FRSecure CISSP Mentor Program

2023

Class #9 – Domain 6

Ryan Cloutier
President of SecurityStudio & vCISO
Infosec Missionary on a Mission

CISSP® MENTOR PROGRAM – SESSION THREE

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.

- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.

- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.

- Failure to abide by the rules may result in disabling chat for you.

- Do not copy or share copy of copyrighted materials.

CISSP® MENTOR PROGRAM – SESSION SIX

WHO I AM?

I love Baby Yoda

Outside of being a security practitioner focused on helping businesses tackle their cybersecurity risks while minimizing friction resulting in increased resiliency and helping to secure people and processes with a solid understanding of the technology involved.

I am a dad, dog dad and career coach. I love helping other to achieve their best. Through this channel, I help veterans with their transitions and others via non-profits like Whole Cyber Human Initiative, Boots2Books and others.

I give back by producing a podcast focused on helping people who are "Breaking into Cybersecurity" by sharing the stories of those who have done it in the past 5 years to inspire those looking to do it now.

Co-authored:
"Develop Your Cybersecurity Career Path: How to Break into Cybersecurity at Any Level"
"Hack the Cybersecurity Interview: A complete interview preparation guide for jumpstarting your cybersecurity career"
And advised on "Understand, Manage, and Measure Cyber Risk"

Do or do not, there is no try

Boomer, ok

Listen here you little s**t

LET'S DO THIS!

And here we go again...

Domain 6: Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)

Page 419

WHAT ARE WE GOING TO COVER?

Agenda – Domain 6: Security Assessment and Testing

(Designing, Performing, and Analyzing Security Testing)

- DESIGN AND VALIDATE ASSESSMENT, TEST, AND
- AUDIT STRATEGIES
- CONDUCT SECURITY CONTROL TESTING
- COLLECT SECURITY PROCESS DATA
- ANALYZE TEST OUTPUT AND GENERATE
- REPORT
- CONDUCT OR FACILITATE SECURITY AUDITS

Starting on page 419 this evening

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Unique Terms and Definitions

- Dynamic Testing – Tests code while executing it
- Fuzzing – A type of black box testing that submits random, malformed data as inputs into software programs to determine if they will crash
- Penetration Testing – Authorized attempt to break into an organization's physical or electronic perimeter (and sometimes both)
- Static Testing – Tests code passively: the code is not running.
- Synthetic Transactions – Also called synthetic monitoring: involves building scripts or tools that simulate activities normally performed in an application

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Assessment and testing are critical.

- Accurately assess real-world security.
- How do you know where to start, unless you've assessed where you are?
- Overall security assessments – including various controls & testing methods.
- Testing software; static and dynamic

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **DESIGN AND VALIDATE ASSESSMENT, TEST, AND AUDIT STRATEGIES**
  - First, determine scope!
    - What are we testing?
    - Why are we testing it?
  - Testing with narrow(er) scope include penetration tests ("pentests"), vulnerability assessments, and security audits.
  - Broad scope assessments often include narrow scope testing.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **DESIGN AND VALIDATE ASSESSMENT, TEST, AND AUDIT STRATEGIES**
  - Internal - Audits, assessments, and testing can be conducted from two perspectives (Internal/External)
    - To conduct an internal audit, the organization must have adequate skills and knowledge on staff, it must have sufficient time and resources to perform the audit, and there must be no requirements for the audit or assessment to be performed by an independent observer who is totally free of conflicts.
    - part of ongoing or continual assessment processes and/or part of continuous monitoring

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **DESIGN AND VALIDATE ASSESSMENT, TEST, AND AUDIT STRATEGIES**

  Internal

  - These are some types of testing that may be best conducted internally:
    - Vulnerability scanning, especially routine scans looking for unpatched software or unknown assets
    - Process and procedure audits like change management or training completion
    - Phishing simulations

Preparing for External Audits

- An audit conducted by internal personnel will never have the same objectivity as an audit conducted by external personnel.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

ENT, TEST, AND

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **DESIGN AND VALIDATE ASSESSMENT, TEST, AND AUDIT STRATEGIES**

- External – An external auditor should have no conflicts of interest, since they are paid to perform an impartial assessment rather than to deliver a report that makes their department look good. External evaluations can also take advantage of specialized skills and knowledge that are valuable but not needed fulltime.

  - use of an external firm for assessments, testing, or audits can identify issues the organization is unintentionally unaware of

  - a fresh pair of eyes can often spot a problem more quickly and offer insight the organization would otherwise miss.

  - External testing may be advisable or even required in some cases, especially for legal or regulatory reasons, such as maturity assessments against a maturity model

  - Audits for compliance purposes — for example, PCI-DSS, ISO 27001, and the U.S. government's Federal Risk and Authorization Management Program (FedRAMP)

Auditor
noun. [ao-di-tour]

Someone Who Does Precision Guesswork based on Unreliable Data Provided by those of Questionable Knowledge.
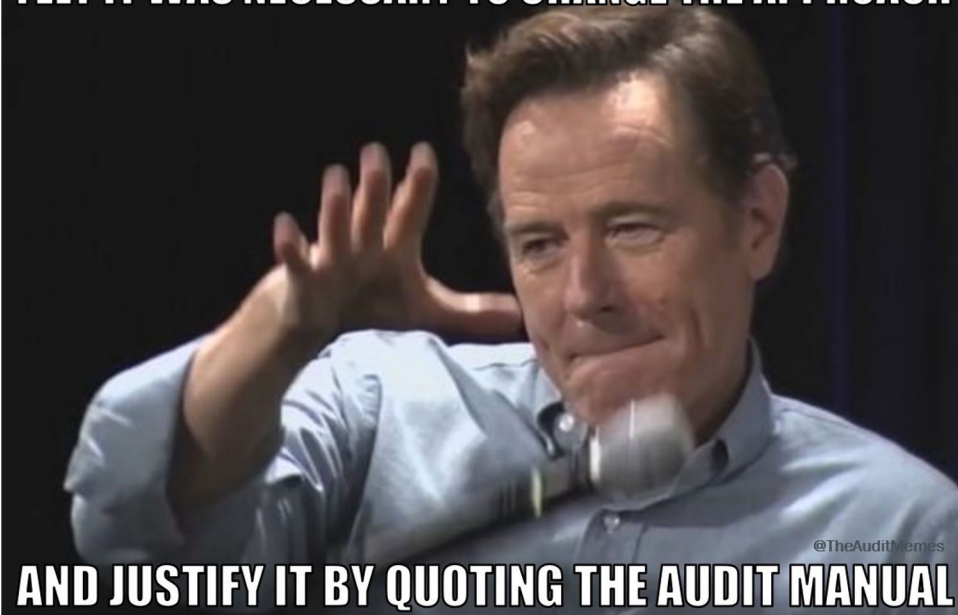
See also: Magician, Wizard

WHEN YOU EXPLAIN IN YOUR WORKPAPER WHY YOU FELT IT WAS NECESSARY TO CHANGE THE APPROACH

AND JUSTIFY IT BY QUOTING THE AUDIT MANUAL

@TheAuditMemes

urity Assessment and Testing

E ASSESSMENT, TEST, AND

- use of an external firm f
  issues the organization i
- a fresh pair of eyes can
  insight the organization
- External testing may be
  especially for legal or reg
  against a maturity mode
- Audits for compliance pu
  the U.S. government's Fe
  Program (FedRAMP)

AUDITORS

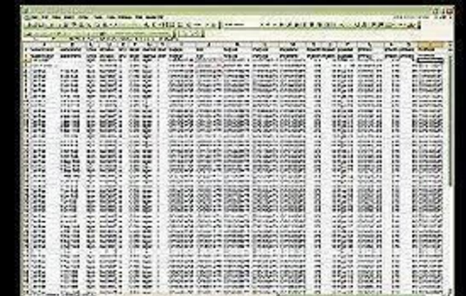What my friends think I do | What my date's parents think I do | What society thinks I do

What my parents think I do | What I think I do | What I actually do

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **DESIGN AND VALIDATE ASSESSMENT, TEST, AND AUDIT STRATEGIES**

- Third Party – a complex series of interconnected organizations, known as a supply chain

- Vulnerabilities in this supply chain can impact the organization, so an audit strategy is needed to identify risks and associated mitigations in the supply chain.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **DESIGN AND VALIDATE ASSESSMENT, TEST, AND AUDIT STRATEGIES**

- CONDUCT SECURITY CONTROL TESTING
  - Testing controls is essential to ensure they are implemented and operating as intended to mitigate risks.

  - Testing may be done from internal or external perspectives and may target complex control implementations across people, process, and technology.
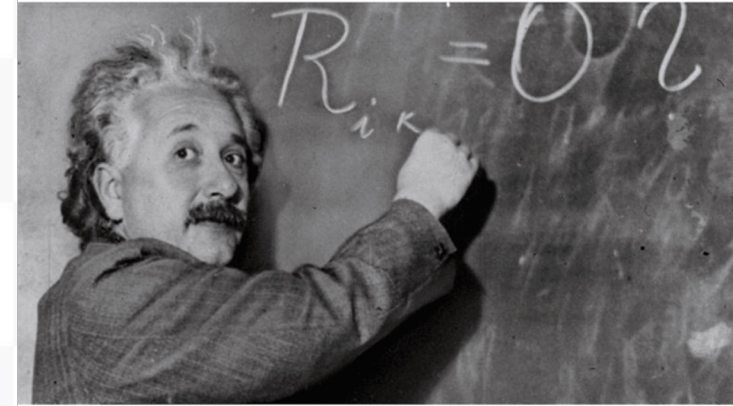
LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **DESIGN AND VALIDATE ASSESSMENT, TEST, AND AUDIT STRATEGIES**

- Vulnerability Assessment
  - Vulnerabilities typically disclosed more frequently than risk assessments are performed, so ongoing vulnerability assessments are a key element of a continuous monitoring strategy.
  - Assessing identified vulnerabilities includes analysis of their impact to the organization given the organization's unique configurations or circumstances.

How I think I look explaining cyber risk to the board

How I actually look

YEA.. WE'RE GOING TO NEED YOU TO..

ADDRESS 10,000 VULS BEFORE MONDAY.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Asset Inventory

- Identifying the organization's critical assets is an important prerequisite to performing a vulnerability assessment.

- It is crucial to understand both the types of systems to be scanned and their criticality to choose appropriate scanning tools and prioritize scanning efforts.

- The asset inventory should capture data from other organizational processes like a business impact assessment (BIA), which identifies the criticality of each system, application, or data asset.

- Vulnerabilities in highly critical systems should be prioritized first since exploiting a vulnerability in a low criticality system is less likely to disrupt operations.
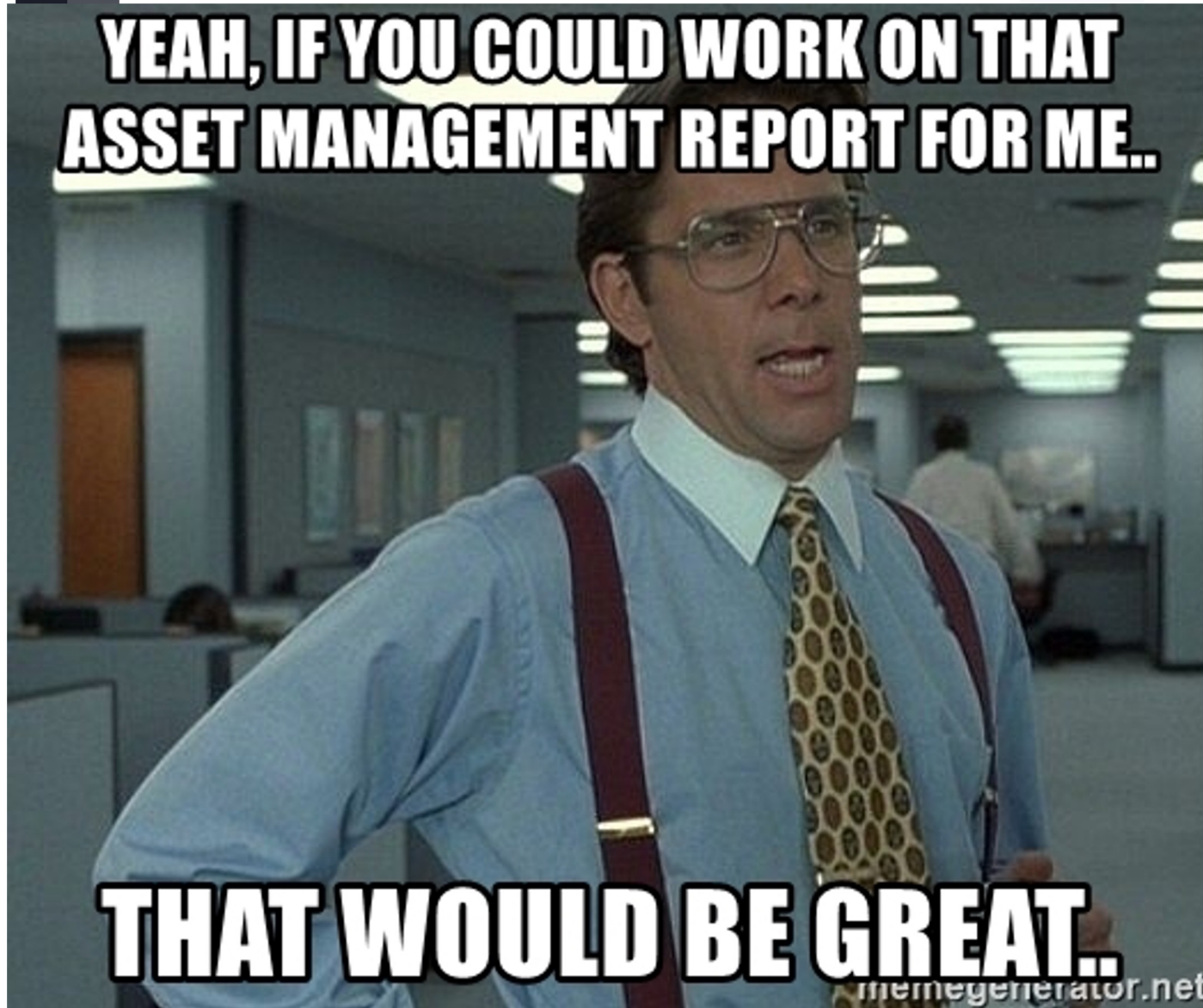
LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **Scanning Tool Functions and Considerations**

- Many popular scanning tools can identify vulnerabilities in hosts, networks, or applications.

- These include open-source tools that are free to use as well as commercial options;

- The choice to use open-source or commercial may include factors such as the availability of support, ability to scan specific systems or platforms, and the level of skill required to operate the tool.

- Proprietary tools may offer more features and support, but with a correspondingly higher price.

- Most scanning tools offer a similar set of basic features and operate in a common manner.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **Scanning Tool Functions and Considerations**

- These automated tools identify targets, which may be a single network endpoint or a range of IP addresses, and then send network traffic and listen for a response to determine if an IP address is in use.

- Once an asset is discovered, the scan performs other automated actions to identify vulnerabilities.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **Scanning Tool Functions and Considerations**

- **Obligations** such as legal, contractual, or regulatory, which may specify the scope, coverage, or frequency of scanning. A free vulnerability scanner might be appropriate for small environments without regulated data, but is likely insufficient for a heavily regulated financial services firm.

- **Depth**, **scope**, or **coverage** of the scanner, including the ability to perform advanced scanning by authenticating to targets being scanned with administrative credentials — sometimes known as credentialed scanning.

- *Vulnerability scanners may generate false positives or provide low-resolution information by only looking at externally accessible information*, but many can be configured with credentials like an administrator password or Secure Shell Protocol (SSH) key that allows the scanners to log in and perform additional checks.

20

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- **Scanning Tool Functions and Considerations**

- **Platform support** is a major consideration for organizations with mixed IT environments, such as Linux and Windows server operating systems or macOS and Windows workstation operating systems. Like all IT tools, the requirements for a vulnerability scanner

- **Cloud environments** may pose unique challenges for vulnerability scanning. ***Software as a service (SaaS)*** environments may prevent users from performing vulnerability scans due to the operational overhead it introduces, which can degrade system performance, and not all vulnerability scanners can be run against targets outside a local network.
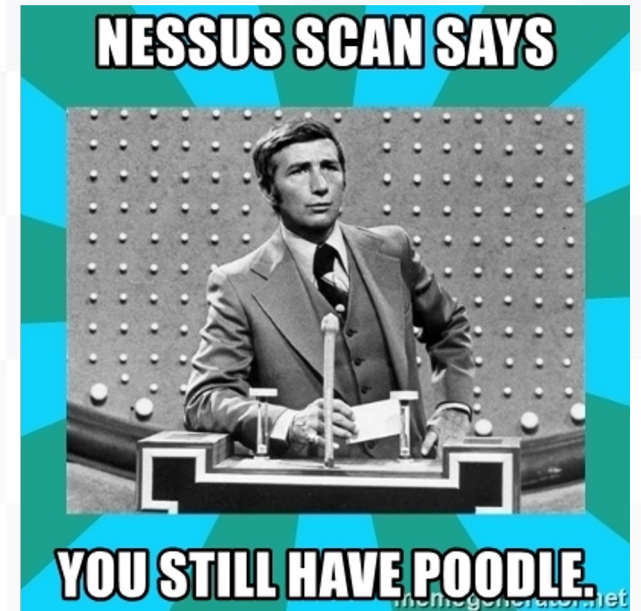
LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

- Vulnerability scanning (also called vulnerability testing) scans a network or system for a list of predefined vulnerabilities such as system misconfiguration, outdated software, or a lack of patching
- Nessus (http://www.nessus.org), OpenVAS (http://www.openvas.org), Qualys, and Rapid 7/Nexpose
- Missing patches and configuration errors
- Common Vulnerability Scoring System (CVSS) - https://nvd.nist.gov/cvss.cfm

NESSUS SCAN SAYS

YOU STILL HAVE POODLE.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

23

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

Excessive Traffic and DoS - *Vulnerability scanners can generate large volumes of traffic that consume network bandwidth and can lead to DoS* conditions on both networks and systems that struggle to process the information.

- **Proper configuration** reduces the likelihood of these issues, such as implementing request throttling to limit the number of requests the scanner generates in a given time period.

24

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

Excessive Traffic and DoS

- **Credentialed scans** *can read configuration information directly from a server's operating system* to see what ports are open, rather than sending traffic to each port individually.

- **Scan scheduling** may also be useful to ensure scans are conducted at times of low user activity.

- **Spreading scans out over a larger time period** can also be useful — scanning a few hosts per day reduces the impact of scanning an entire network.

IF YOU WERE WAITING FOR THIS A SIGN IS IT

vulnerability scans... a must

Memecreator.org

25

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

Excessive Traffic and DoS

- **Credentialed scans** can also help reduce the amount of traffic — a *credentialed scan can read configuration information directly from a server's operating system* to see what ports are open, rather than sending traffic to each port individually.

- **Scan scheduling** may also be useful to ensure scans are conducted at times of low user activity.

- **Spreading scans out over a larger time period** can also be useful — scanning a few hosts per day reduces the impact of scanning an entire network.

YA'LL GOT ANY MORE OF THEM
TWO FACTOR AUTHENTICATION?

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

Finally fixed all the vulnerabilities from our 2006 scan

Alerts and Incidents

- When a vulnerability scanner performs the same actions, particularly if the scan triggers a DoS attack or unusual host activity, it will generate security alerts and possibly trigger incident response (IR) processes.

- **Many security tools are designed to flag activity commonly used by both attackers and vulnerability scanners, like sequential port scans.**
    - An attacker might send a request to each port number in sequence to identify open services that could be exploited, which looks similar to a vulnerability scanner identifying open services.

- **Configuring other security tools to ignore legitimate vulnerability activity is essential**
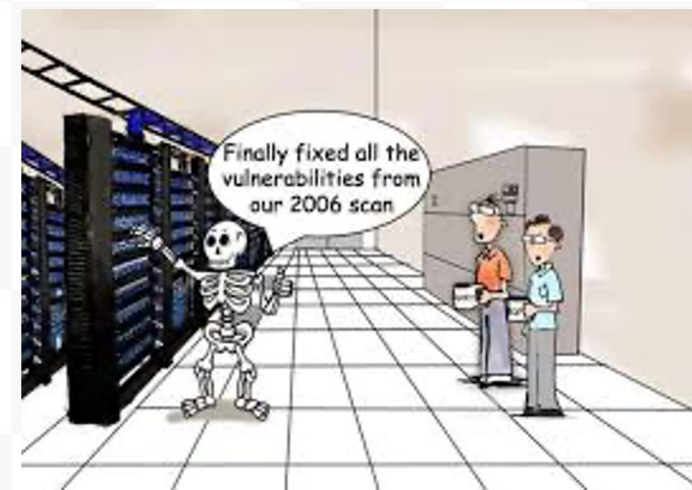
LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

Cross-Functional Ownership

- Cross-functional teams and ownership of scan results can be an issue that requires not only security skills, but also project and business management skills.

- Vulnerability scanners are often owned by a security or IT team, while the applications and network assets where vulnerabilities are identified belong to another team.

- Fostering a relationship across those teams is crucial to ensure vulnerabilities are taken seriously and addressed
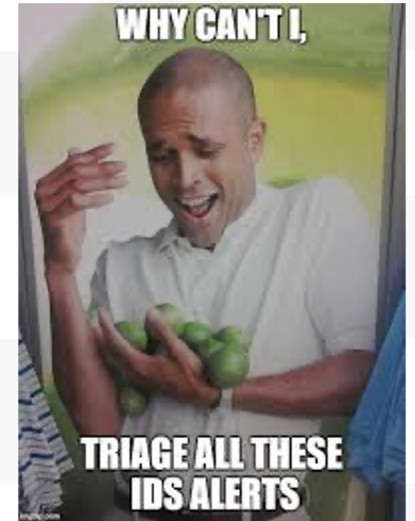
LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

Cross-Functional Ownership

- There may be additional issues of communicating the context of any findings.
  - Non-security personnel typically do not understand CVSS scores
  - **Communicating context** to the audience is important and *may require formatting results in a way that is best suited to the asset owner*.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

Data Integrity Pollution

- Vulnerability scanners can perform **automated actions like filling in form fields on a web application** to check for issues including Structured Query Language (SQL) injection or cross-site scripting (XSS).

- Some scanners can be configured to ignore certain types of fields, or the scanner can be configured to put in a recognized type of test data that can be easily ignored or cleaned up after the scan.

- It may be necessary to conduct vulnerability assessments against a different environment altogether, such as a staging environment configured exactly like production but without live production data.
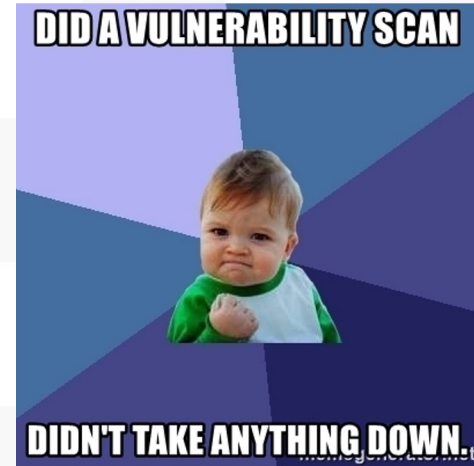
LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

Network Segmentation

- *Segmenting or isolating different parts of a network with access controls like firewalls is a security best practice* that may create problems when attempting to perform vulnerability scanning.
  - The vulnerability scanner itself is a network endpoint, and **it requires access to all other endpoints in scope for scanning**;
  - if the network is segmented using virtual LANs (VLANs), routers, or firewall rules, **the scanner may not be able to reach its targets**.
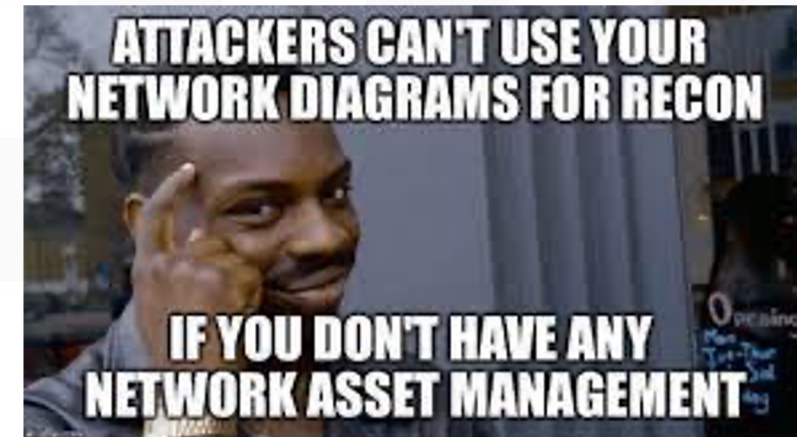
ATTACKERS CAN'T USE YOUR NETWORK DIAGRAMS FOR RECON

IF YOU DON'T HAVE ANY NETWORK ASSET MANAGEMENT

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

Network Segmentation

- Zero trust network architecture and microsegmentation are particularly challenging in cloud computing environments where these *principles are the default and access follows a deny-all, allow-by-exception model.*

  - Distributed scanning is an architecture that places scanning agents inside network segments to allow the endpoints in that segment to be scanned, and then consolidates the results to a central console.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Scanning Tool Functions and Considerations

Pen Test Scoping: It's Not Safe to Ignore Systems!

- *Many organizations scope pen tests to focus on a narrow set of systems or applications, usually as a cost-saving measure since pen testing an entire network is costly.* In other cases, the pen test simply meets a compliance requirement, **so only particular systems are in scope.** While understandable, both approaches can create a false sense of security.

- Networks are highly interconnected, which means a narrowly scoped pen test will likely **miss vulnerabilities in out-of-scope systems that an attacker could exploit.**

- If a *pen test does discover something on a system that is out of scope,* the organization *should never ignore the finding just because it is "out of scope."* Attackers would certainly be happy to exploit that vulnerability.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Penetration Testing

- Lots of different types of penetration tests, depending on the what and why (and a little how).
    - Network (Internet)
    - Network (internal or DMZ)
    - War dialing
    - Wireless
    - Physical (attempt to gain entrance into a facility or room)
- Simulate client-side attacks, server-side attacks, Web application attacks, etc.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Penetration Testing - Black Hats and White Hats

- Black hat attackers are malicious hackers, sometimes called crackers.
  - "Black" derives from villains in fiction: Darth Vader wore all black
  - Lack ethics, sometimes violate laws, and break into computer systems with malicious intent, and may violate the confidentiality, integrity, or availability of organization's systems and data

- White hat hackers are the "good guys"
  - Professional penetration testers who break into systems with permission
  - Malware researches who research malicious code to provide better understanding and ethically disclose vulnerabilities to vendors, etc.
  - Also known as ethical hackers; they follow a code of ethics and obey laws
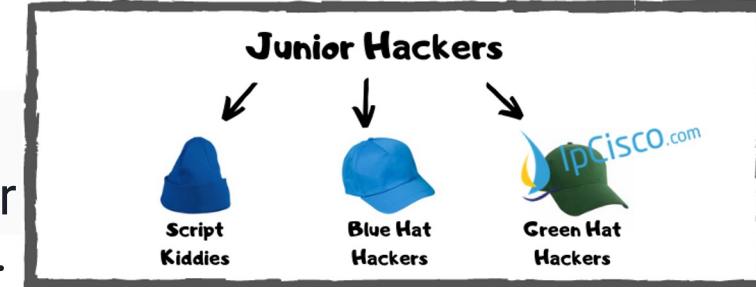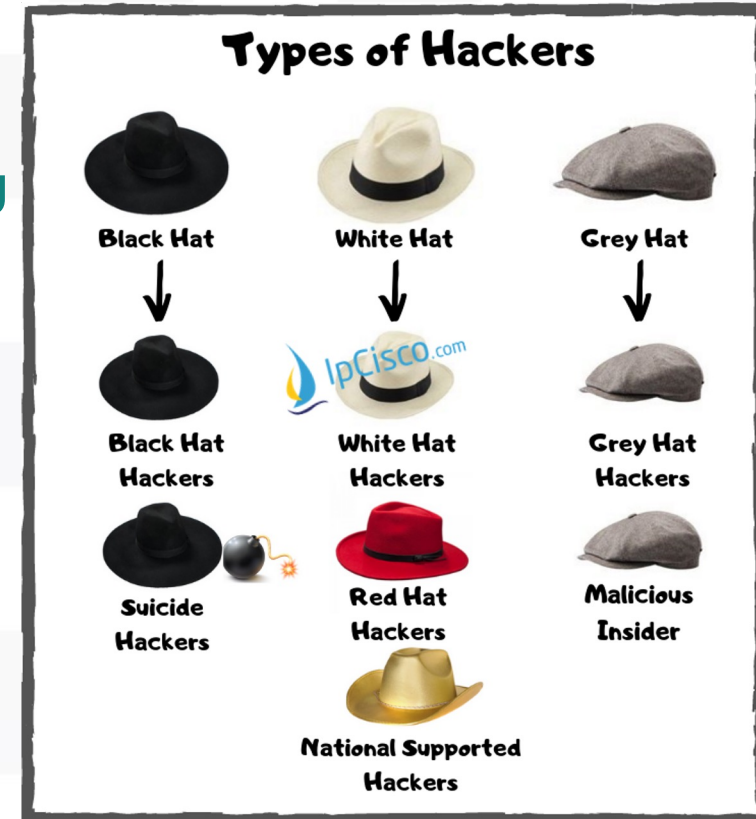
Types of Hackers

Black Hat — Black Hat Hackers
White Hat — White Hat Hackers
Grey Hat — Grey Hat Hackers
Suicide Hackers
Red Hat Hackers
Malicious Insider
National Supported Hackers

Junior Hackers

Script Kiddies
Blue Hat Hackers
Green Hat Hackers

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Penetration Testing - Black Hats and White Hats

- Gray hat hackers fall somewhere between black and white hats
  - Exploits a security weakness in a computer system or product in order to bring the weakness to the attention of the owners
  - Unlike a black hat, a gray hat acts without malicious intent
  - The goal of a gray hat is to improve system and network security

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Penetration Testing

- *War dialing* uses modem to dial a series of phone numbers, looking for an answering modem carrier tone (the penetration tester then attempts to access the answering system); the name derives from the 1983 movie WarGames

- *Social engineering* uses the human mind to bypass security controls
  - May be used in combination with many types of attacks, especially client-side attacks or physical tests
  - An example of a social engineering attack combined with a client-side attack is emailing malware with a Subject line of "Category 5 Hurricane is about to hit Florida!"
  - A physical social engineering attack (used to tailgate an authorized user into a building)

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Penetration Testing

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Penetration Testing

- A *zero-knowledge* (also called <u>black box</u>) test is "blind"; the penetration tester begins with no external or trusted information, and begins the attack with public information only

- A *full-knowledge* test (also called <u>crystal-box</u>) provides internal information to the penetration tester, including network diagrams, policies and procedures, and sometimes reports from previous penetration testers

- *Partial-knowledge* tests are in between zero and full knowledge: the penetration tester receives some limited trusted information

- Most penetration tests have a scope that includes a limitation on the time spent conducting the test

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Penetration Testing Tools and Methodology

- Penetration testing tools:
  - Open source Metasploit (http://www.metasploit.org)
  - Closed source Core Impact (http://www.coresecurity.com) and Immunity Canvas (http://www.immunitysec.com)
  - Top 125 Network Security Tools (http://sectools.org/)
  - Custom tools

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Penetration Testing Tools and Methodology

- Pene
  - C
  - C
    a
  - T
  - C

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Penetration Testing Tools and Methodology

- Penetration testers use the following methodology:
  - Planning
  - Reconnaissance
  - Scanning (also called enumeration)
  - Vulnerability assessment
  - Exploitation
  - Reporting
- Black hat hackers typically follow a similar methodology
- Black hats will also cover their tracks (erase logs and other signs of intrusion), and frequently violate system integrity by installing back doors (in order to maintain access)
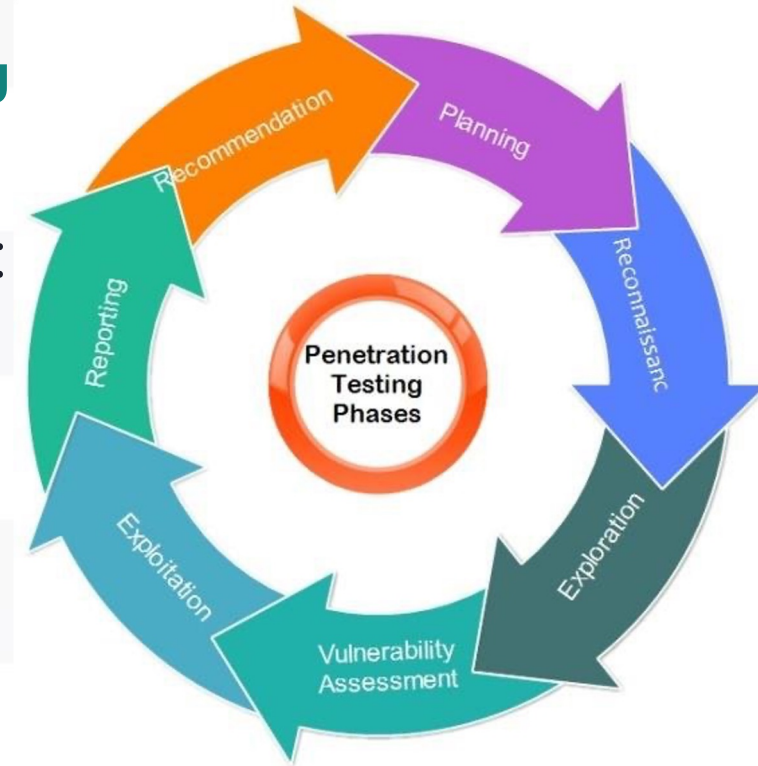
Phase 1: Discovery or Reconnaissance
Goal: Gather information regarding the target(s)

Phase 2: Scanning and Probing
Goal: Utilize gathered information to probe for vulnerabilities and identify entry points
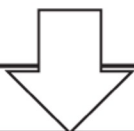
Phase 3: Exploitation
Goal: Utilize approved methods to exploit vulnerabilities and attempt to gain access
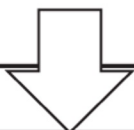
Phase 4: Post-exploitation
Goal: Continue the attack by attempting further exploits using the access gained

Phase 5: Reporting
Goal: Document and present report on actions taken, exploits achieved, suggested remediations

Remediate and Retest
The organization addresses any vulnerabilities discovered, and the pen testers repeat the test to identify if the remediation was successful.
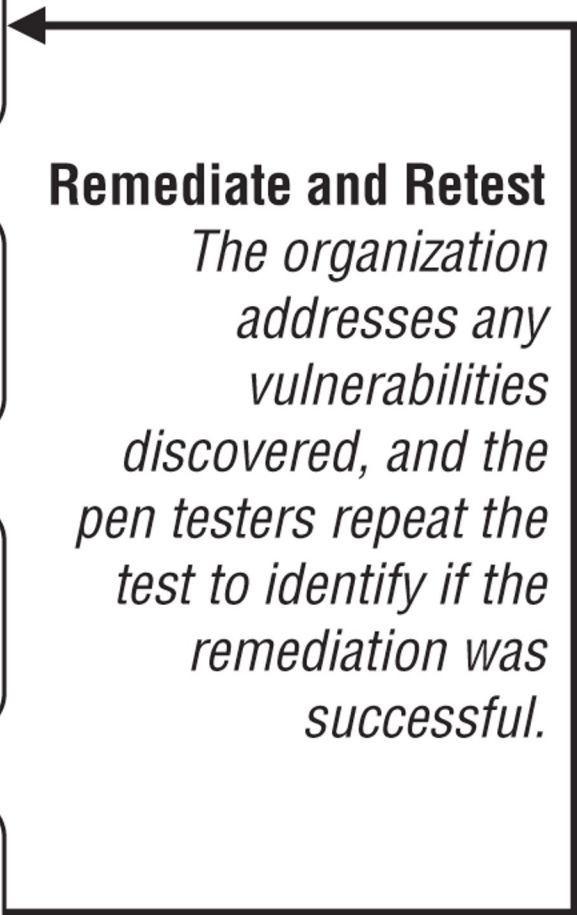
LECTURE

Agenda – Domain 6: Security Assessment and Testing

Penetration Testing Tools and Methodology

The PenTesters Framework (PTF)

A TrustedSec Project - Copyright 2018

Written by: David Kennedy (@HackingDave)

https://www.trustedsec.com

Twitter: @TrustedSec, @HackingDave

The PenTesters Framework (PTF) is a Python script designed for Debian/Ubuntu/ArchLinux based distributions to create a similar and familiar distribution for Penetration Testing. As pentesters, we've been accustom to the /pentest/ directories or our own toolsets that we want to keep up-to-date all of the time. We have those "go to" tools that we use on a regular basis, and using the latest and greatest is important.

PTF attempts to install all of your penetration testing tools (latest and greatest), compile them, build them, and make it so

Pentest Methodology Template*

Sample Project Flow

Intelligence Gathering	Threat Modeling	Vulnerability Analysis	Exploitation	Post Exploitation	Reporting
STAGE 1	STAGE 2	STAGE 3	STAGE 4	STAGE 5	STAGE 6

EXAMPLE TACTICS, TECHNIQUES, AND ATTACK VECTORS

1. Gather E-mail addresses and User Info.
2. Create Phishing Campaigns
3. Verify Target(s)
4. Develop Delivery Mechanisms
5. Develop Exploits (browser, MS Office, etc.)
6. Develop Blended Attack Vectors

7. Deliver the payloads to target
8. Run the exploits (scripts, code, binaries)
9. Use PW Hash, file, Registry or OS Services to "own" the local system
10. Establish C2 from the compromised host(s)
11. Identify weak passwords or known OS exploits to escalate privileges
12. Obtain tokens and/or credentials

13. Perform additional recon through port scanning, sniffing or probing
14. Collect Authentication credentials (Kerberos tickets, OS Services, file share) for access across the network
15. Exploit groups, passwords, and domain trusts
16. Access sensitive data via mail, files, financial systems, databases
17. #Winning

*Follows Industry Standard Stages documented in Lockheed Martin Cyber Kill Chain

LECTURE

Agenda – Domain 6: Security Assessment and Testing

PENETRATION TESTING
PRT1_RECON

Phase 1: Discovery or Reconnaissance

Discovery or reconnaissance requires the pen tester to gather information regarding the target. This often begins with open-source intelligence (OSINT), since the tester wants to emulate attackers and remain undetected. OSINT sources include the following:

- **Social media** to identify targets or useful personal details for phishing.

- **Public records** like Domain Name System (DNS) or company websites with information regarding services or locations.

- **Attack surface data** like enumerating the IP addresses associated with the target's DNS records and potential details about services in use. Publicly available tools Shodan or Have I Been Pwned can also be used.

- **Physical observations** like monitoring employee movements, photographing, driving by, or observing facilities, or dumpster diving to obtain hard copy.

Pen testers generally **try to evade** detection by the organization and seek information outside of the organization's monitoring abilities like DNS records, which are publicly accessible and maintained by a domain Registrar.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Phase 2: Scanning and Probing

Scanning and probing require some traffic to be sent to the organization or target systems, which introduces the risk of detection by the organization's security processes.

- Network footprinting: Testers define the footprint of a network, or what endpoints exist and services running on them.
  - Tools like Nmap, nslookup, ping sweeps, and port scanning are used to perform queries that determine active network hosts and services running on a network.

- Banner grabs: Testers analyze information returned by endpoints, which often contains useful information including software names and versions.

- Vulnerability scanning: While an obvious approach, the use of a vulnerability scanner increases the pen tester's efficiency.
  - These tools automate tasks like footprinting and parsing information from banners.

- Exploitation toolkits: Tools like Metasploit combine reconnaissance, footprinting, vulnerability scanning, and partially or fully automated exploitation into a single software interface.
  - Since these tools combine multiple functions, they are utilized across multiple phases.

LECTU

Agenda –

Phase 2: S

Scanning and p
introduces the

- Network foo
  services run
  - Tools lik
    that det

- Banner grab
  information

- Vulnerability
  the pen test
  - These t

- Exploitation
  scanning, an
  - Since th

WHAT IS THE DIFFERENCE?

PENETRATION TEST	VS	VULNERABILITY SCAN
Discover & Exploit Vulnerabilities		Checks for known Vulnerabilities
Usually Human		Automated
Simulate a full attack		Single attack phase
$$$$		$
General Frequency: Annual or after major changes		General Frequency: Daily/Weekly/Monthly
A security best practice		A security best practice

www.sternsecurity.com

stems, which

s exist and

orm queries

ontains useful

nner increases

banners.

, vulnerability
rface.

ple phases.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Phase 3: Exploitation

The testers exploit the identified vulnerabilities and attempt to gain access. They may use a variety of methods as defined by the rules of engagement, which are discussed in detail in a later section. The goal of exploitation is gaining access to systems or data that should not be accessible. These are some automated and manual exploitation tools:

- **Exploitation toolkits** like Metasploit, which can automate many aspects of pen testing

- **Password crackers** like John the Ripper, Hashcat, or Hydra, which are useful if the tester gathers hashed passwords and needs to identify a valid password

- **Monitoring tools and proxies** like Wireshark and Burp Suite, which allow the tester to capture, analyze, and modify network traffic

- **Application security** tools like Nikto or fuzzing tools, which can identify and attempt to exploit application vulnerabilities like buffer overflows or SQL injection

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- ### Phase 4: Post-exploitation

- Once the testers have gained initial access, **they will attempt to pivot or use that access to gain further access**.

- For example, compromising a system in the demilitarized zone (DMZ) is not highly valuable since sensitive data is typically not stored here.

  - However, **DMZ assets may be authorized to connect to endpoints on an internal network segment**, which could grant the tester unauthorized access to something more valuable.

  - The *compromised DMZ could even be used to iterate Phase 2 activities and perform network footprinting of internal resources* that are not reachable from outside the network.

- Endpoints or assets discovered will be categorized, and attention will be paid to high-value targets.

  - *Once network endpoints have been enumerated, various techniques are used to fingerprint them* — the goal is to discover useful details like operating system and application software versions. **Exploits will be tried against these until the tester is discovered, runs out of time, or exhausts all identified possibilities.**

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Phase 5: Reporting

Throughout the testing process, **documentation should be created to capture all activities performed, vulnerabilities found, and any access the testers achieve**.

- These findings are compiled into a report, and it is typical for the testers to include recommendations for the organization to remediate any identified vulnerabilities.

- **This report is usually presented in a formal meeting, which marks the end of the pen test engagement.**

- Different reports, or different parts of the report, may be designed for different audiences.

  - An executive summary with the scope, high-level synopsis of tests performed, and number of findings is often prepared to share with management or users outside the organization

  - More technically detailed parts of the report are in a separate document or appendix designed for internal IT staff.

51

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Physical Penetration Testing

Gaining unauthorized physical access to certain facilities is illegal in some circumstances, so physical pen testers should be given a get out of jail free card that details the purpose of their activity and a point of contact within the organization who can verify their story.

Red teamers arrested during penetration test

Cyber Work

Justin Wynn & Gary DeMercurio Coalfire

TWO SAY 'HIRED' TO BREAK INTO COURTHOUSE
BOTH MEN FACE CURRENTLY FACE BURGLARY CHARGES

JUSTIN WYNN   GARY DEMERCURIO

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Assuring Confidentiality, Data Integrity, and System Integrity

- Penetration testers must ensure the confidentiality of any sensitive data that is accessed during the test
- Testers will often request that a dummy file containing no regulated or sensitive data (sometimes called a flag) be placed in the same area of the system as the credit card data, and protected with the same permissions
- If the tester can read and/or write to that file, then they prove they could have done the same to the credit card data
- Penetration testers must be sure to ensure the system integrity and data integrity of their client's systems
- The risk of encountering signs of a previous or current successful malicious attack (discuss this before starting a test)

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Synthetic Transactions

- Synthetic transactions are automated activities run against a monitored target to measure its performance.

Synthetic transactions can be employed as a test mechanism for a variety of purposes:

- **SLA monitoring**: Hosted or cloud-based services may guarantee certain levels of service, such as a SaaS application that guarantees 99.9 percent uptime.

- **Data integrity monitoring**: Systems with complex business logic may have dynamic rules for handling data

- **System or service monitoring**: Even in the absence of an Service Level Agreement (SLA), systems can be monitored to ensure they are online and responding as expected.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Log Reviews - Security Audit Logs

- Reviewing security audit logs within an IT system is one of the easiest ways to verify that access control mechanisms are performing adequately

- Reviewing audit logs is primarily a detective control

- Remember; we cannot prevent all bad things from happening, so we must be able to detect and respond. – NOT risk elimination, but risk management.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Log Reviews - Security Audit Logs

- According to NIST Special Publication 800-92 (http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf), the following log types should be collected:
  - Network Security Software/Hardware:
  - Antivirus logs
  - IDS/IPS logs
  - Remote Access Software (such as VPN logs)
  - Web proxy
  - Vulnerability management
  - Authentication servers
  - Routers and firewalls

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Security Audit Logs – Centralized Logging

- Assists in log retention (sufficient for legal/regulatory compliance and investigation)
- Assists in log protection (integrity & availability) – attackers delete logs, destroying evidence.
- SIEM
  - Log protection
  - Log aggregation
  - Log correlation
  - Dashboard reporting

SIEM isn't plug and play.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Security Assessments

- A holistic approach to assessing the effectiveness of access control

- Broad scope

- Security assessments view many controls across multiple domains, and may include the following:

  - Policies, procedures, and other administrative controls

  - Assessing the real world-effectiveness of administrative controls

  - Change management

  - Architectural review

  - Penetration tests

  - Vulnerability assessments

  - Security audits

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Security Assessments

- Key words… "assessing the effectiveness"
- Where there are gaps in control (weakness/vulnerability), what are the applicable threats?
- Vulnerabilities + Threats = Likelihoods & Impacts = **RISK**
- FRSecure specializes in assessments – FISA™ and FISASCORE®

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Security Assessments

- Remember our definition of information security?
  - Administrative Controls – policies, procedures, training & awareness, etc.
  - Physical Controls – the things we can touch; locks, cameras, etc.
  - Technical Controls – the effectiveness of the technology we employ to protect assets.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Security Assessments

- FRSecure specializes in assessments – S2Score™ is at our core.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Software Testing Methods

- **Static testing** tests the code passively: the code is not running. This includes walkthroughs, syntax checking, and code reviews.
- **Dynamic testing** tests the code while executing it.
- **White box software testing** gives the tester access to program source code, data structures, variables, etc.
- **Black box testing** gives the tester no internal details: the software is treated as a black box that receives inputs.
- **Traceability Matrix** (sometimes called a Requirements Traceability Matrix, or RTM) can be used to map customer's requirements to the software testing plan: it "traces" the "requirements," and ensures that they are being met.
- **Fuzzing** (also called fuzz testing) is a type of black box testing that enters random, malformed data as inputs into software programs to determine if they will crash.
- **Combinatorial software testing** is a black-box testing method that seeks to identify and test all unique combinations of software inputs.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Software Testing Methods

Misuse Case Testing

- Misuse case or negative testing is designed to assess how a system or application responds to unexpected inputs or situations, and identifies vulnerabilities which might be exploitable under these unexpected circumstances

Abuse Cases

- Unlike a misuse case, an abuse case is a specification of a deliberate, harmful interaction between a user and a system. They are often used to identify security requirements by specifying the ways a system could be abused by a malicious actor and are an integral part of threat modeling.

63

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Software Testing Methods

- **Static testing** tests the code passively: the code is not running. This includes walkthroughs, syntax checking, and code reviews.
- analysis of computer software that is performed without actually executing programs
- In most cases the analysis is performed on some version of the source code, and in the other cases, some form of the object code
- List of tools for static code analysis (https://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis)

64

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Software Testing Methods

- **Static testing** tests the code passively: the code is not running. This includes walkthroughs, syntax checking, and code reviews.
  formed without actually

65

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Software Testing Methods

- Traceability Matrix (or Requirements Traceability Matrix or RTM)
  - Map customer requirements to the software testing plan.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Software Testing Levels

- Synthetic Transactions (aka synthetic monitoring):
  - Scripts and/or tools to simulate "normal" activities.
  - Establish baselines and performance metrics (usually)

BASIC UPTIME MONITORING

TRANSACTION MONITORING

PERFORMANCE MONITORING

SYNTHETIC MONITORING

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Software Testing Levels

- **Unit Testing**: Low-level tests of software components, such as functions, procedures or objects
- **Installation Testing**: Testing software as it is installed and first operated
- **Integration Testing**: Testing multiple software components as they are combined into a working system. Subsets may be tested, or Big Bang integration testing tests all integrated software components
- **Regression Testing**: Testing software after updates, modifications, or patches
- **Acceptance Testing**: testing to ensure the software meets the customer's operational requirements. When this testing is done directly by the customer, it is called User Acceptance Testing.

THIS TIME I'M GONNA RING-FENCE ENOUGH TIME FOR TESTING

OOOH SHINY NEW UI LIBRARIES!

It'll save you time in the long run...

BEFORE REGRESSION TESTING

AFTER REGRESSION TESTING

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Software Testing Levels

Fuzzing

- Black box testing that enters random, malformed data as inputs into software programs to determine if they will crash.
- Typical causes are boundary checking issues, leading to possible buffer overflows
- Typically automated, repeatedly presenting random input strings as command line switches, environment variables, and program inputs attack
- List of good fuzzers; http://sectools.org/tag/fuzzers/.
- Burp Suite https://portswigger.net/burp/

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Software Testing Levels

Fuzzing

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Other Software Testing Terms

- **Misuse Case Testing** - derived from and is the inverse of use case testing; describes the process of executing a malicious act against a system, while use case can be used to describe any action taken by the system
- **Test Coverage Analysis**
- **Interface Testing** – testing of all interfaces exposed by the application.
- **Combinatorial software testing** - a black-box testing method that seeks to identify and test **all** unique combinations of software inputs.
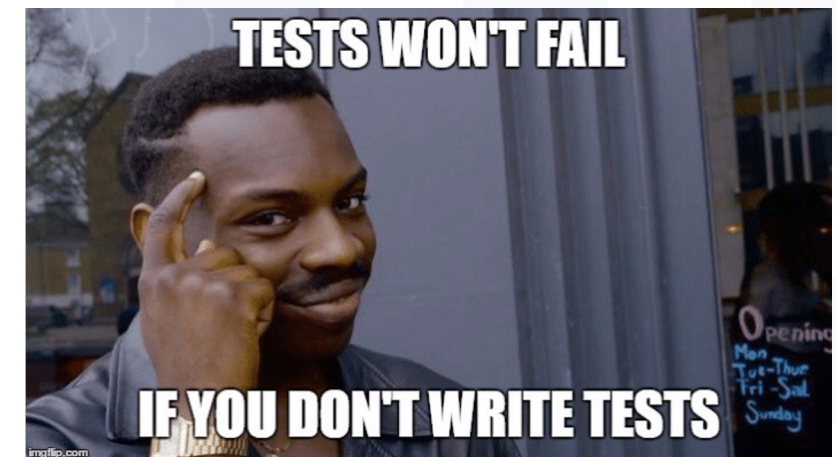
LECTURE

Agenda – Domain 6: Security Assessment and Testing

Test Coverage Analysis

- Test coverage refers to the number of functions in a system or application that are tested and can be expressed as a percentage of the total system that has been tested or a specific number of things tested, such as functions or modules.

Test coverage analysis measures four main criteria to identify sub-elements of a program or system being tested:

- **Branch coverage** ensures that each branch in a control statement has been executed.

- **Condition coverage** requires each Boolean expression in the code to be validated for both true and false conditions.

- **Function coverage** makes sure that every function in the program is called.

- **Statement coverage** validates the execution of every statement in the program.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Interface Testing

- An interface is an interaction point with a system.

- Examples include the user interface (UI), which provides a way for a human user to interact with a system, and APIs, which are used for system-to-system interaction.

- UIs often take the form of a graphical user interface (GUI) with windows and menus or text-based interaction using a command-line interface (CLI).

- APIs may be implemented using a variety of methods like Representational State Transfer (REST) APIs for web applications, inter-process communication (IPCs), and remote procedure calls (RPCs).
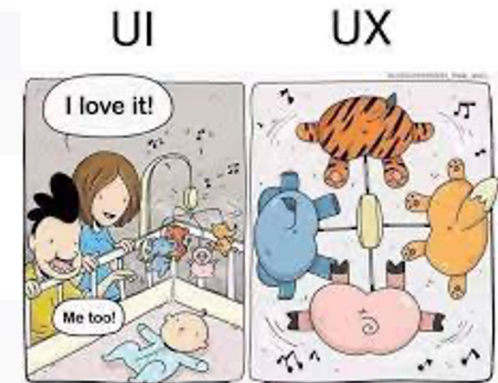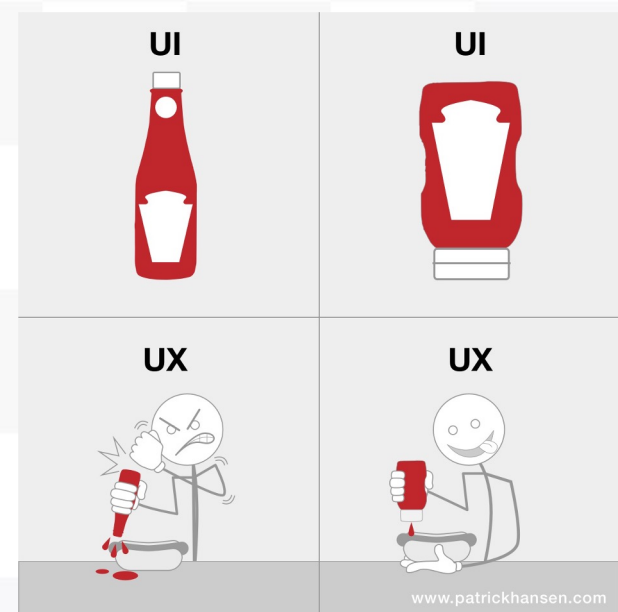
LECTURE

Agenda – Domain 6: Security Assessment and

Breach Attack Simulations

- Breach attack simulations or breach and attack simulations (BAS) are an emerging method of automated testing designed to simulate a realistic attacker attempting to gain unauthorized access.

The categories of attacks carried out by a BAS are often categorized by the target or vector and can include the following:

- **Endpoint**: The BAS performs action on or against a network endpoint, such as creating files or processes that match known malware signatures to test endpoint detection and response (EDR) capabilities.

- **Network**: The BAS sends network traffic that should be blocked and generates an alert if known bad or malicious traffic is not blocked by controls like firewalls or routers.

- **Email**: Spam filters, email spoofing controls, and content filters can be tested by test messages generated and sent by the BAS.

- **Behavior-based**: Advanced BAS functions can test behavior-based security controls like security tools monitoring for malicious network scans or complex interaction with applications that should be blocked by a web application firewall (WAF).

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Compliance Checks

- Compliance frameworks generally combine a set of risks specific to an industry or region, and the required security controls are designed to mitigate them.

Some examples of security and compliance frameworks that require compliance audits are identified here:

- ISO 27001 audits are performed every three years by an external auditor to achieve certification, while the organization must perform continuous monitoring and oversight, including internal auditing and surveillance audits on an annual basis.

- PCI-DSS requires organizations to undergo an annual audit by a third-party auditor and perform routine internal activities such as quarterly vulnerability scans.

- FedRAMP requires an ongoing annual assessment after the initial full security assessment and also requires a continuous monitoring strategy for key risks in order to maintain Authority to Operate (ATO) status.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

COLLECT SECURITY PROCESS DATA

- Once an organization has identified risks and implemented appropriate controls to mitigate them, it is important to monitor the status of those controls and their effectiveness at achieving the desired risk mitigation.

- Continuous monitoring is a complex task that requires an organization to have mature cybersecurity capabilities.

- Once these controls are in place, a logging and monitoring strategy can be developed, starting with basics like enabling logging on all systems, centralizing log files, and automating monitoring with tools like a security information and event management (SIEM) platform.

- Data trends can be analyzed using automated means to generate trending data such as key performance indicators (KPIs), and the emerging field of artificial intelligence and machine learning (AI/ML) offers some solutions to automate data analysis tasks.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Technical Controls and Processes

- Technical or logical controls are implemented with or by electronic systems, like username and password prompts to access an information system or the configuration of a firewall to reject traffic from a known malicious source.

To do so, it is useful to capture metrics across categories like these:

- **Prevent**: Preventative technical processes include encryption of data and securing access to decryption keys, network access controls like virtual private networks (VPNs), and endpoint controls like host-based firewalls.

- **Detect**: These technical processes include any controls that detect incidents or deviations, such as EDR and SIEM. Detective security data may come from controls that overlap with operations, such as monitoring the status of hardware or software to detect unexpected outages.

- **Respond**: When something goes wrong, response controls are designed to correct the issue, and include EDR as well as network- and host-based intrusion prevention systems (IPSs).

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Administrative Controls

- Administrative controls are implemented in policies and procedures, like acceptable use policies, access review procedures, and personnel security controls such as job rotation.

Metrics about the implementation of this control could measure the following:

- **Policy reach:** How many users have read and acknowledged their understanding of the policy by signing it?

- **Education effectiveness**: How many users attempt to access restricted content?

- **Technology effectiveness:** Based on web traffic, how many users are able to reach restricted content, and how effective are technology controls at enforcing the policy?

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Account Management

- An account Is a set of credentials used to access a resource.

To restrict and monitor access, the following controls may be put in place. The data generated by these controls should be collected and analyzed to evaluate effectiveness.

- **Administrative process** for requesting user access, including formal request and approval before access is granted. This may require an access request ticket or hard-copy access request form.

- **Technical implementation** might include the system for submitting the request, performing reviews and approvals, and the actual identity and access management tool where the user account is created like Active Directory, Okta, or a local computer operating system.

- **Physical controls** will also be used to enforce the access control, such as placing information system components in access-restricted spaces. The implementation of user access controls may also utilize physical devices like tokens, smartcards, or trusted devices, which require policy, procedure, and training to ensure restricted physical access is maintained.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Account Management

Key process data to collect from account management processes includes the following:

- **Timely account management** such as removal of access within specified timeframes after a user changes roles or leaves employment

- **Timely notifications** received for account provisioning or deprovisioning, like notification within 24 hours of a user joining or leaving the organization

- **Proper account reviews** performed according to the organization's defined schedule

- **Proper process execution** such as out-of-bound distribution of passwords, proper verification before password resets, or properly configured network access controls

80

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Management Review and Approval

Management is responsible for defining and executing the mission of an organization, including supporting functions like security and privacy.

Assessments, audits, and ongoing monitoring of security process metrics provide timely data to management, and it is essential for decision-making like identifying organizational risks and the proper course of mitigating action.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Management Reviews for Compliance

There are several frameworks that formally define management review and approval processes related to security. Specific security and compliance frameworks, and their requirements for management review, include the following:

- **ISO 27001** control 9.3 specifies that management must periodically review the information security program for "continuing suitability, adequacy and effectiveness."

- **NIST** and **FedRAMP** define management roles for assessment and authorization and continuous monitoring. Management must review the plans for assessing information systems and the results of assessments and then make a formal decision to authorize the system for use by issuing an authorization to operate (ATO).

- **Certification and accreditation:** Certification is a formal process for evaluating a system or process against a set of criteria, and accreditation is a formal decision about the system's fitness to perform the specified function.

- **SOC 2** requires management to establish "performance measures," as well as generate and use "relevant, quality information to support the functioning of internal control."

- **Control Objectives for Information Technologies (COBIT)** is a management framework for IT and cybersecurity, and it is geared toward high-level management tasks like planning adequate resources, capacity, and oversight tasks like reviews of the organization's control program.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Key Performance and Risk Indicators

Security metrics communicate the effectiveness of existing security controls at mitigating risk and monitor the state of risks that could impact the organization in the future.

- Key performance indicators (KPIs) are the monitoring tool for existing risk mitigations

- Key risk indicators (KRIs) allow the organization to maintain awareness of potential future risks

KPIs should exist to identify how effectively controls are operating to mitigate risks, and provide notice if a control is ineffective, which indicates a risk that may be more likely to occur.

A performance baseline must be established, well as thresholds for upper and lower bounds on the process being monitored.

Processes may have strict or loose requirements for performance, and the thresholds will reflect that — any deviation from the baseline is cause for concern in a strict process, with greater variation allowed for a loose process.

RISK INDICATORS
Types of Metrics
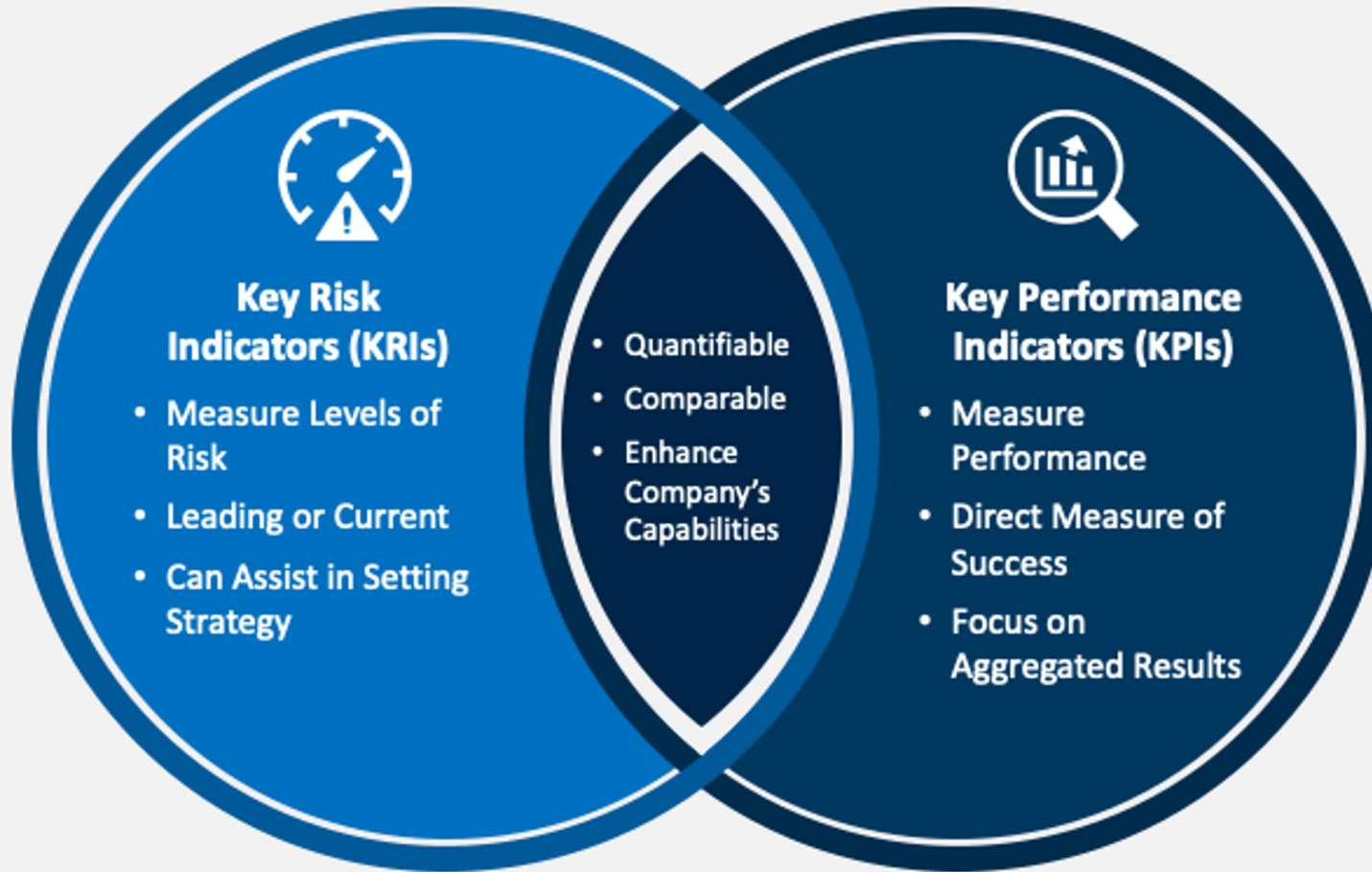
Key Risk Indicators (KRIs)

- Measure Levels of Risk
- Leading or Current
- Can Assist in Setting Strategy

- Quantifiable
- Comparable
- Enhance Company's Capabilities

Key Performance Indicators (KPIs)

- Measure Performance
- Direct Measure of Success
- Focus on Aggregated Results

LECTURE

Agenda – Domain 6: Security Assessment and Testing
Key Performance and Risk Indicators

Examples of important metrics to track and define KPIs for include the following:

- **Mean time to detect (MTTD):** This measures the mean time required to detect a security incident or threat.

- **Mean time to resolve (MTTR):** This measures the time required to resolve incidents.

- **Security scores:** Many vendors provide security scorecards or grades, which can be an indicator of the maturity of an organization's security efforts.

- **Return on Investments (ROI) :** the risk-reducing effect of controls must always be balanced against their cost.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Key Risk Indicators

KRIs can provide the organization with a window into future risks and should be designed to capture how the changing risk landscape might impact the organization.

- Sources of KRIs include common security practices like vulnerability scanning, auditing and assessments, security incident response, malware infection and containment rates, and other security process data.

KRIs aren't historical metrics, they're leading indicators.

When used correctly, they can act as an effective **early warning system.**

ERMInsightsByCarol.com

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Key Risk Indicators

Examples of other valuable KRIs include the following:

- **Number of security incidents:** An increase in the number of security incidents could indicate that the threat environment has changed, and more robust security tools or additional staff are needed.

- **Number of findings:** An increase in findings from audits and assessments could indicate security program deficiencies that require additional attention or resources.

- **Number of phishing attempts detected or reported:** An increase in phishing attempts is often the precursor to an attack, as attackers seek to gain valid credentials to access the organization's resources. Additional system monitoring, multifactor authentication (MFA), and user training could all be deployed in response to this threat.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Backup Verification Data

- Data and system backups are an essential control for integrity and availability, so ensuring they are usable in the event of data loss or corruption is critical.

- The first step is identifying critical data or systems that the organization needs to continue operations and designing a backup strategy appropriate for the recovery needs.

- THEN TEST YOUR BACK-UPS

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Disaster Recovery and Business Continuity

Business continuity and disaster recover (BCDR) topics, including strategies for gathering requirements, designing a plan to address them, and testing the plan

- **Insufficient or negative answers indicate weaknesses that might be addressed by updating the plan documents or iterating processes like business impact analysis (BIA) or plan exercises**.

- Do appropriate plan documents exist, and are they updated? Examples include a BCDR plan, continuity of operations plan (COOP), or individual BC and DR plans.

- Are key personnel aware of their roles and responsibilities under the plan?

- Are new staff trained on key BCDR roles as part of onboarding? This can be a shared metric between security training and BCDR data collection.

- Is the current version of the plan readily accessible and securely stored?

- Are the organization's current critical functions captured in the plans?

- **HAVE THE PLANS BEEN TESTED?**

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Training and Awareness

Establishing and maintaining a program to deliver security awareness, education, and training is vital, because users can be both a critical line of defense against attacks as well as a high-value target of attacks

To *test and evaluate the effectiveness of security training and awareness programs,* the following metrics can be useful:

- Training completion rates: Users who do not complete training may be more liable to miss indications like a phishing email or unexpected system behavior.

- Long-term information retention and habit building: If users take a training, complete a quiz, and immediately forget the information, the program is ineffective.

- Coverage: Threats and risks are constantly evolving; training programs must be updated to address these.

- Audience needs: Some security practices are too technical or might be unimportant for all users, so it is important to deliver an appropriate level of knowledge and training material to the audience.

90

LECTURE

Agenda – Domain 6: Security Assessment and Testing

ANALYZE TEST OUTPUT AND GENERATE REPORT

- Security evaluations such as vulnerability scans, penetration tests, gap assessments, continuous monitoring, and audits generate a large volume of data.

- Reviewing all output generated is time-consuming and may be impossible for non-security practitioners, although users outside the security team do need to access data related to security processes.

- It is essential, therefore, to generate reports that:
    - summarize key details of testing and evaluation activities
    - circumstances or assumptions used to conduct testing
    - actions performed during testing
    - findings or issues discovered,
    - any recommended remedial steps to address the findings
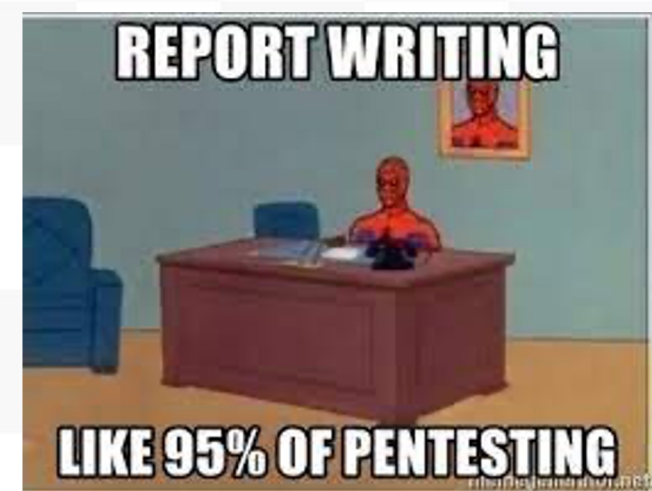
LECTURE

Agenda – Domain 6: Security Assessment and Testing

Typical Audit Report Contents

- **Executive summary:** This section contains a high-level overview of the testing activities and findings and typically takes up no more than one page.

- **Dashboards** present similar high-level information without a narrative and are often present in automated, repetitive testing tools like vulnerability scanners. They provide a summary of the findings and often support the ability to drill down into more technical data.

- **Assumptions or constraints:** Testing often involves constraints, such as a limited amount of time or scope of activities. Scope: It is critical for a reader to understand the coverage of the findings and testing activities

- **Summary of activities:** Tests, evaluations, or audit activities performed should be summarized to show the work performed by the evaluation team.

- **Findings or issues:** Findings, deficiencies, or issues are often presented in a table or bulleted list, and each one should include details like where it was found, the severity, and any evidence supporting the finding.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Typical Audit Report Contents

- **Recommendations:** Assessors may provide generic recommendations, like "Apply all current patches" or more detailed recommendations like which cipher suites to disable on specific webservers along with the relevant system configuration commands.

- **Appendixes:** Relevant information is often placed in an appendix for reference if needed, as raw data generated by security testing tools can be complex and lengthy.
  - Placing such information in an appendix provides a more usable report for quick consumption, as well as providing details for a more technical audience might require if needed.
  - Appendixes are where the details go to die.

YOU MAY USE AN APPENDIX

BUT I WON'T LOOK AT IT OR USE FOR GRADING YOUR REPORT

BRACE YOURSELVES

APPENDIX MEMES ARE COMING
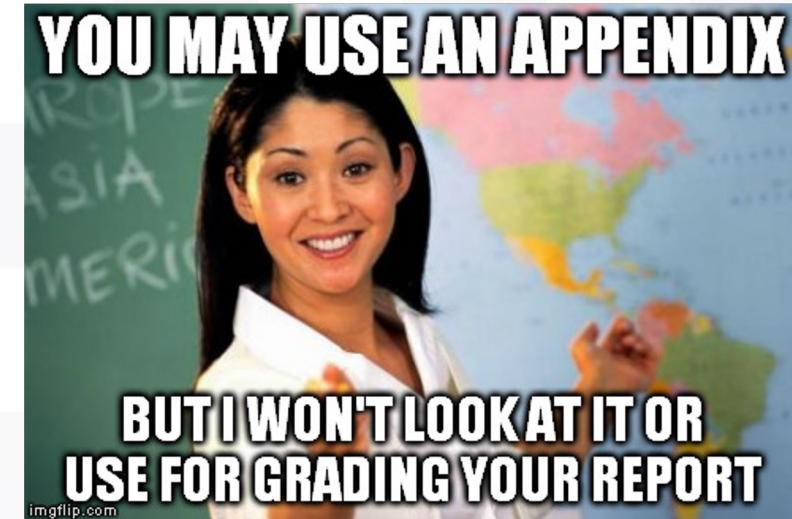
LECTURE

Agenda – Domain 6: Security Assessment and Testing

Remediation

Identifying deficiencies or issues with security controls is the main goal of performing security tests, evaluations, assessments, and audits. Remediation process is designed for addressing any findings.

- This requires project management skills like prioritizing work to be performed, identifying timelines and milestones, and tracking the work through to completion.

- Audit findings may be input to other areas of the security program like risk analysis and may be handled using the processes from that area.

- Go by different names like Plan Of Action and Milestones (POAM), risk mitigation plans, or audit issue mitigation plans.
  - Details of the finding
  - Mitigating or other relevant circumstances
  - Prioritization
  - Timeframe for resolution
  - Resources required
  - Milestones (key dates) and expectations

94

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Exception Handling

When an audit or other security evaluation discovers an issue that cannot be remediated, it must be handled through an exception process.

This is similar to and follows the same steps as documenting policy exceptions, used when a particular system is unable to meet the requirements specified in a policy. Although exceptions may be granted, it should be noted that they should be granted only on a temporary basis.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

This is information typically documented for exception handling:

- **Risk details:** The specifics of the risk, deficiency, or issue, including when it was found and by whom.

- **Reason(s) for exception:** The intended outcome of risk management is mitigation, so management will need details about why a particular risk cannot be mitigated.

- **Compensating controls:** Even if a risk cannot be directly treated to meet the organization's risk threshold, it may be possible to partially mitigate with compensating controls such as increased monitoring.

- **Exception approval:** Management must make an explicit decision to assume additional risk, and documenting the review and approval process provides accountability for this decision.

- **Time:** Most exceptions should be granted on a temporary basis. If the identified deficiency requires a long-term plan to address the risk, such as a major IT project, the exception should be granted only for the anticipated time required to complete the project.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Ethical Disclosure

There is a growing community of security researchers who identify and report these issues to the organization responsible for the affected resource, with the goal of responsibly disclosing the vulnerability before a malicious actor can find it. These researchers are often ethical hackers, and this process is known as ethical or responsible disclosure.

The special circumstances for responsibly disclosing findings include the following:

- Nondisclosure: There may be contractual or legal obligations that prevent disclosure of a vulnerability; for example, when disclosing a vulnerability might compromise an active criminal investigation.

- Full disclosure: This is a philosophical argument that any time a weakness is discovered, it should be fully and transparently reported to the organization responsible for fixing it as soon as possible. While the goal of improving security is admirable, many vendors may be hostile to researchers who attempt to report vulnerabilities.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Ethical Disclosure

- **Responsible disclosure:** This principle defines a responsibility for the discoverer to report a weakness to the organization in a timely manner and give the organization time to fix the vulnerability before publicly disclosing it.

- **Mandatory reporting:** In certain circumstances, reporting a discovered vulnerability to law enforcement or other authorities may be mandatory. Legal and regulatory frameworks around the world vary, so this can be a difficult situation if the discoverer is in one jurisdiction but the organization responsible for the software or system is in another.

- **Whistleblowing:** A whistleblower is someone who feels ethically obligated to report a dangerous or illegal situation, and many jurisdictions have laws designed to protect whistleblowers from retribution for reporting.

- In the case of discovered security vulnerabilities, whistleblowers may be protected from prosecution for copyright infringement or other digital crimes if they follow proper channels for disclosing discovered vulnerabilities.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Internal and 3rd-Party Audits

- Internal audit
  - Structured audits – external audience, validate compliance, etc.
  - Unstructured audits – internal audience, improve security, etc.
- 3rd-Party audits
  - Experts (hopefully)
  - Adds credibility
  - Teach

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Designing an Audit Program

- An organization's audit program can be designed to conduct internal audits, facilitate external audits, or both if needed. Appropriate resources, oversight, and support from management are essential, as is a realistic schedule for performing audits. One-off, point-in-time audits provide a useful snapshot of a security program, but a recurring audit schedule allows the program to be tracked over time and show improvements.

Common Audit Frameworks

- If an organization is pursuing a specific type of audit, such as FedRAMP or SOC 2, then the audit program will be dictated by the standard, as this is what external auditors are required to follow.

- The audit frameworks may also be used as a guide to best practices when designing an internal program.

- In fact, designing an internal program aligned to the same standard an external auditor uses makes sense, as it allows the organization to uncover the same issues an external auditor might find.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Designing an Audit Program

These are common information security frameworks that provide a standard against which to perform an audit:

- SSAE 18 is the Statement on Standards for Attestation Engagements that is used by auditors when performing audits for SOC 2.

- ISO/IEC 15408-1:2009, "Information technology — Security techniques — Evaluation criteria for IT security," is the foundation for the Common Criteria certification, which is a formal assessment process for technology products against a defined set of security functional requirements. This document and ISO/IEC 18045 are available free of charge.

- ISO/IEC 18045:2008, "Information technology — Security techniques — Methodology for IT security evaluation," is a companion to ISO 15048 and provides standards for consistent criteria and evaluation methods.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

- ISO/IEC 27006:2015, "Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems," is the official set of requirements and guidance for auditors performing certification audits against ISO 27001.

- NIST Special Publication (SP) 800-53A, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," is a guide to assessing the controls outlined in NIST SP 800-53. It introduces a simple set of testing procedures to assess control effectiveness: test, examine, or interview. Although applicable to U.S. government agencies, it is freely available and may be adapted for use by any organization.

- The NIST Cybersecurity Framework (CSF) and FedRAMP Security Assessment Framework (SAF) are both freely available as well and may be used to perform assessments with evaluation methods similar to those in NIST SP 800-53A.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Sampling

When designing an audit program, the cost of work to gather information and gain assurance should be balanced against the benefit of risk visibility. Sampling is a technique utilized in audits to reduce work while maintaining assurance that deficiencies are identified.

Internal Audits

An internal audit is conducted by the staff of an organization and offers the benefit of auditor familiarity with processes, tools, and personnel.

103

LECTURE

Agenda – Domain 6: Security Assessment and Testing

External Audits

An external audit is performed by personnel from outside the organization and is often a requirement for regulatory compliance audits.

- The key advantage of an external auditor is total independence from the organization being audited — the auditors are invested fully in the process of conducting the audit and should have no conflict of interest to overlook or suppress findings.

Third-Party Audits

Third-party audits are a vital risk management tool used for external suppliers, vendors, and partners. A security practitioner may be in charge of conducting such an audit or be a consumer of an audit report provided by the external party.

LECTURE

Agenda – Domain 6: Security Assessment and Testing

And now we're done…

LECTURE

Agenda – Domain 6: Security Assessment and Testing

Let's get a jump start on Domain 7: Security Operations.

And now we're done…

Or are we?!

106

2023

Class #9 – Domain 6

Ryan Cloutier

President of SecurityStudio & vCISO
Infosec Missionary on a Mission