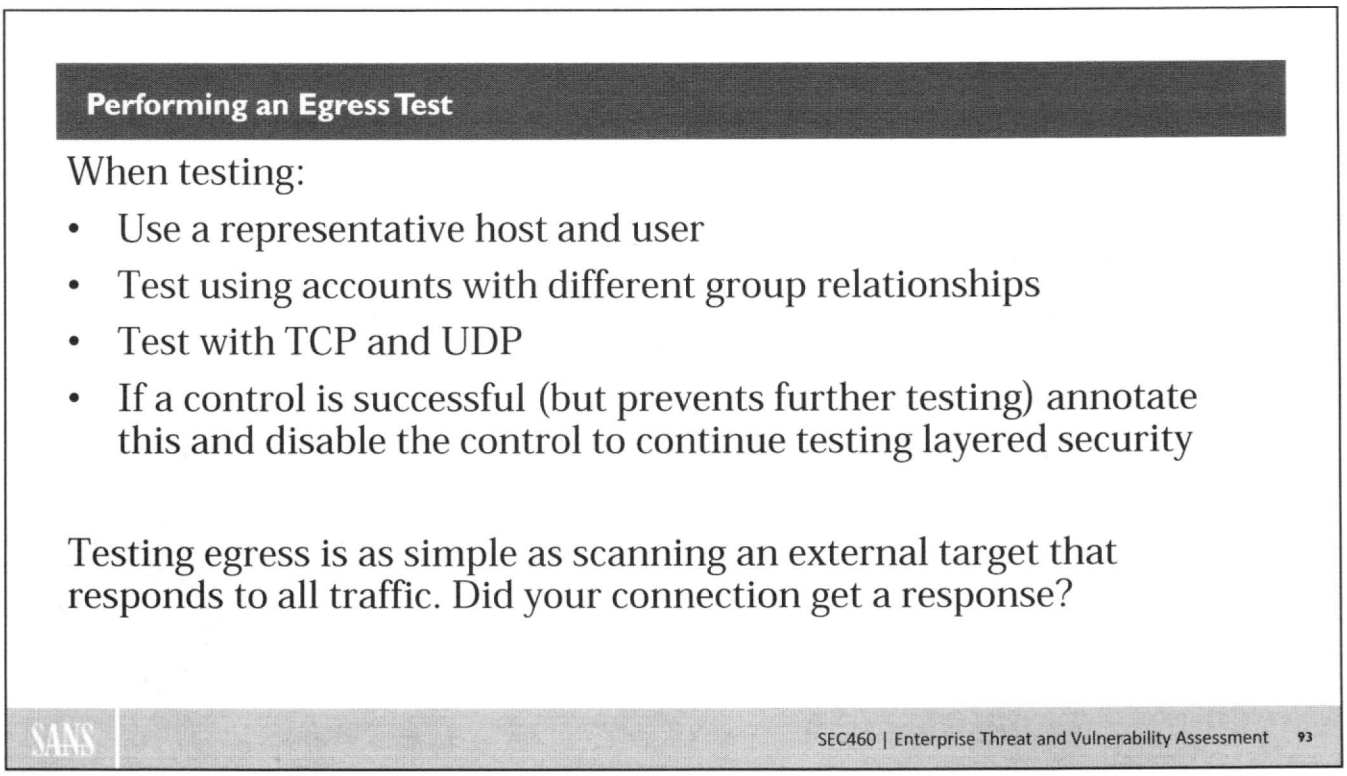


Egress Testing

Egress Testing identifies attack detection capabilities and network security control implementation failures

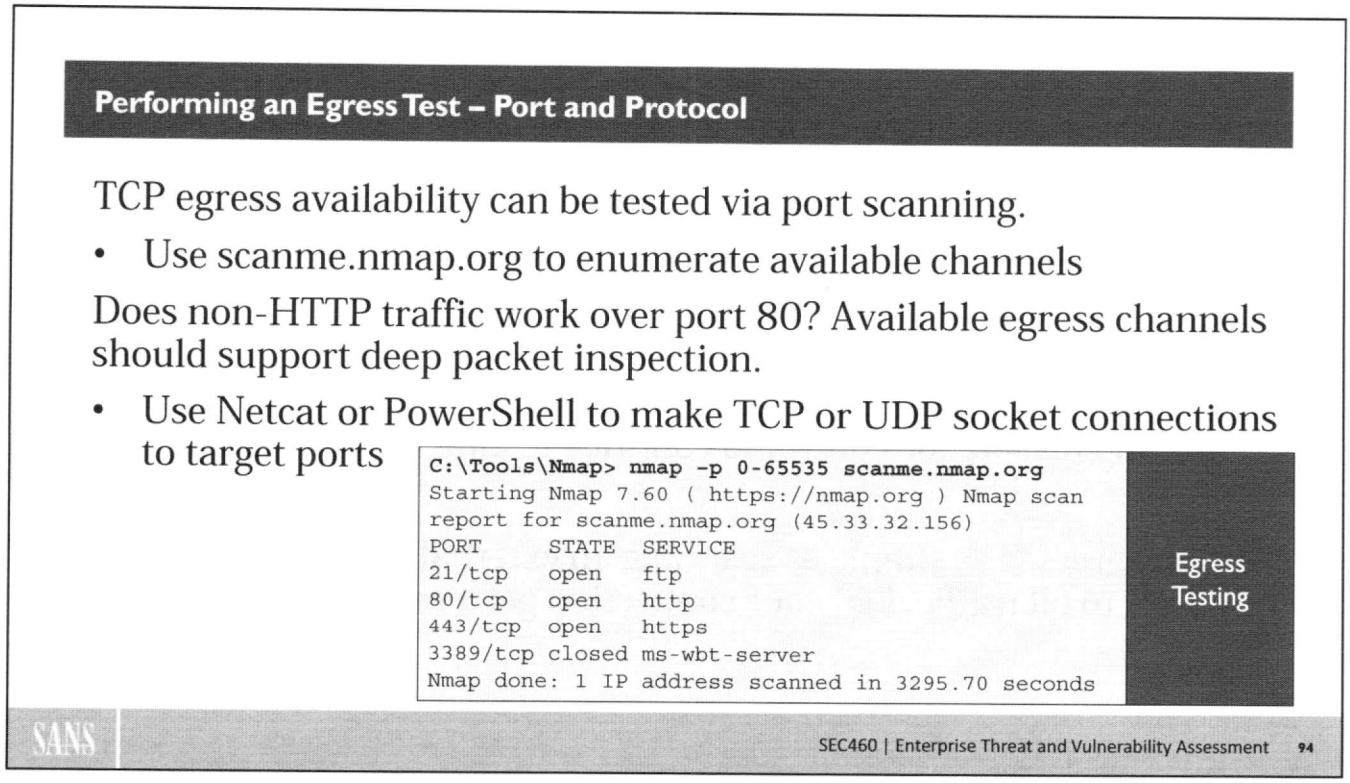
Secure egress configurations minimize available outbound communication channels by means including:

- Ports
- Protocols
- Hosts
- Processes



Performing an Egress Test

Use a representative host and user to perform testing. It may be advisable to conduct tests as users from differentiated groups to ensure full coverage.



Performing an Egress Test – Port and Protocol

Performing an Egress Test – Host and Process

Not all systems should be allowed to connect to certain services on the internet.

- Only admins should have access to network management protocols and only if necessary
- SCADA or otherwise sensitive systems should be heavily restricted to include access to HTTP and HTTPs

Processes should be similarly restricted. Network access for specific processes can be restricted using the Windows firewall.

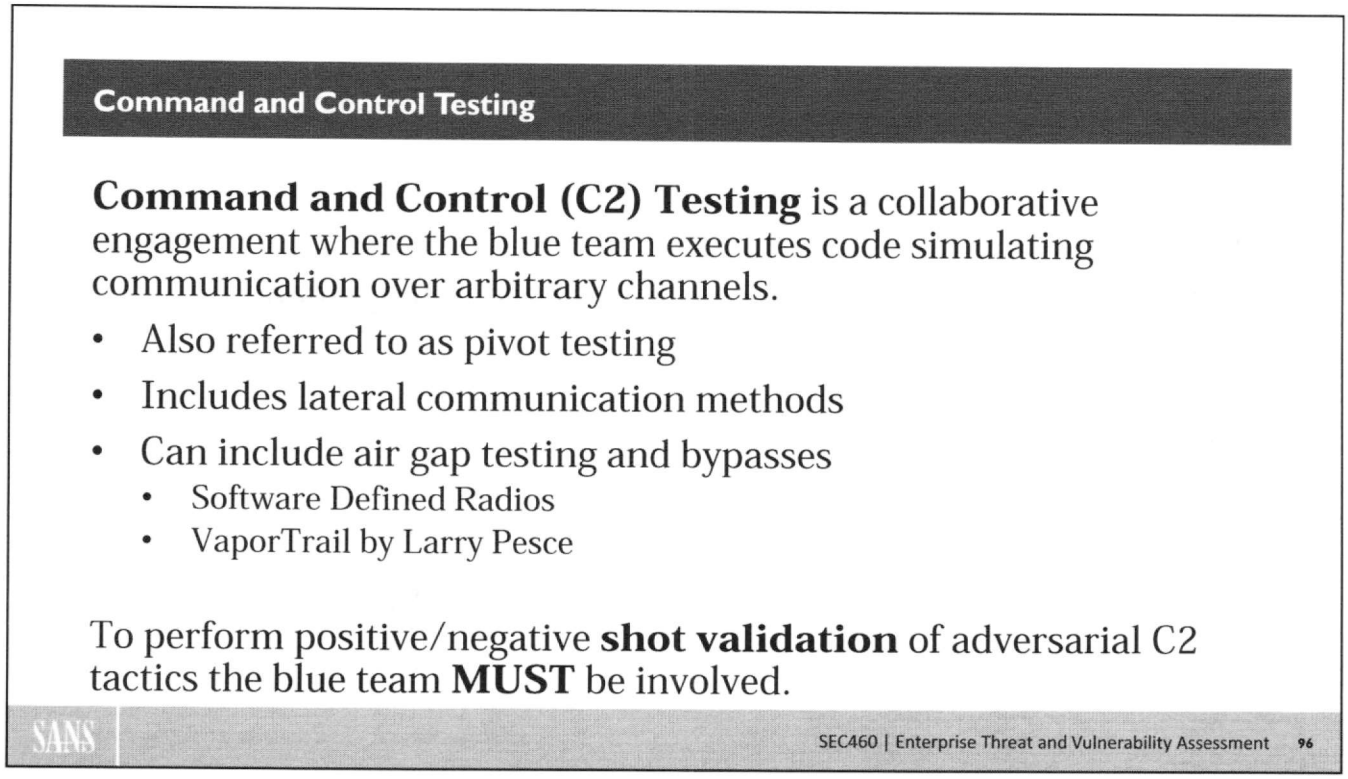
```
C:\> netsh advfirewall firewall add rule
name="Block PowerShell Networking" dir=in
action=deny program="C:\program\powershell.exe"
enable=yes
```

Netsh Process Restriction

Performing an Egress Test – Host and Process

Not all systems should be allowed to connect to certain services on the internet. Only admins should have access to network management protocols and only if necessary. SCADA or otherwise sensitive systems should be heavily restricted to include access to HTTP and HTTPs. Processes should be similarly restricted. Network access for specific processes can be restricted using the Windows firewall. Remember, least privilege. Modeling your legitimate users to identify pattern of life behaviors, is the first step toward detection of anomalous behaviors and can be a giant leap forward for a dedicated security team.

C:\> netsh advfirewall firewall add rule name="Block skype" dir=in action=deny program="C:\program\skype.exe" enable=yes



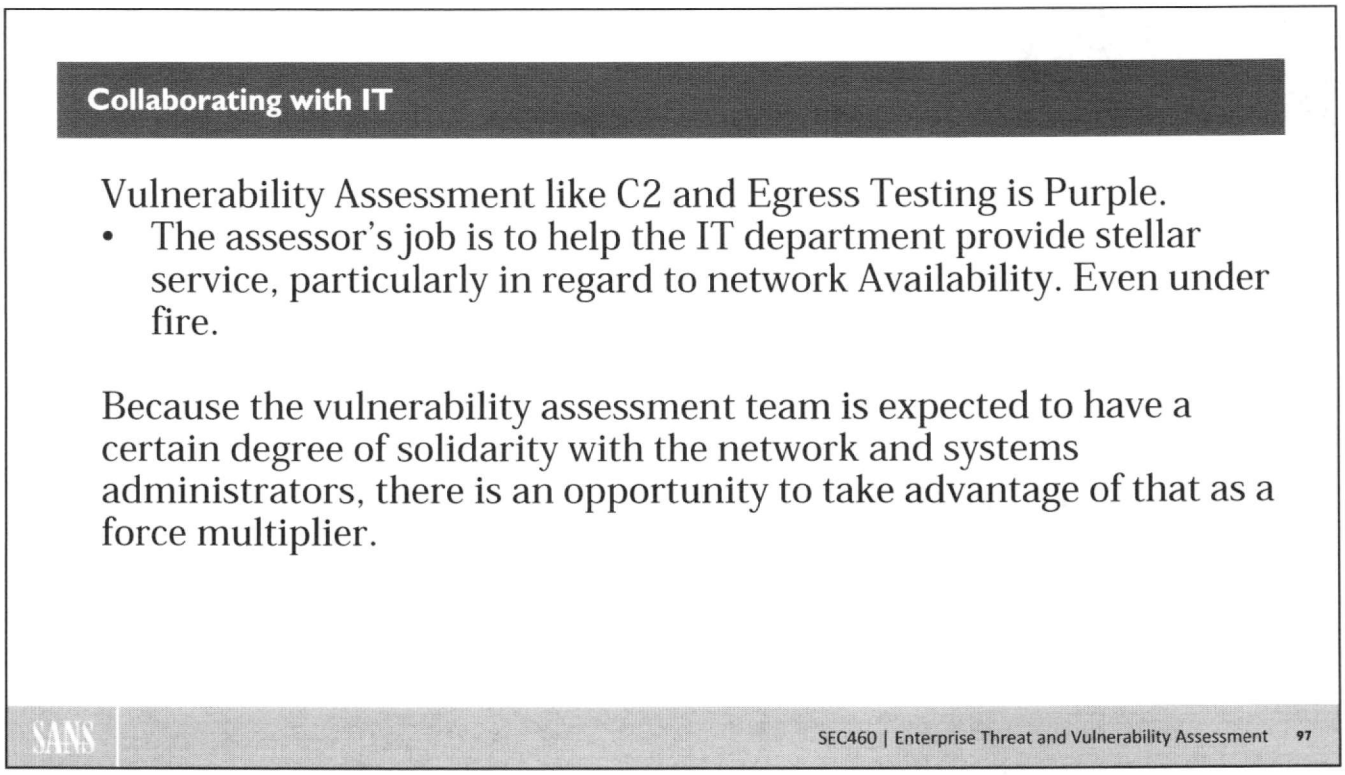
Command and Control Testing

Command and Control (C2) Testing is a collaborative engagement where the blue team executes code simulating communication over arbitrary channels. It is also occasionally referred to as pivot testing and can (but does not always) include lateral movement techniques and covert communication channels. These tests **MUST** be collaborative in nature. The security tester performs a sequence of **local execution** and remote **command and control** tactics that a threat actor may attempt to use during a cyber-attack.

The goal is three-fold:

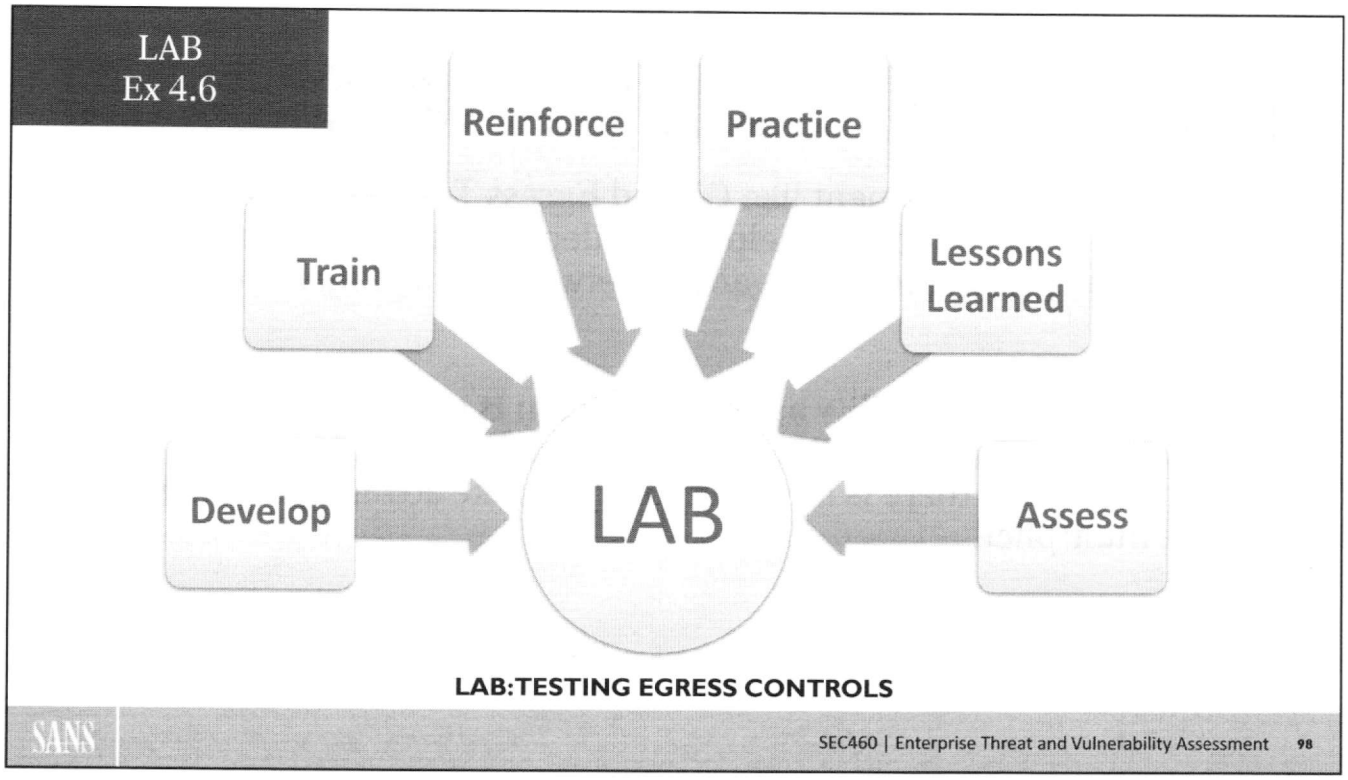
1. Technically speaking, which techniques worked. Which ones didn't. Why?
2. If it worked did the blue team detect it? Which tools/techniques were used in detection? Should those defensive tactics receive increase emphasis in the future?
3. If worked, but was not detected, why? What could an attacker with this level of undetected access do? What would he do next?

A focused security strategy forms and endless cycle of if/than wargames where the blue team, empowered by the red team, has the opportunity to establish a home-field advantage within their cyber-turf. This process of fire and evaluate is called **shot validation.**



Collaborating with IT

Vulnerability Assessment like C2 and Egress Testing is a purple service. The assessor's job is to help the IT department provide stellar service, particularly in regard to network Availability. Even under fire. Because the vulnerability assessment team is expected to have a certain degree of solidarity with the network and systems administrators, there is an opportunity to take advantage of that facet and use it as a force multiplier.



LAB: Testing Egress Controls

Please refer to the Wiki for Exercise 4.6.

Course Roadmap

- Day 1: Methodology, Planning, and Threat Modeling
- Day 2: Discovery
- Day 3: Enhanced Vulnerability Scanning and Automation
- **Day 4: Validation, Triage, and Mass Data Management**
- Day 5: Collaboration, Remediation, and Reporting
- Day 6: Capstone Exercise

SEC460.4

Vulnerability Validation
Manual Validation
- **Lab: Manual Validation**

Authenticated Scanning
- **Lab: Authenticated Scanning**

PowerShell WinRM Enhanced Engagements
- **Lab: PowerShell and WinRM Enhanced**

Data Management
Overcoming Data Management Pitfalls
- **Lab: Data Management Mayhem**

Enterprise Knowledge Management
- **Lab: Data Management and Collaboration**

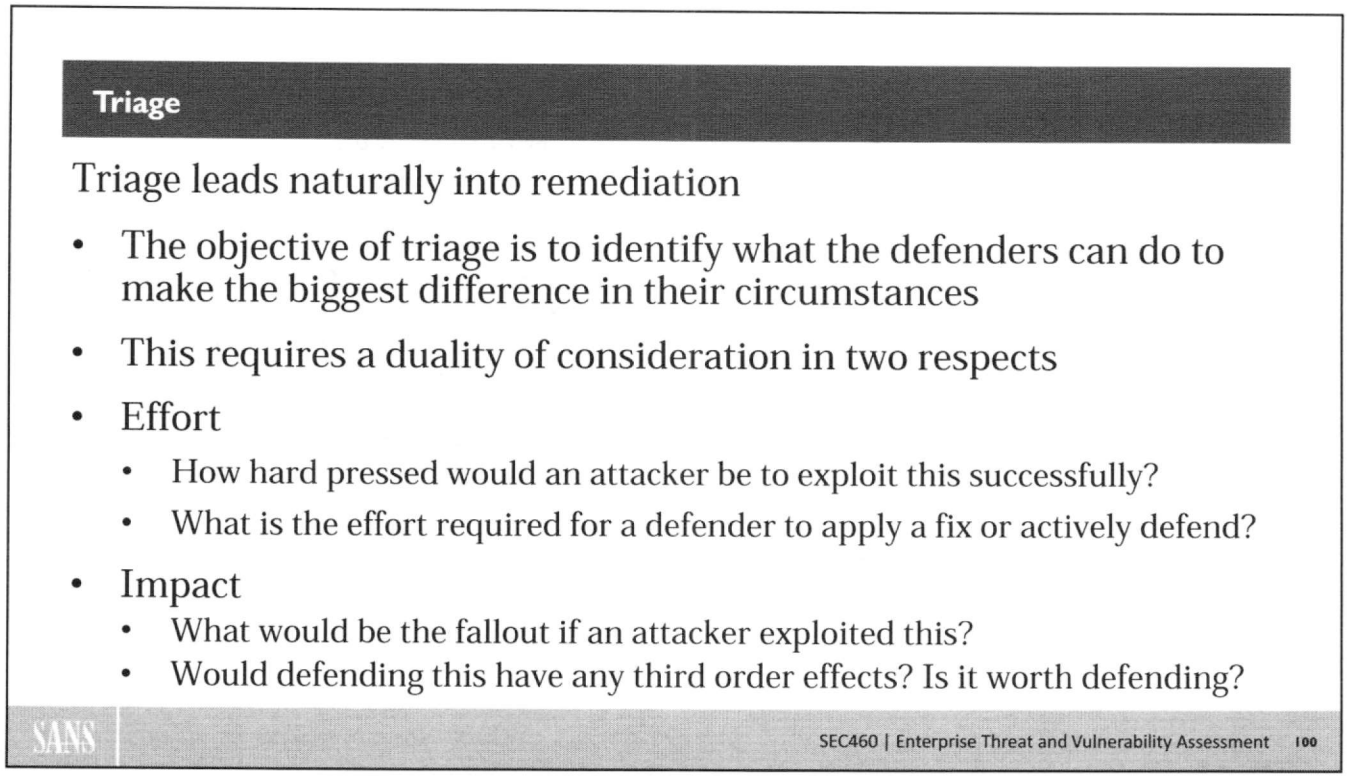
Collaboration and Purple Teaming
- **Lab: Testing Egress Controls**

Triage
- **Lab: Triage**

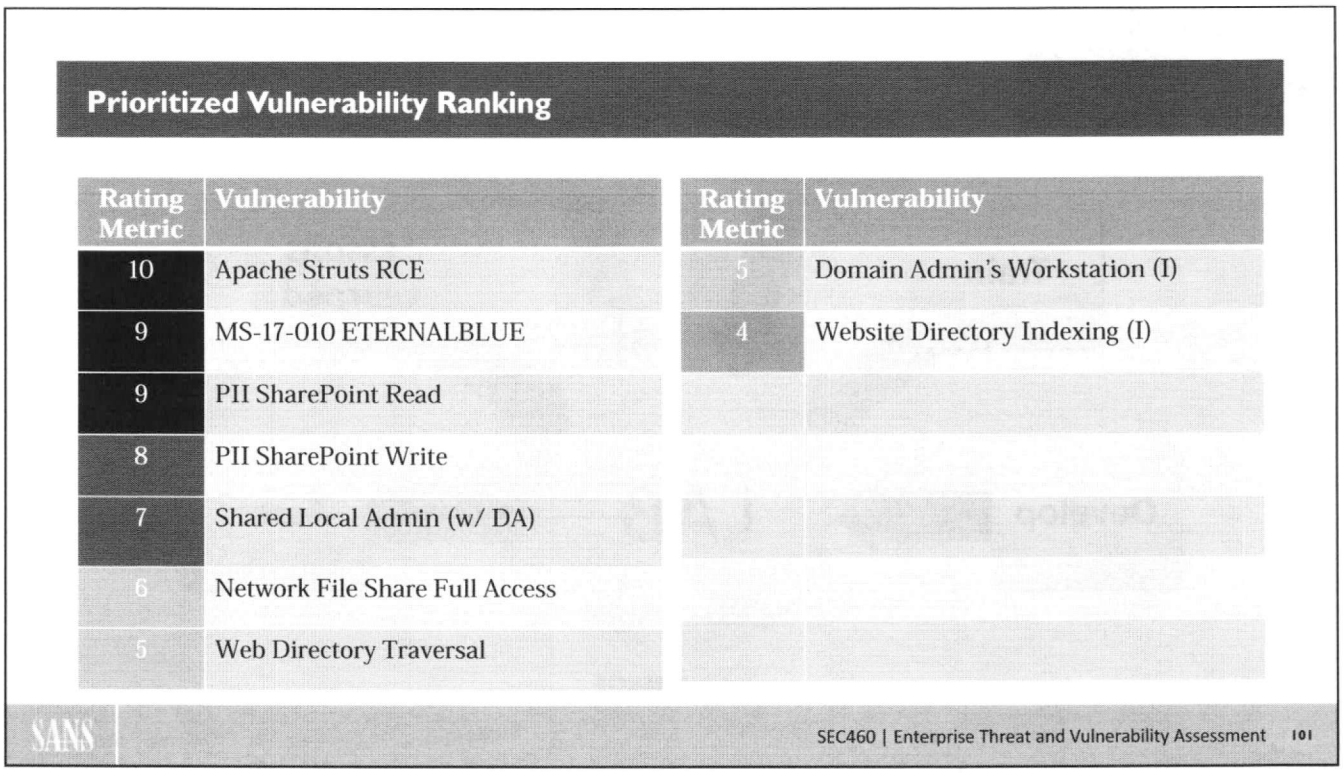
SANS

SEC460 | Enterprise Threat and Vulnerability Assessment 99

This page intentionally left blank.

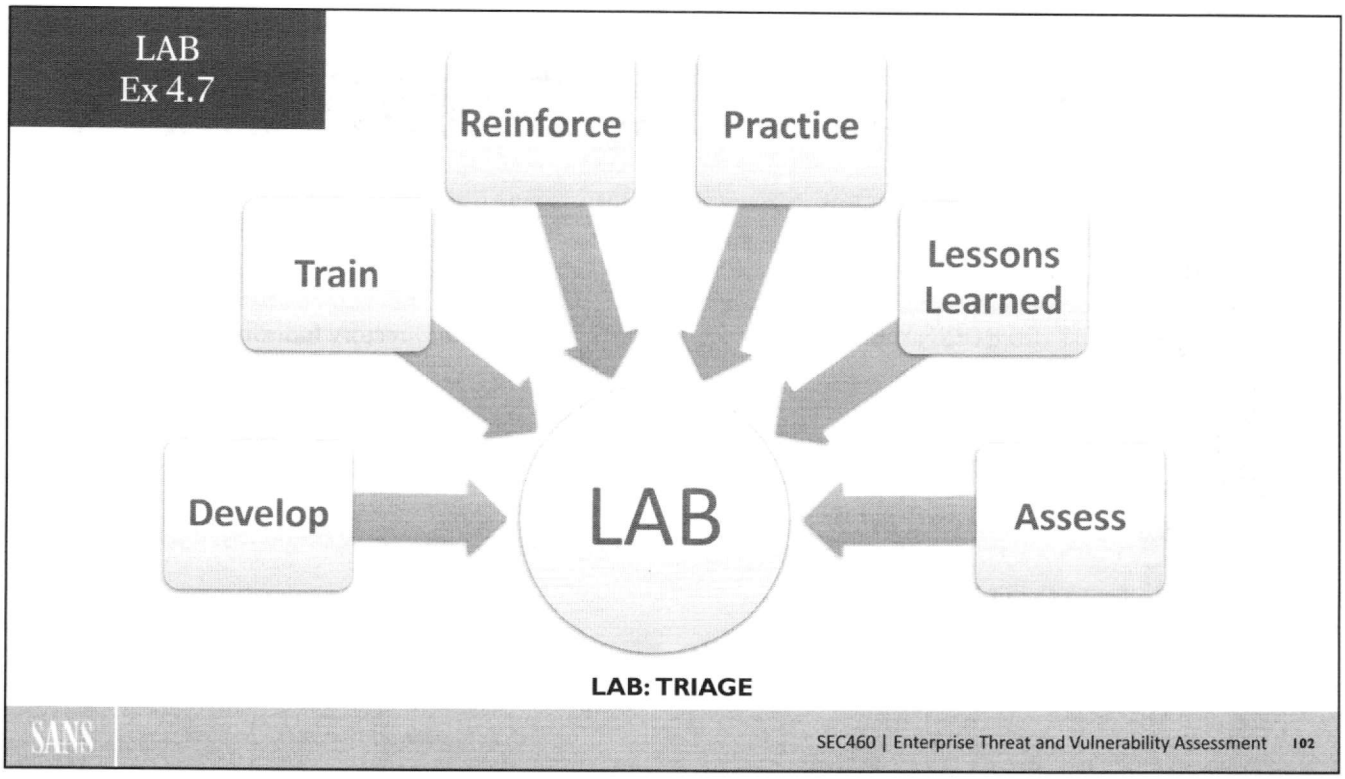


Triage
Triage leads naturally into remediation but requires careful consideration due to its duality of focus it two opposing respects. What is the effort required to attack/defend? What is the impact if attacked/defended.



Prioritized Vulnerability Ranking

A prioritized ranking of security conditions to be remediated is the output of triage.



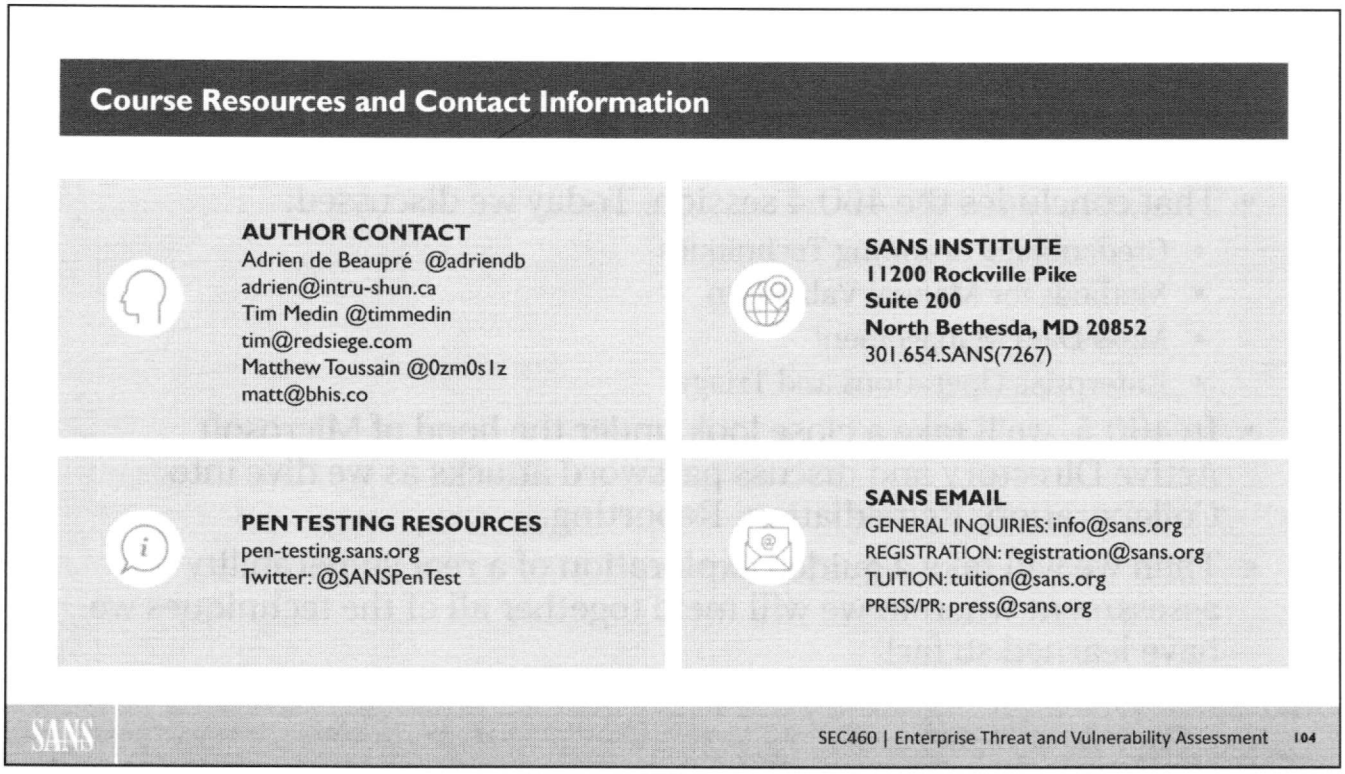
LAB: Triage

Please refer to the Wiki for Exercise 4.7.

Conclusion for 460.4

- That concludes the 460.4 session. Today we discussed:
  - Credentialed Scanning Techniques
  - Methods for Manual Validation
  - Mass Data Management
  - Enterprise Operations and Triage
- In 460.5, we'll take a close look under the hood of Microsoft Active Directory and discuss password attacks as we dive into Collaboration, Remediation, Reporting.
- Then we will take a guided exploration of a real vulnerability assessment wherein we will meld together all of the techniques we have learned so far!

This page intentionally left blank.



Course Resources and Contact Information

Please feel free to reach out to the course authors:

Adrien de Beaupré	@adriendb	adrien@intru-shun.ca
Tim Medin	@TimMedin	tim@redsiege.com
Matthew Toussain	@0zm0s1z	matt@bhis.co