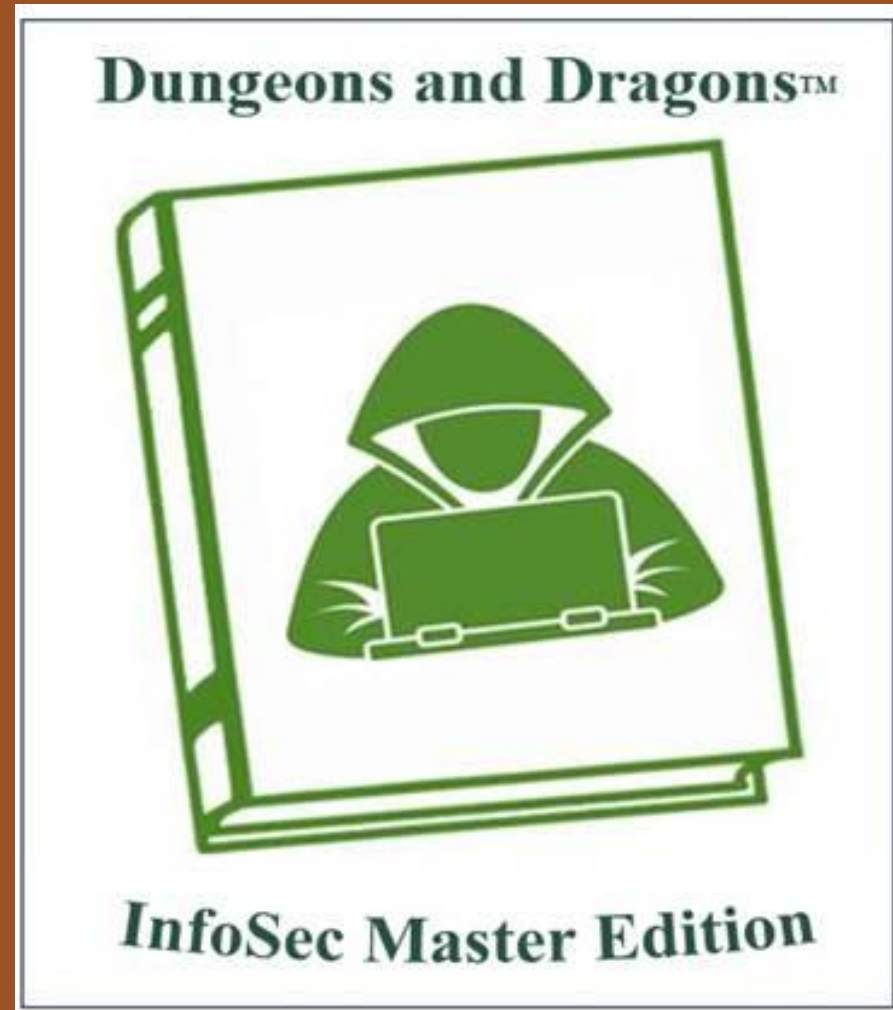


Welcome To The 10th Annual Hacking Conference



Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session
on the app!





How to Plan Effective Pentests

Josh Schmidt
Sam Zarn

October 2023

Who Are We

Josh Schmidt

Partner, CyberSecurity Assessment

- Senior penetration tester
 - Eight years offensive security
 - Ten years system administration
- University of Oregon
- Personal Interests
 - Compression ignition engines
 - Rugby
 - Property remodeling

jschmidt@bpm.com



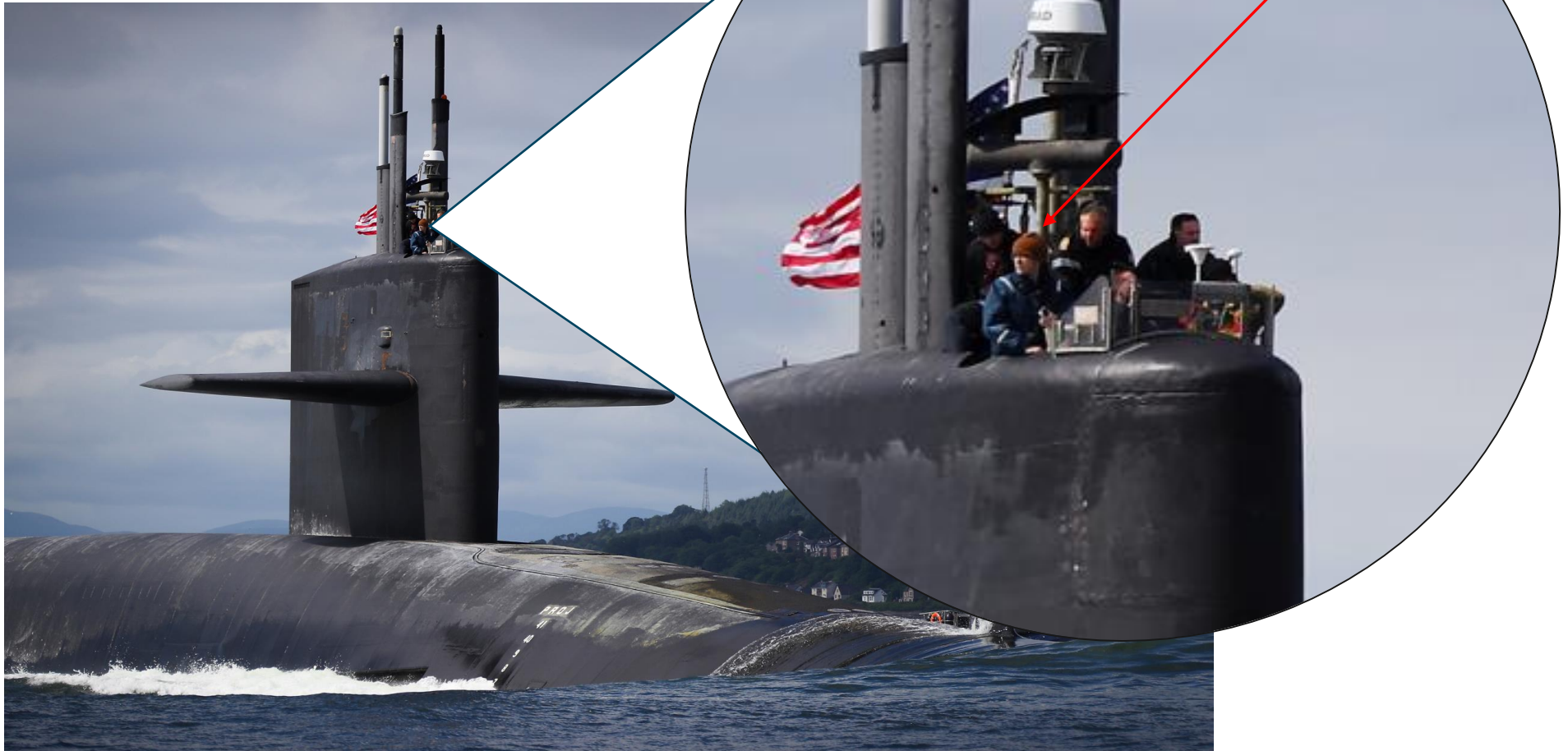
Sam Zarn

- Senior Penetration Tester
 - Network
 - Cloud
 - OT/SCADA
 - Wireless
- Process Engineer
 - Oregon State University, cum Laude, 2014
- Radio Hobbyist
- Former Submariner



szarn@bpm.com

Sam Zarn



What BPM does

Assurance

Strengthen your business with in-depth, unbiased and accurate assessments from experienced auditors who have a comprehensive understanding of your industry.

Advisory

With vast experience across industries, capabilities and backgrounds, our advisory team is fully equipped to support you through every phase of your business life cycle — from start-up to exit.

Tax

We support all your corporate, international and private accounting needs — including helping you find credits you didn't know were available to you, navigating international tax obligations and managing your charitable giving.

What we do

Assurance

- AUDIT >
- IT ASSURANCE >
- RISK ASSURANCE >

Advisory

- BUSINESS APPLICATIONS >
- BUSINESS TRANSFORMATION >
- MANAGED SERVICES >
- TECHNOLOGY SOLUTIONS >

Tax

- CORPORATE TAX >
- FLOW-THROUGH >
- INTERNATIONAL TAX >
- NATIONAL TAX SERVICES >
- PRIVATE CLIENT SERVICES >

- BUSINESS APPLICATIONS
- CYBERSECURITY ASSESSMENT
- IT CONSULTING & MANAGED IT
- IT SECURITY
- SECURITY OPERATIONS CENTER (SOC)

- BPM’s CyberSecurity Assessment team personnel are experts at defeating security controls and providing controls assurance
 - Emulate threat actors through the perspective of an ethical hacker

Overview

Agenda

- Goals
- Scoping
- Budgeting
- Vendor Evaluation
- Value “Adds”
- Common Pitfalls
- Lessons Learned


What is a Pentest?

- “Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.” – NIST SP 800-115
- Risk
 - $\text{RISK} = (\text{LIKELIHOOD of vulnerability being exploited}) * (\text{IMPACT if the vulnerability is exploited})$
 - Risk ratings lend themselves to prioritization of vulnerabilities
 - Prioritization \neq triage
- Provides empirical evidence demonstrating the real-world impact of identified vulnerabilities

Polling Question #1

- What penetration testing model provides the tester with credentials to test authenticated functionality, but no direct access to privileged information or source code?
- A) Black Box
- B) Grey Box
- C) White Box
- D) None of the above

Polling Question #1

- What penetration testing model provides the tester with credentials to test authenticated functionality, but no direct access to privileged information or source code?
- A) Black Box
- B) Grey Box 
- C) White Box
- D) None of the above

What is a Pentest?

Degrees of Insight:

- Black Box
 - Testing is performed with no prior knowledge of underlying systems
- Grey Box
 - Partial knowledge of systems is provided
 - Credentials or low-level access may be provided
- White Box
 - Testing is performed open-book with complete transparency
 - Can be performed with the assistance of technical employees
 - Source code, configuration files, and documentation could all be provided
 - Benefits include:
 - Additional levels of testing rigor
 - Safer testing of mission critical systems
 - Increased efficiencies
 - Specific systems, security controls, or known vulnerabilities can be targeted



What *isn't* a Pentest?

Manage Expectations:

- A guaranteed locator of all vulnerabilities
- A prioritized list of issues
- A session in exploit development
- A redteam
- An end-all, be-all solution to your security woes



Identify your Goals

Compliance Requirements

- Credit Unions
 - 12 CFR § 748 Appendix A
- Banks
 - 12 CFR §30, §364 Appendix B
- Healthcare
 - HIPAA
- Payment Recipients
 - PCI
- Utilities
 - NERC CIP

Reasons for Pen Testing

Why does your organization perform penetration tests?

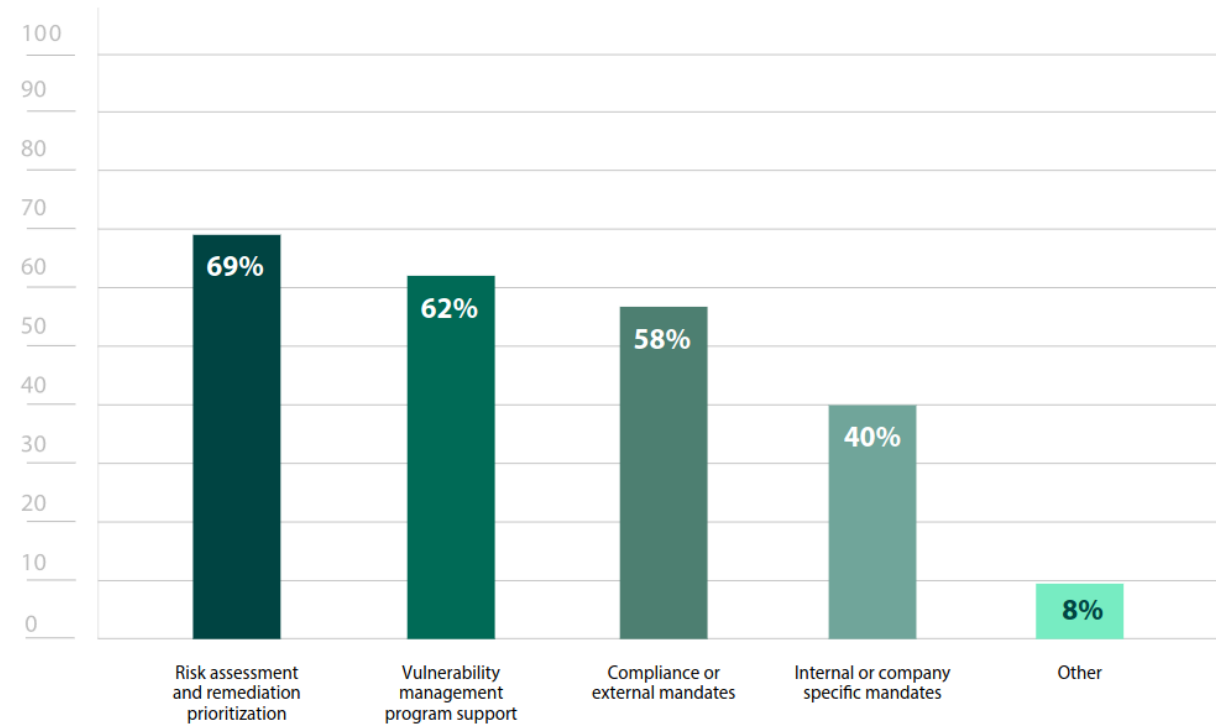


Figure 1: Reasons for performing penetration tests

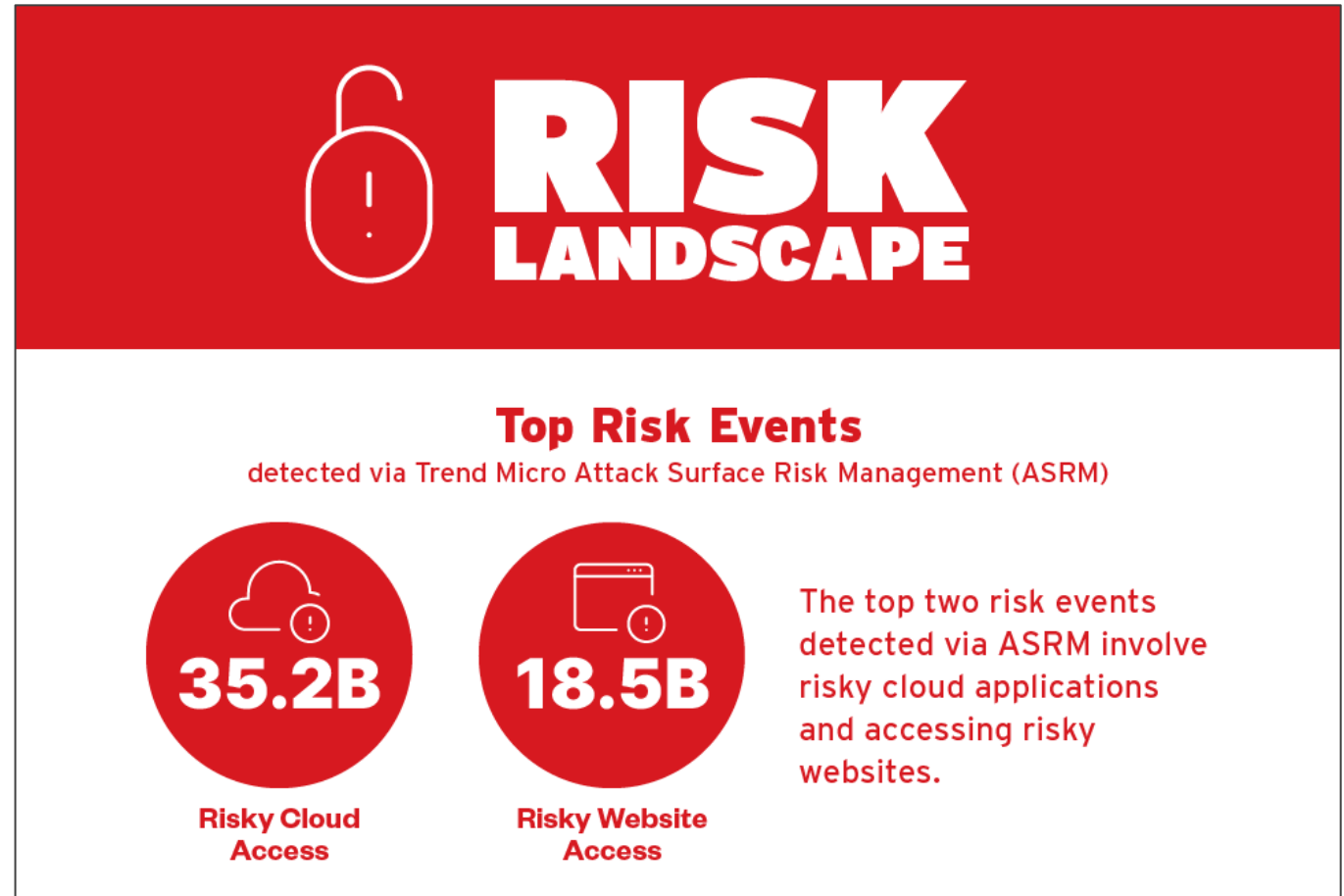
Strategic Plan

- Due Diligence
 - Self Assessment -> drive your own organization to a higher security standard
 - Remove yourself from the echo chamber
- Zero Trust
 - Paradigm shift
 - Erasing some internal/external boundaries
- Infrastructure Hardening
 - Business combinations
 - Infrastructure migrations
 - Datacenter relocation
- Migration to the Cloud
 - Running your stack on someone else's computer
 - Expanding the attack surface
- Cyber Insurance
 - Potential business requirements



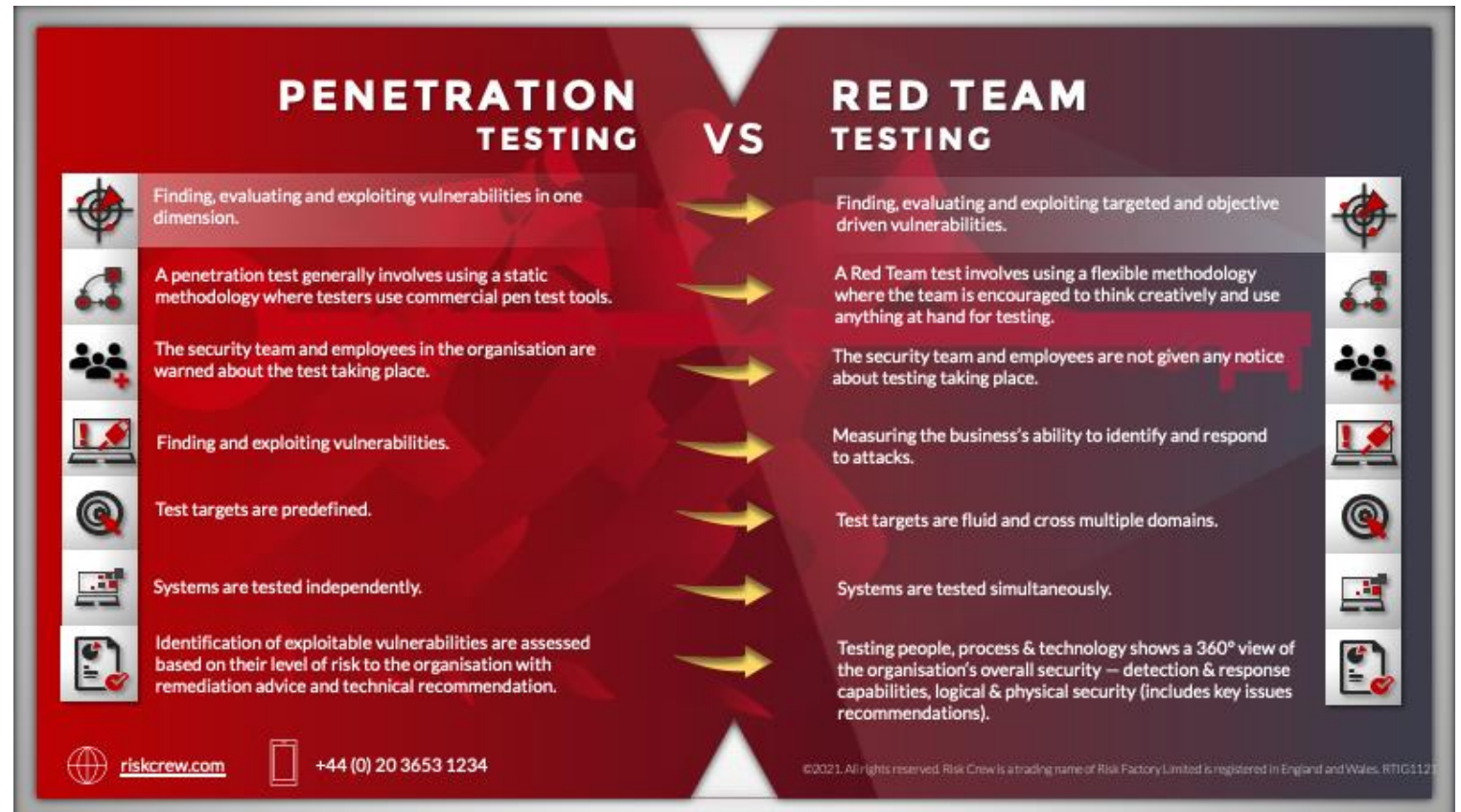
Threat Models

- Indiscriminate / opportunistic hackers
 - Sophisticated targeted threat actors
 - Malicious employee or vendor relation
 - Employee error through improper training or negligence
 - Physical breach
-
- What's most likely?



Redteam or Pentest?

- Consider your organization's InfoSec maturity
- A redteam engagement is likely to produce a much shorter list of findings
 - Also offers the potential to produce higher impact findings
- Does a redteam meet the same regulatory requirements?
 - Short answer -> No
 - PCI-DSS
 - https://listings.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf
 - NCUA & 12 CFR
 - <https://www.ecfr.gov/current/title-12/chapter-I/part-30>
- A value-add to a regular pentest?



Tricks of the Trade

- Adopt a methodology rooted in standards
 - NIST SP 800-53 and NIST SP 800-115
- Make room for “unknown unknowns”
 - A prescriptive check-box approach only proves/disproves what’s already known
- Develop a remediation strategy template *before* you begin
 - You don’t have to know what’s wrong, how long it’ll take to fix, or how much it’ll cost to have a procedure for addressing it
 - Responsible Party
 - Timeline
 - Retest & Validation
 - Internal reporting & Communication

Identification \ Certainty		Certain (Known)	Uncertain (Unknown)	
			Impact	Occurrence
Identified (Known)		Known known (identified knowledge)	Known unknown (identified risk)	
Unidentified (Unknown)	Consequence	Unknown known (untapped knowledge)	Unknown unknown (unidentified risk)	
	Event			

Define a Scope

What's Required?

- Compliance-Based
 - 12 CFR §30, §364, & § 748.0
 - PCI
 - HIPAA
 - NERC/CIP
 - FedRAMP
- Regulations define the minimum set of required controls but are often vague by design
 - Require knowledgeable internal resources to satisfy them while coordinating meaningful assessments
- Rules of Engagement (RoE)

- Strategic Goals
 - Defense in depth
 - Zero-trust
 - Security incident remediation
 - Continuous Improvement



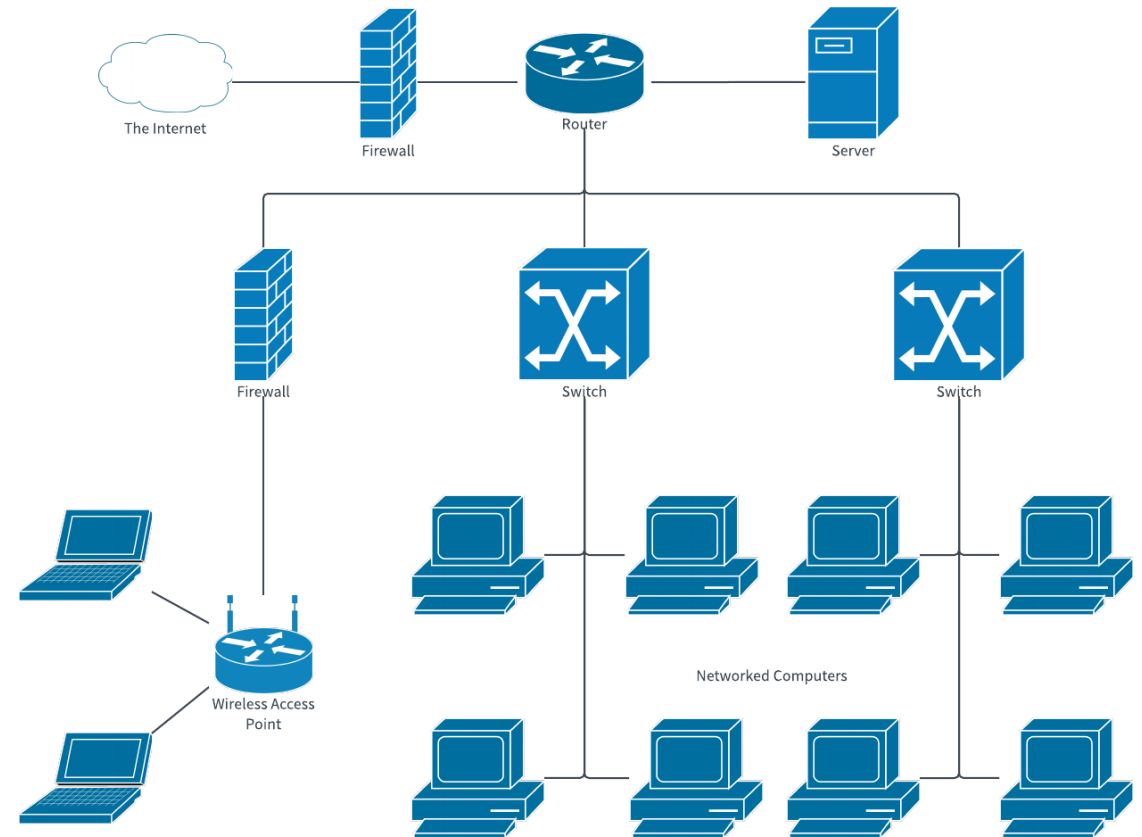
Internal, External?

A classic comprehensive penetration test includes the following:

- External technical assessment
 - Include all company-owned/ISP leased public facing IP addresses
 - Inbound email security controls
 - Employee social engineering
 - Phishing
 - Phone calls, SMS
- Internal technical assessment
 - Assumed breach of internal network access
 - Could be from: VPN account, vendor 3rd party access, employee workstation, physical controls
 - Leverage an internal footprint to evaluate as many paths as possible to the institution's "crown jewels"

Exclusions:

- Minimize number of excluded assets
- Risk-based analysis
 - Can compensating controls be used to allow testing?
- Can the vendor perform a "white-glove" approach?



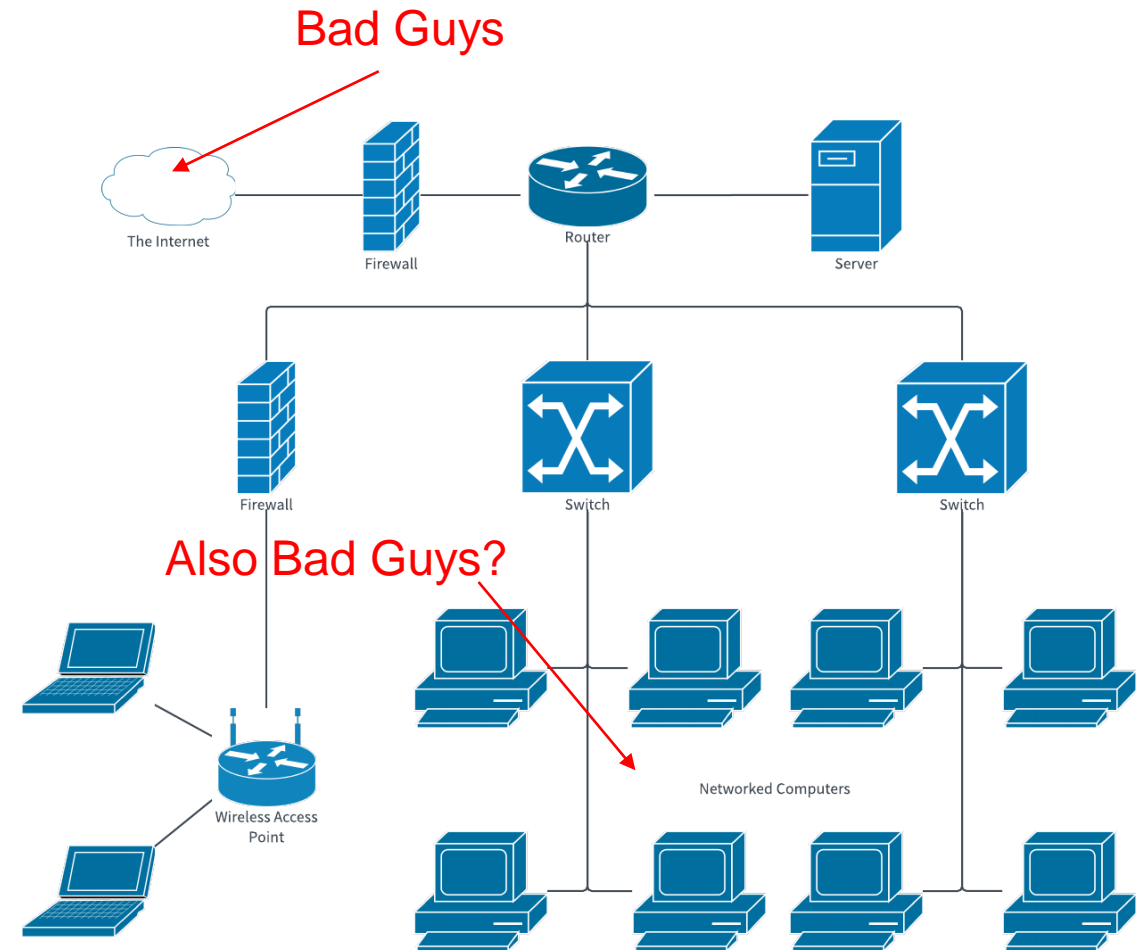
Internal, External?

A classic comprehensive penetration test includes the following:

- External technical assessment
 - Include all company-owned/ISP leased public facing IP addresses
 - Inbound email security controls
 - Employee social engineering
 - Phishing
 - Phone calls, SMS
- Internal technical assessment
 - Assumed breach of internal network access
 - Could be from: VPN account, vendor 3rd party access, employee workstation, physical controls
 - Leverage an internal footprint to evaluate as many paths as possible to the institution's "crown jewels"

Exclusions:

- Minimize number of excluded assets
- Risk-based analysis
 - Can compensating controls be used to allow testing?
- Can the vendor perform a "white-glove" approach?



Third Party?

- Common third party utilization:
 - Hosted website/blog
 - Online Banking App
 - eCommerce
- What attack surface do these third parties provide for you?
 - Are they tied to other internally managed infrastructure?
- Consider that vendors may bracket host counts, so the addition of several third party hosts may not change cost
- Cloud Assets?

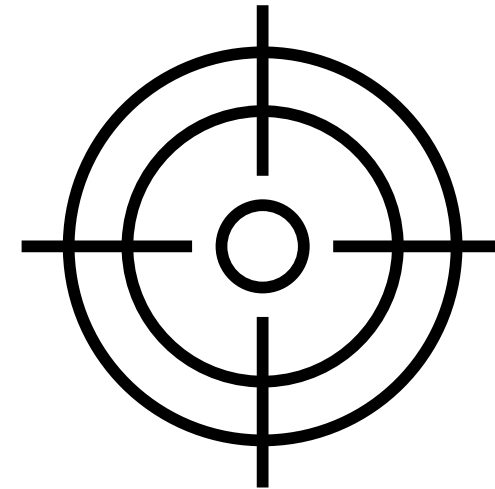
Third Party?

- Common third party utilization:
 - Hosted website/blog
 - Online Banking App
 - eCommerce
- What attack surface do these third parties provide for you?
 - Are they tied to other internally managed infrastructure?
- Consider that vendors may bracket host counts, so the addition of several third party hosts may not change cost
- Cloud Assets?
 - Azure – no notification/permission required
 - <https://learn.microsoft.com/en-us/azure/security/fundamentals/pen-testing>
 - GCP – no notification/permission required
 - <https://support.google.com/cloud/answer/6262505?hl=en#zippy=%2Cdo-i-need-to-notify-google-that-i-plan-to-do-a-penetration-test-on-my-project>
 - AWS – no notification/permission required
 - <https://aws.amazon.com/security/penetration-testing/>



Bonus Attack Surface

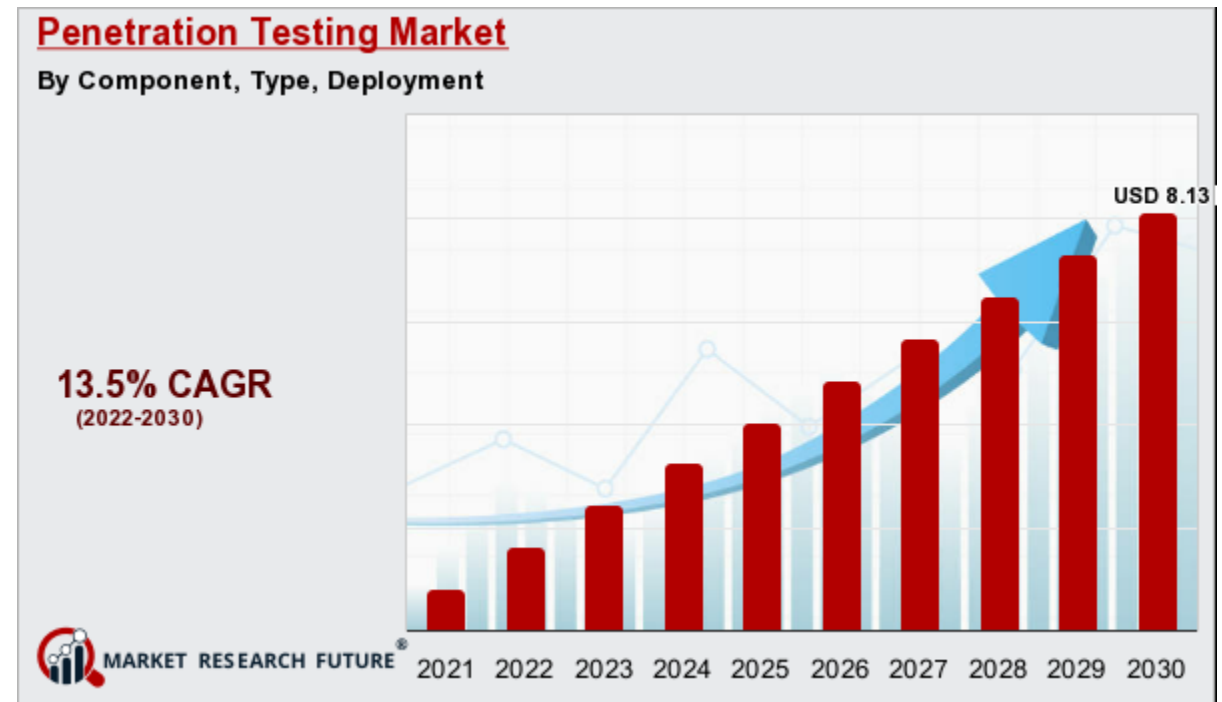
- Social Engineering
 - Phishing
 - Phone-based social engineering
 - In person
- Physical security testing
 - Open book assessment of all physical security controls such as: buildings doors, locks, electronic access systems, cameras, etc.
- Wireless infrastructure
 - More than just wifi
- Operational Technology
 - SCADA/ICS
 - Building Automation



Budgeting

How much is enough?

- Enough to cover:
 - Full scope and complexity of environment
 - Fulfilling all regulatory requirements
 - Meeting all organization goals
 - Testing at the depth desired
- But wait, there's more...
 - Remediation efforts
 - Long-term planning
 - Software/License changes
 - Additional security products
 - Increased cost as organization grows



How much is too much?

- It depends
- The same factors outlined in scoping are the factors that affect cost
 - Internal
 - External
 - Number of hosts
 - Social engineering
 - Complexity
 - Specific web application testing?
 - API testing
 - Password audit
 - Configuration review
- What's the cost of *not* doing a pentest?



Evaluate Vendors

Polling Question #2

- What is the typical document used to solicit services from a variety of potential vendors?
- A) RFP
- B) RFC
- C) RFB
- D) RFQQ

Polling Question #2

- What is the typical document used to solicit services from a variety of potential vendors?
- A) RFP ←
- B) RFC
- C) RFB
- D) RFQQ

What Goes in an RFP?

- Everything you care about and nothing you don't
- Be specific
- Highlight goals and desired outcomes as well as reasons for submitting the RFP
- Don't put lipstick on the pig
 - Vendors don't need to see your knowledge of jargon any more than you need to see theirs
- Include:
 - Scope of work
 - Deliverables
 - Qualifications or Due Diligence
 - Budget
 - Timeline
 - How you'll evaluate responses



What Goes in an RFP?

Real world take:

- The Ask:
 - “What’s one thing you wish was included in RFPs more often?”

What Goes in an RFP?

Real world take:

- The Ask:
 - “What’s one thing you wish was included in RFPs more often?”
- The Answers:
 - More context surrounding project goals
 - “I think one of the problems within our industry is that there are not clear terms of what specific services entail, so when there are industry buzz words being used to describe desired services, it makes it harder to understand how to actually respond to what they are looking for.”

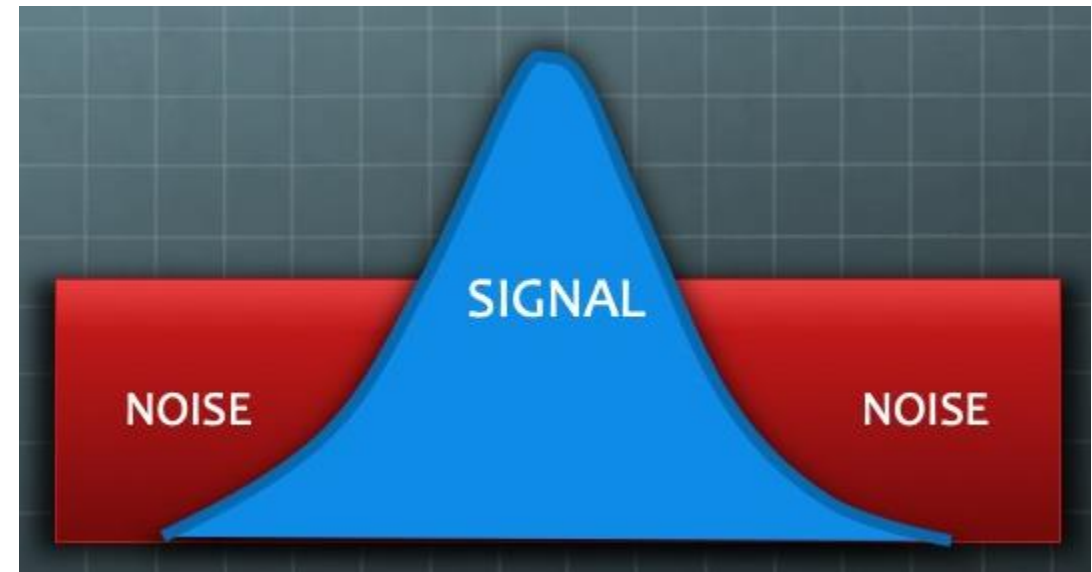
What Goes in an RFP?

Real world take:

- The Ask:
 - “What’s one thing you wish was included in RFPs more often?”
- The Answers:
 - More context surrounding project goals
 - “I think one of the problems within our industry is that there are not clear terms of what specific services entail, so when there are industry buzz words being used to describe desired services, it makes it harder to understand how to actually respond to what they are looking for.”
 - Scoping data
 - “RFPs in my experience are either too much info that needs clarifying or missing details that would make it easier to respond.”

Talk it Out

- Ask pointed questions to lower the noise floor
- Define deliverable expectations
 - Detailed penetration test report
 - Specific reporting requirements?
 - Vulnerability summary
 - Letter of attestation
- Post assessment expectations
 - Technical presentation of findings
 - High-level executive presentation
 - Remediation validations or guidance



Polling Question #3

- In 2023, what do you think was the biggest challenge faced by survey participants with their penetration testing program?
- A) Trouble getting executive sponsorship and funding
- B) Inability to hire enough skilled personnel to do the testing
- C) Lack of qualified third parties to do the testing
- D) Lack of resources to act on findings / perform remediation

Polling Question #3

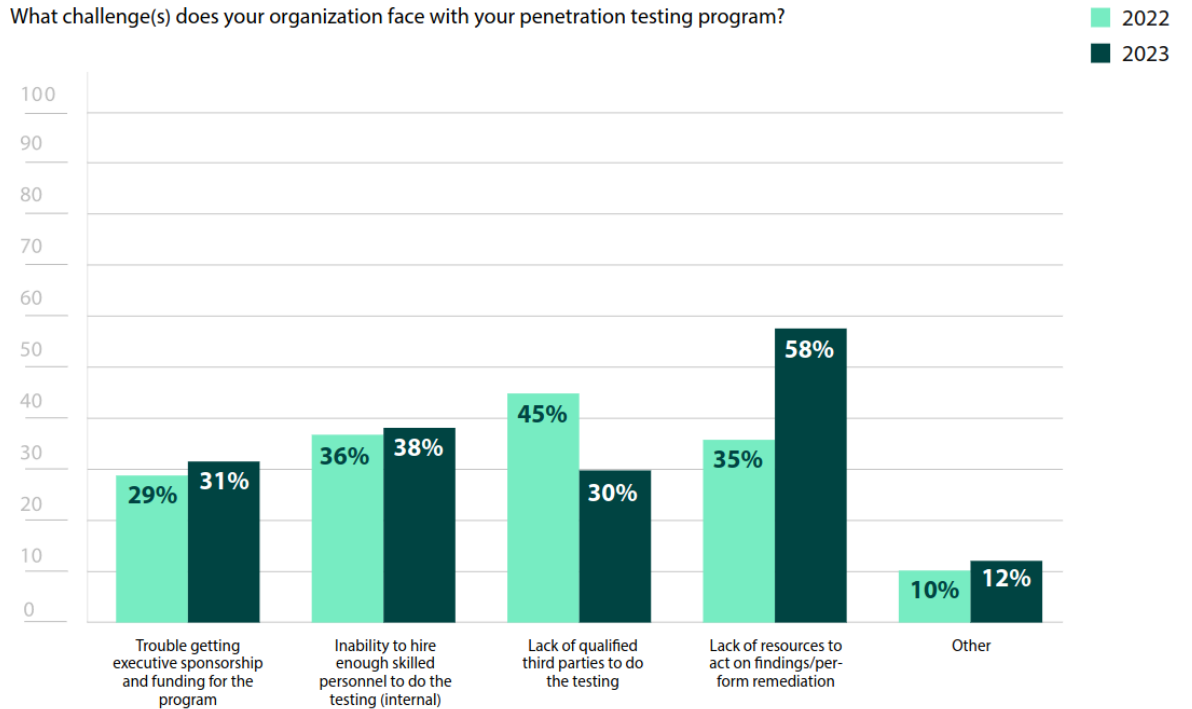
- In 2023, what do you think was the biggest challenge faced by survey participants with their penetration testing program?
- A) Trouble getting executive sponsorship and funding
- B) Inability to hire enough skilled personnel to do the testing
- C) Lack of qualified third parties to do the testing
- D) Lack of resources to act on findings / perform remediation ←

Drive the Process

- Ultimately you're paying for a nearly fixed number of hours
- Weigh in on things that matter to you
 - You're not paying for a list of problems, but a step toward formulating solutions

General Pen Testing Challenges

What challenge(s) does your organization face with your penetration testing program?



Drive the Process

- Ultimately you're paying for a nearly fixed number of hours
- Weigh in on things that matter to you
 - You're not paying for a list of problems, but a step toward formulating solutions
 - Should they spend time on discovery and OSINT, or do you care about focusing the time allotted on exploitation
 - Disclosure of assets and critical endpoints



Value “Adds”

Common Examples

- OSINT / Content Discovery
- Security Training Workshops
- Retest / Remediation Verification
- Executive/Board/Audit Reporting
- Program Review
- Configuration Review
- Password Audit
- Redteam?



Is It Worth It?

- Consider whether or not the process will take the assessor's time to complete
- Is this a service you'd consider paying additional for separate from your pentest?
- An exercise:
 - If the service is of interest, what would an RFP for it look like?
 - What would your budget be?
 - What deliverables would you expect?
 - What timeline is acceptable?
- Just because it's an add-on doesn't mean it's a second-rate citizen



Common Pitfalls

Planning, Planning, Planning

- Internal communication
 - Early
 - Often
- Lack of time allocation from the test-taker
 - A penetration test is not hands-off
- Develop a response plan to the published findings
 - Triage doesn't always follow severity
 - How much time and effort will it take to remediate a finding?
 - Hold your organization to small, measurable, achievable remediation goals to fulfill the larger picture
 - Your testing is wasted if you don't act



Lessons Learned

No Mistake Twice

- Don't assume scoping is prescriptive
 - OSINT had begun for a pentest prior to having preliminary scoping information and an RoE call complete
- Who's running the meeting?
 - Does your vendor provide a formalized results call?
 - Are you scheduling it as the client?
- Who has PTO planned?



Communication Breakdown

- Difference in understanding and desire between teams
 - Internal Audit
 - Information Security
- Misunderstanding of the service agreed upon
 - Vulnerability assessment \neq penetration test



Conclusion

Key Takeaways

- Develop a plan early
 - Iterate often
- Keep the reason you're conducting a pentest at the forefront
- Communicate
- Evaluate add-ons as a separate service
- RFPs
 - Present what is valuable to you
 - Skip the filler & jargon
 - Provide context and goals

References

- <https://www.stratcom.mil/Media/News/News-Article-View/Article/1895032/uss-alaska-ssbn-732-arrives-at-hmnb-clyde/>
- <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
- <https://asmed.com/black-box-grey-box-white-box-testing/>
- https://t3.ftcdn.net/jpg/01/82/34/44/360_F_182344447_cBOWy2b9uLQZPIR7subUd7qC8u6cKipn.jpg
- <https://static.fortra.com/core-security/pdfs/guides/cs-2023-pen-testing-report-gd.pdf>
- <https://www.gartner.com/en/insights/strategic-planning>
- https://documents.trendmicro.com/images/TEx/articles/Risk_Landscape_infographic-aypd962.png
- <https://www.riskcrew.com/wp-content/uploads/2022/02/Penetration-Testing-vs-Red-Team.png>
- <https://www.pmi.org/learning/library/characterizing-unknown-unknowns-6077>
- <https://www.complianceforge.com/product/security-by-design-privacy-by-design/>
- <https://d2slcw3kip6qmk.cloudfront.net/marketing/pages/chart/examples/officenetworkdiagram.png>
- <https://www.padok.fr/blog/aws-gcp-azure>
- <https://www.marketresearchfuture.com/reports/penetration-testing-market-5847>
- <https://www.meetingsnet.com/strategic-meetings-management/how-elevate-e-rfp-process-10-best-practices>
- <https://www.dirkstanley.com/2020/01/signal-to-noise-provider-communication.html>
- <https://static.fortra.com/core-security/pdfs/guides/cs-2023-pen-testing-report-gd.pdf>
- <https://www.dumblittleman.com/2010/05/how-to-really-begin-adding-value.html>
- <https://www.managementguru.net/advantages-of-planning/>
- <https://humornama.com/meme-templates/spiderman-pointing-meme-template/>
- <https://www.cnn.com/interactive/2018/10/entertainment/led-zeppelin-cnnphotos/>

Questions?

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session
on the app!

