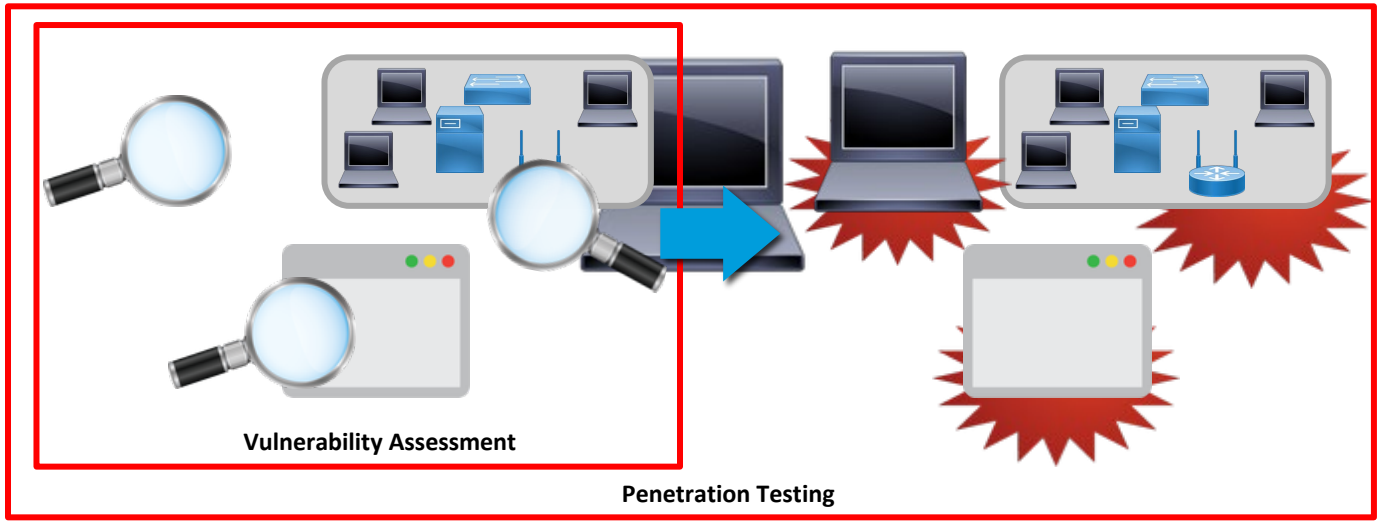
Planning and Scoping Penetration Tests

- Introduction to Penetration Testing Concepts
- Plan a Pen Test Engagement
- Scope and Negotiate a Pen Test Engagement
- Prepare for a Pen Test Engagement

Penetration Testing

Vulnerability assessment: The practice of evaluating a computer, network, or application to identify potential weaknesses.

Penetration testing (pen testing): The practice of evaluating a computer, network, or application to identify potential vulnerabilities, and then exploiting them to gain unauthorized access to key systems and data, and culminating in the production of evidence and a report.



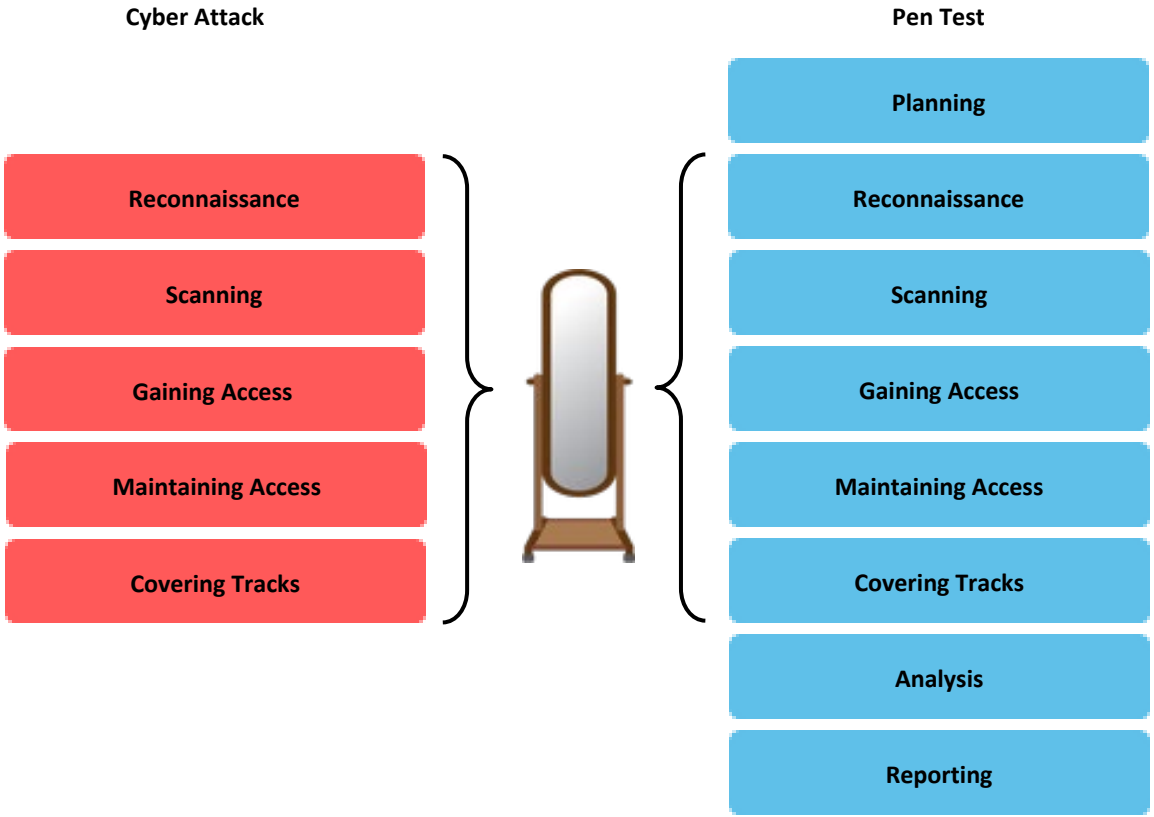
Benefits of Pen Testing

- Testing cyber-defense capabilities.
- Revealing vulnerabilities.
- Finding and plugging security holes before they can be exploited.
- Supporting risk management.
- Enhancing QA.
- Ensuring business continuity.
- Protecting clients, partners, and others.
- Protecting organizational reputation.
- Ensuring regulatory compliance.
- Maintaining trust.
- Identifying ROI.

Pen Testing Standards and Frameworks

Standard or Framework	Description
CHECK framework	• Developed by UK government. • Intended to ensure that government agencies and public entities can contract with government-approved pen testers.
OWASP testing framework	• Developed by Open Web Application Security Project. • Covers all sorts of software testing, including pen testing.
OSSTMM	• Open Source Security Testing Methodology Manual • Pronounced “awstem.“ • Security testing and analysis for better operational security.
PTES	• Penetration Testing Execution Standard • Developed by security service practitioners. • Basic lexicon and guidelines for pen tests. • General standard; the PTES Technical Guide provides specifics.
NIST SP 800-115	• Technical Guide to Information Security Testing and Assessment. • Developed by NIST. • Practical recommendations for designing, implementing, and maintaining pen test processes and procedures.

Processes Commonly Used for Pen Testing (Slide 1 of 2)



Processes Commonly Used for Pen Testing (Slide 2 of 2)

Tools Commonly Used in Pen Testing (Slide 1 of 4)

Tool Type	Examples
Scanning tools	• Nmap • Nikto • OpenVAS • SQLmap • Nessus
Credential testing tools	• Hashcat • Medusa • THC-Hydra • CeWL • John the Ripper • Cain and Abel • Mimikatz • Patator • Dirbuster • W3AF

Tools Commonly Used in Pen Testing (Slide 2 of 4)

Tool Type	Examples
Debugging tools	• OLLYDBG • Immunity debugger • GDB • WinDBG • IDA
Software assurance tools	• Findbugs and findsecbugs • Peach • AFL • SonarQube • YASCA
OSINT tools	• Whois • Nslookup • FOCA • theHarvester • Shodan • Maltego • Recon-ng • Censys

Tools Commonly Used in Pen Testing (Slide 3 of 4)

Tool Type	Examples
Wireless tools	• Aircrack-ng • Kismet • WiFite • WiFi-Pumpkin
Web proxy tools	• OWASP ZAP • Burp Suite
Social engineering tools	• SET • BeEF
Remote access tools	• SSH • Ncat • Netcat • Proxychains

Tools Commonly Used in Pen Testing (Slide 4 of 4)

Tool Type	Examples
Networking tools	• Wireshark • Hping
Mobile tools	• Drozer • APKX • APK Studio
Miscellaneous tools	• Searchsploit • Powersploit • Responder • Impacket • Empire • Metasploit Framework

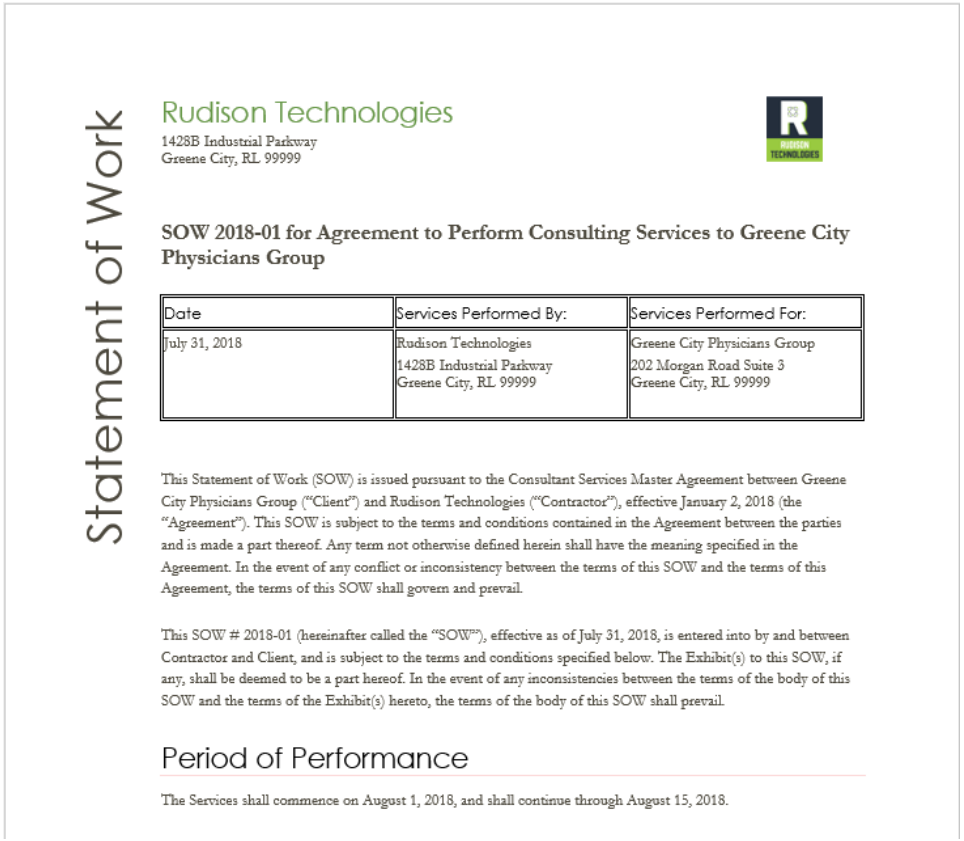
Communication and the Pen Testing Process

- Communication path, or chain of command.
- Communication with client counterparts.
- Communication within the pen testing team.
- What information to communicate and when.
- Regular process briefings.
  - Within the team.
  - With the client.
- Clear identification of the reasons behind communication actions.
- Possible adjustments to the engagement.
- Disclosure of findings.

Contract Types

MSA **Master service agreement**	An agreement that establishes precedence and guidelines for any business documents that are executed between two parties.
NDA **Non-disclosure agreement**	A business document that stipulates the parties will not share confidential information, knowledge, or materials with unauthorized third parties.
SOW **Statement of work**	A business document that defines the highest level of expectations for a contractual arrangement.

A Sample SOW



Statement of Work

Rudison Technologies

1428B Industrial Parkway
Greene City, RL 99999

SOW 2018-01 for Agreement to Perform Consulting Services to Greene City Physicians Group

Date	Services Performed By:	Services Performed For:
July 31, 2018	Rudison Technologies 1428B Industrial Parkway Greene City, RL 99999	Greene City Physicians Group 202 Morgan Road Suite 3 Greene City, RL 99999

This Statement of Work (SOW) is issued pursuant to the Consultant Services Master Agreement between Greene City Physicians Group ("Client") and Rudison Technologies ("Contractor"), effective January 2, 2018 (the "Agreement"). This SOW is subject to the terms and conditions contained in the Agreement between the parties and is made a part thereof. Any term not otherwise defined herein shall have the meaning specified in the Agreement. In the event of any conflict or inconsistency between the terms of this SOW and the terms of this Agreement, the terms of this SOW shall govern and prevail.

This SOW # 2018-01 (hereinafter called the "SOW"), effective as of July 31, 2018, is entered into by and between Contractor and Client, and is subject to the terms and conditions specified below. The Exhibit(s) to this SOW, if any, shall be deemed to be a part hereof. In the event of any inconsistencies between the terms of the body of this SOW and the terms of the Exhibit(s) hereto, the terms of the body of this SOW shall prevail.

Period of Performance

The Services shall commence on August 1, 2018, and shall continue through August 15, 2018.

Authorizations

- Written authorization to conduct pen testing activities.
- Document is often a SOW addendum.
- Control liability of pen testers.
- Third-party service providers.
- Contents:
  - Proper signing authority (statement and signature).
  - Identification of individuals who can perform the pen test.
  - What networks, hosts, and applications can be tested.
  - Time limits.
- Legal review.

Sample Authorization Template (Slide 1 of 2)

SOW Addendum: Authorization for Pen Testing

Scope

To properly secure the organization's information technology assets, the InfoSec team is responsible for periodic assessment and testing of the organization's security stance. When this testing includes penetration testing, in accordance with the Statement of Work (SOW) signed on *<sow-date>*, the following activities are considered to be necessary to complete the pen testing:

- Use social engineering and other techniques to gather information about the organization and its resources.
- Scanning desktop and laptop computers, servers, network devices, and any other computing devices owned by the organization.
- Using scan results to make further inroads to the network and its resources.

Purpose

The purpose of this document is to grant authorization to the undersigned members of the InfoSec team so that they can perform penetration tests against the organization's assets in accordance with the SOW signed on *<sow-date>*.

Sample Authorization Template (Slide 2 of 2)

Attestation

The following individual has the authority to grant permission for penetration tests to be conducted:

- *<name-of-signing-authority>*

The following people are granted permission to scan the organization's computer equipment to conduct penetration tests against organizational assets:

- *<name-of-tester-1>*
- *<name-of-tester-2>*

The time frame for conducting penetration tests is from *<start-date>* to *<end-date>*.

_____
<name-of-signing-authority>
<title-of-signing-authority>

<signing-date>

_____
<name-of-tester-1>
<title-of-tester-1>

_____
<name-of-tester-2>
<title-of-tester-2>

Legal Restrictions

- Export restrictions.
- Local and national governmental restrictions.
- Corporate or organizational policies.

Target Audience Types

- Types of information systems being tested will affect the target audience composition.
  - Hosts
  - Networks
  - Web servers
  - Applications
  - Databases
- Combination of upper management, IT management, IT personnel, and others.
  - Technical and non-technical people.
- Is the testing team internal or external?

Resources and Requirements (Slide 1 of 2)

Support Resource	Description
WSDL/WADL	XML documents that describe SOAP-based or RESTful web services.
SOAP project file	Enables testing of SOAP-based web services.
SDK documentation	Documentation for using development tools that support creating applications for a certain platform.
Swagger document	REST API equivalent of a WSDL document.
XSD	Defines the structure and data for an XML schema.
Sample application requests	• Like test code or code snippets. • Can assist pen testers in gaining access to resources.
Architectural diagrams	• Application architecture diagrams show possible points of weakness in apps. • Network architecture maps can reveal potential access points.

Resources and Requirements (Slide 2 of 2)

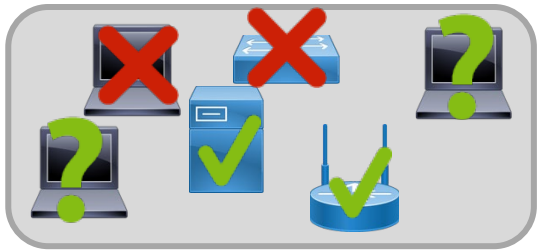
- Confidentiality of findings.
  - Pen tester discovers a major vulnerability.
  - Who gets informed of discoveries?
- Knowns and unknowns.
  - Pen tester discovers evidence of prior breaches.

Budget

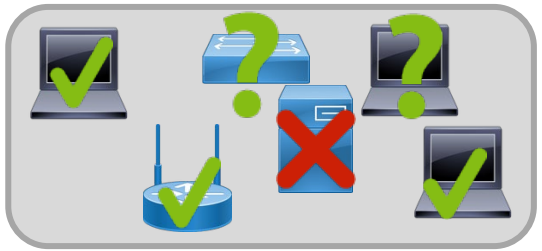
- Services provided must be worth the money that is spent.
- Budget has a significant effect on the pen test's scope.
- Service provider/pen tester:
  - Minimize expenses of testing.
  - Maximize revenue/compensation.
  - Provide acceptable QoS to client.
- Service consumer/client:
  - Minimize costs.
  - Maximize volume/depth of testing.
  - Maximize QoS.

Technical Constraints

- What is to be tested?
- What is not to be tested?
- What cannot be tested?
- Budgetary considerations.
- Examples:
  - Fragile legacy server
  - Third-party hosted website
  - Offshore data center



Headquarters



Satellite Office

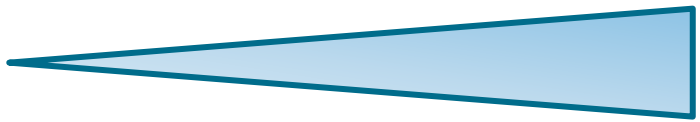
Rules of Engagement

Rules of engagement: In pen testing, a document or section of a document that outlines how the pen testing is to be conducted.

Component	Description
Timeline	• List of tasks that make up the engagement and who performs them. • Adjustable progress indicator. • Often in Gantt chart format.
Test team location	• Where test team is in relation to client properties. • Multiple locations, countries, and technologies should be considered.
Temporal restrictions	Days and times individual tests can be performed.
Transparency	• What client personnel are in the know? • What resources will be provided to the testers?
Test boundaries	• What gets tested? • Acceptable social engineering test. • Acceptable physical security tests. • Restrictions on invasive attacks.

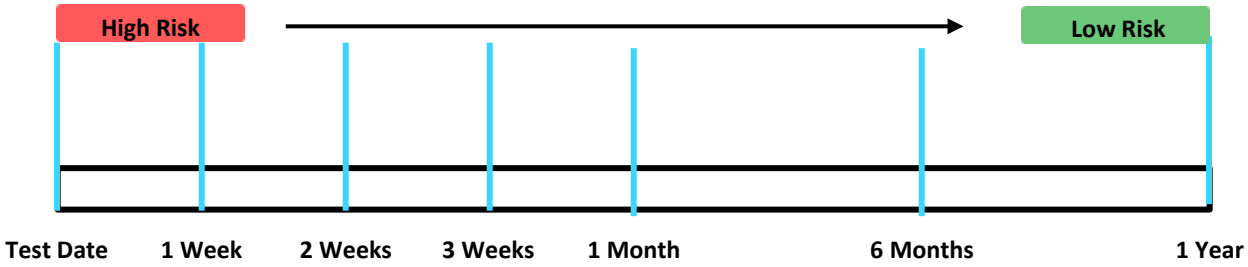
Impact Analysis

- What effect will the pen test have on normal business operations?
- Potential impact:
  - Target type
  - Criticality
  - Testing approach
- Unforeseen issues.
- Risk management is a team effort.
  - Triggers, escalation procedures, and timelines.
- Prioritization of pen test results.



Remediation Timeline

- Implementing solutions to eliminate vulnerabilities.
- What should be handled first?
  - High-risk
  - Low-cost
  - Other
- Where does risk acceptance come into play?



Disclaimers

- Point-in-time assessment
- Comprehensiveness
- Others?

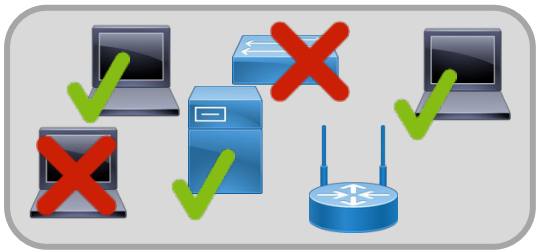
Guidelines for Planning Pen Test Engagements

- Be sure that you understand the target audience.
- Identify the resources and requirements that will govern and facilitate the pen test engagement.
- Determine any budget restrictions that might affect the engagement.
- Document any technical constraints that will affect the engagement.
- Clearly define the rules of engagement.
- Develop impact analysis and remediation timelines.
- Identify any disclaimers that will affect the engagement.

Scoping

Scope: In a pen test engagement, the boundaries that describe the extent of the engagement, including what specific systems are to be tested, to what degree the systems should be tested, and how the pen testers should spend their time.

- Crucial step in contract negotiations.
- Scope forms the basis of the SOW.
  - Defines appropriate targets and limitations.
- What happens when something outside the scope is discovered?
  - Pen test team response and escalation when necessary.

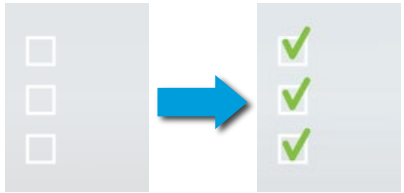


End Goals and Deliverables

- Identify why the testing is needed.
  - Compliance or legal requirement?
  - Need and desire for improving organizational security?
- End goals might be adjusted during the scoping process.
- Main deliverable is an actionable report.
  - Describes tests performed, vulnerabilities identified, analysis, and mitigation suggestions.
- Translate technical findings to potential organizational risk.
  - Threat ranking: probability x impact

Types of Assessments

- Goal- or objective-based:
  - What needs protection?
- Compliance-based:
  - Industry or governmental mandate.
- Red team

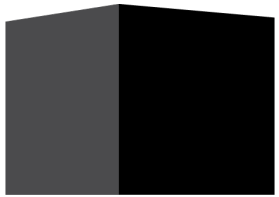


Compliance-Based Assessments

- Normally assessed using audits of administrative, technical, and physical controls.
- Takes precedence over organizational policy.
- What to look for: Clear objectives based on regulations.
- How to look: Possible rules for completing the assessment.
- Focus:
  - Password policies
  - Data isolation
  - Key management
- Limitations:
  - Network access
  - Storage access

Types of Strategies

Pen Test Strategy	Description
Black box test	• No information is provided to the pen tester. • Simulates an outsider attack with basic reconnaissance. • AKA zero knowledge test, because the tester must gather information about the target and verify the scope. • Few have knowledge of the test.
Gray box test	• Some information is provided to the pen tester. • Simulates an internal attack with limited knowledge. • AKA partial knowledge test, because the pen tester uses reconnaissance to gain more information about the target.
White box test	• Comprehensive information is provided to the pen tester. • Simulates an insider attack with full knowledge. • Opposite of a black box test. • Reconnaissance phase might be unnecessary.



Types of Threat Actors (Slide 1 of 2)

Threat actor: An entity partially or wholly responsible for an incident that affects or can affect an organization's security.

Script kiddies: Novice or inexperienced hackers with limited technical knowledge who rely on automated tools to hack into targets.

Hacktivists: Hackers who gain unauthorized access to and cause disruption in a computer system in an attempt to achieve political or social change.

APT: A threat that uses multiple attack vectors to gain unauthorized access to sensitive resources.

Insider threats: Present and past employees, contractors, partners, and any entities that have access to proprietary or confidential information and whose actions result in compromised security.

Types of Threat Actors (Slide 2 of 2)

Tier	Description
I	Those who invest a relatively small amount of money to use off-the-shelf tools to exploit known vulnerabilities.
II	Those who invest a relatively small amount of money to develop their own tools to exploit known vulnerabilities.
III	Those who invest millions of dollars to discover unknown vulnerabilities that enable them to steal personal and corporate data that they can sell to other criminal elements.
IV	Organized, highly technical, proficient, well-funded professionals who work in teams to discover new vulnerabilities and develop new exploits.
V	Nation states that invest billions to create vulnerabilities by influencing commercial products and services.
VI	Nation states that invest billions to carry out a combination of cyber, military, and intelligence operations to achieve a political, military, or economic goal.

Capabilities and Intent of Threat Actors

- Capabilities often related to tier assignment.
  - Lower-tier adversaries are less likely to have expensive or sophisticated capabilities.
  - Higher-tier adversaries can use tools and methods of the tiers below them.
- Intent and motivations can vary no matter what tier the adversaries occupy.
  - Greed/theft.
  - Power/revenge and blackmail.
  - Reputation and recognition/espionage and defamation of character.
  - Association or affiliation with others/political and social change.
  - Thrills and exploration/blackmail and defamation of character.

Threat Models

- Identify and classify potential attack methods/attack vectors.
- Models vary in scope.
  - Overall security of an organization.
  - Security of specific computers or other assets.
- Activity-focused or asset-focused.
- Help evaluate risks and mitigation strategies.
- Start from the end, and reverse engineer.
  - Bad result (data stolen or lost).
  - What steps would the attacker need to take?
  - Identify and implement controls to counter each step.
- Goal: Disrupt attack vectors so that bad results can't occur.

Types of Targets (Slide 1 of 3)

Target Type	Description	Attack Considerations
Internal	• Assets can be accessed from within the organization. • Possibly caused by malicious insiders or external hackers.	A good candidate for all attack types IF direct access to the internal network can be established.
On-site	Asset is physically located where an attack is occurring,	• Accessibility depends on site controls. • Physical attacks might be undetected at a large facility with many people. • Centralized resource locations will probably have more points of entry and attack vectors to choose from.
Off-site	Asset provides a service for an organization but is not necessarily located at the same place.	• Remote offices and satellite locations may have fewer security controls than headquarters. • Attackers lose the cover of anonymity, but physical, Wi-Fi, or remote access/VPN attacks might be viable. • Remote locations might provide a backdoor (such as an unguarded WAN or VPN link) to the main facility.

Types of Targets (Slide 2 of 3)

Target Type	Description	Attack Considerations
External	• Asset is visible on the Internet. • Websites, web applications, email, or DNS servers.	Not a good candidate for attacks (such as sniffing or ARP poisoning) that require direct access to the network segment.
First-party hosted	Hosted by the client organization.	• Might be easier to attack than third-party hosted services. • Most companies don't have the resources, expertise, or security focus that a provider does.
Third-party hosted	Hosted by a vendor or partner of the client organization.	• Not impossible targets, but established providers are more likely to have good controls in place. • Smaller, newer hosting companies may have fewer resources and less security expertise. • These might be easier to attack than larger, more mature providers. • All third parties can be vulnerable to zero-day attacks.

Types of Targets (Slide 3 of 3)

Target Type	Description	Attack Considerations
Physical	• Client organization's premises. • Any physical device belonging to the client organization.	Physical attacks are an excellent way to plant sniffers, remote-controlled devices, keyloggers, and other attack tools in the private network.
Users	Can have access to resources that might be restricted to outside parties.	Can be the easiest attack vector because they are so susceptible to social engineering.
SSIDs	Can be targets when an attacker is attempting to access a wireless network.	Evil twins and other Wi-Fi attacks require close physical proximity to the premises.
Applications	Can be targets, as they are often linked to sensitive data such as credit card numbers.	• Determine which applications are in use. • If an app runs in user context, try to escalate privilege once it is compromised.

Specialized Systems

Type of System	Description
ICSs	• Networked systems that control critical infrastructure. • Water, electrical, transportation, and telecom services.
Embedded systems	• Computer hardware and software systems that have a specific function within a larger system. • Home appliances or industrial machines.
SCADA systems	ICSs that send and receive remote-control signals to and from embedded systems.
IoT devices	Any objects (electronic or not) that are connected to the Internet by using embedded electronic components.
Mobile systems	Smartphones, tablets, wearable devices, and other portable devices.
PoS systems	Stations that typically consist of a cash register, barcode scanner, and a debit and credit card scanner.
Biometric devices	• Devices that identify individuals by their physical characteristics. • Thumbprint scanners, retinal scanners, voice-recognition software.
Application containers	Virtualized environments designed to package and run a single computing application or service and that can share the same host kernel.
RTOSs	Specialized operating systems that feature a predictable and consistent processor scheduler.

Risk Responses

Risk Response	Description
Avoidance	• Action taken to ensure that risk has been completely eliminated, or reduced to zero. • Terminating the process, activity, or application that is the source of the risk.
Transference	• Responsibility for risk management moved to another entity. • Insurance company, cloud service provider, or other outsourcing provider.
Mitigation	• Controls and countermeasures implemented to reduce the likelihood and impact of risk. • Goal is to reduce potential effects to within acceptable risk thresholds.
Acceptance	• Risks are identified and analyzed, and deemed to be within established limits. • No additional action required.

Tolerance to Impact

- Pen testing will affect performance.
  - Networks
  - Hosts
  - Applications
- Balance the need for testing with continuity of business operations.
- Determine which business operations and assets can be tested, and which should be left alone.

In Scope	Out of Scope
• Network storage • Intranet • Product databases • Employee email accounts • Time-tracking app	• E-commerce servers • Customer-facing websites • Email servers • R&D network

Scheduling

- Timeline to define when events should occur.
- Specify test days and hours, as well as duration.
  - DDoS to take place for up to one week, but only between 12:00 and 3:00 A.M.
  - Start date: 7/23/2018
  - End date: 7/30/2018
- Notifications to client stakeholders.

List of events

Date and time restrictions

Client stakeholder notifications

Scope Creep

Scope creep: The condition that occurs when a client requests additional services after a SOW has been signed and the project scope has been documented and agreed upon.

- Any type of project, not just pen testing.
- Takes resources and effort away from the items documented in the SOW.
  - Less time unless you add more testers.
  - Less diligent testing is possible.
  - Testing organization can be forced to take a financial loss.
  - Legal protection might be affected.
- Try to get another agreement to cover the additional work.
  - Extra time.
  - Extra money.
  - Possible reduction in costs for client.

General Considerations (Slide 1 of 2)

Consideration	Description
Organizational policies	• Formalized statements defining how long-term goals are to be met. • Policies can cover security, privacy, compliance, and acceptable use of resources, among other topics. • Pen test engagements should be designed to support and coordinate with existing policies.
Security exceptions	• In some organizations, you can apply for policy exceptions. • Certain policies not enforced for identified technologies or resources. • Determine if security exceptions should be within or outside the scope of the engagement.
NAC	• NAC is a collection of protocols, policies, and hardware governing device connection. • Health check required for network connection. • Agent-based or agentless.

General Considerations (Slide 2 of 2)

Consideration	Description
Whitelisting and blacklisting	• Whitelisting blocks all users/IP addresses except those specifically allowed. Blacklisting allows all users/IP addresses except those specifically denied. • Often used with IPSs and WAFs. • Whitelisting provides tighter security.
Certificate and public key pinning	• Pinning is the process of associating a host with its expected X.509 certificate or public key. • It bypasses the CA hierarchy and chain of trust, lessening the impact of man-in-the-middle attacks. • Used to secure wireless channels and protect against VPN, SSL, and TLS vulnerabilities.

Special Considerations for Scoping Engagements

Premerger security testing: A special type of security testing that takes place prior to an organizational merger.

Supply chain security: The practice of analyzing and implementing controls to ensure the protection of data that moves through an organization's production processes.

Scoping Checklists

GCPG Penetration Test Scope

What are the client's security concerns and reasons for authorizing the test?

Click or tap here to enter text.

What type of pen test assessment(s) should be conducted?

Click or tap here to enter text.

What type of threat actor(s) should the test simulate?

Click or tap here to enter text.

What background information should the client provide, if any?

Click or tap here to enter text.

What known networks, hosts, applications, and other assets should be tested?

Click or tap here to enter text.

What known networks, hosts, applications, and other assets should *NOT* be tested?

Click or tap here to enter text.

What third-party assets should be in the scope of the test?

Guidelines for Scoping and Negotiating Pen Test Engagements (Slide 1 of 2)

- Determine the types of assessments you want to conduct.
- Clearly define the end goals of the engagement.
- Determine what testing strategy you need to use.
- Determine what types of threat actors you want to emulate.
  - Capabilities and intent.
- Consider recommending threat modeling.
  - Clear definition of objectives and expectations.
- Identify all targets and the risk tolerance associated with each.
  - Conventional and specialized systems.

Guidelines for Scoping and Negotiating Pen Test Engagements (Slide 2 of 2)

- Account for existing controls and scenarios.
  - Org policies and security exceptions.
  - Whitelists and/or blacklists.
  - Certificate and public key pinning.
  - NAC devices and controls.
  - Premerger or supply chain security testing.
- Create, maintain, and adhere to a comprehensive schedule.
- Avoid scope creep.
  - Use disclaimer language to protect the test team.
- Use a scoping checklist.
- Identify each deliverable.
  - Documents
  - Meetings

Team Preparation (Slide 1 of 2)

- Prepare the client.
  - Gather technical points of contact.
  - Inform key IT personnel.
  - Verify the existence of current, verified backups of all critical systems.
  - Verify client personnel are aware of possible risks and will work with the pen test team to restore crashed or compromised systems.
  - Warn against stopgap security measures implemented before testing begins.

Team Preparation (Slide 2 of 2)

- Prepare the pen test team.
  - Clarify scope and limitations.
  - Verify testers know the objectives and deliverables.
  - Verify testers have contact information and escalation procedures available.
  - Have testers document all actions and outcomes in a central repository.
  - Verify testers have documented authorization for pen test activities.
  - Verify the project lead is managing the engagement schedule properly.
  - Verify testers know to report accidents or errors immediately.

Data Collection and Documentation (Slide 1 of 2)

- Follow a plan that maps pen tests to identified objectives.
- Verify all tests contribute to the client organization's goals.
- Document everything, including mistakes and accidents.
- Keep documentation clear, concise, and objective.
- Use a central repository to store test data.
- Collect as much data as you can.
- Upload test results and data in their original format.

Data Collection and Documentation (Slide 2 of 2)

- Record the steps taken to collect data.
- Verify enough data is collected to analyze.
- Keep original copies of all data.
- If prior or current hacking activity is discovered, note that in your findings.
  - Ongoing activity should be flagged for escalation.
- If problems outside the engagement scope are discovered, document them and forward to your supervisor.
  - Only pursue them if explicitly told to do so.

Activity Assignment and Sequencing (Slide 1 of 2)

- Start with initial task sequencing based on the pen test process.

- Work in non-technical tests as soon as possible.
  - Social engineering
  - Physical attacks
- Front load activities at the start of the engagement.
- Spend time on activities that are:
  - Opportunity-dependent (social engineering and physical attacks)
  - Evasion-oriented (slow vulnerability scans)
- Remember, findings can spawn new areas of investigation.

Activity Assignment and Sequencing (Slide 2 of 2)

- Verify all investigations work towards the goals and objectives.
- Partner newer pen testers with experienced testers when feasible.
- If findings fall outside the established scope, inform the client.
  - Ask what should be done.
  - Don’t expand scope unless permitted by the SOW.
- When assignments and sequencing are drafted, present at a tactical meeting.

Contingency Planning

- Pen test team uses hacking tools.
  - Problems will arise during testing.
  - Targeted systems or collateral damage.
  - Testing adds a stress load to systems, which can crash if they are already unstable.
- Current, verified backups a must.
- Established contingency plan helps restore services relatively quickly.
  - Reboot systems.
  - Reload VM snapshots.

Escalation Path for Communications

- Alleviates the need for pen testers to make risky or possibly damaging decisions without input from other stakeholders.
- A clear chain of command provides the starting point for escalating issues.
  - Team members report issues only to those who are above them in the chain of command.
- Encourage the client organization to appoint a point person who is the counterpart of the pen test project supervisor.
- Always have a supervisor on duty.
- Train team members:
  - Check in with the lead, especially at the start and end of a specific task.
  - Notify the lead when anomalies are discovered.
  - Notify the lead if out-of-scope issues arise.
  - Refrain from action on out-of-scope issues until authorized to act.

Go Live

- The actual “green light” to start the testing.
- Date and time for Go Live is usually kept secret.
- In some cases, information gathering might start before Go Live date.
  - Passive reconnaissance
  - OSINT

Point in time for the test to begin.

Go Live date and time might be secret.

Information gathering might start first.

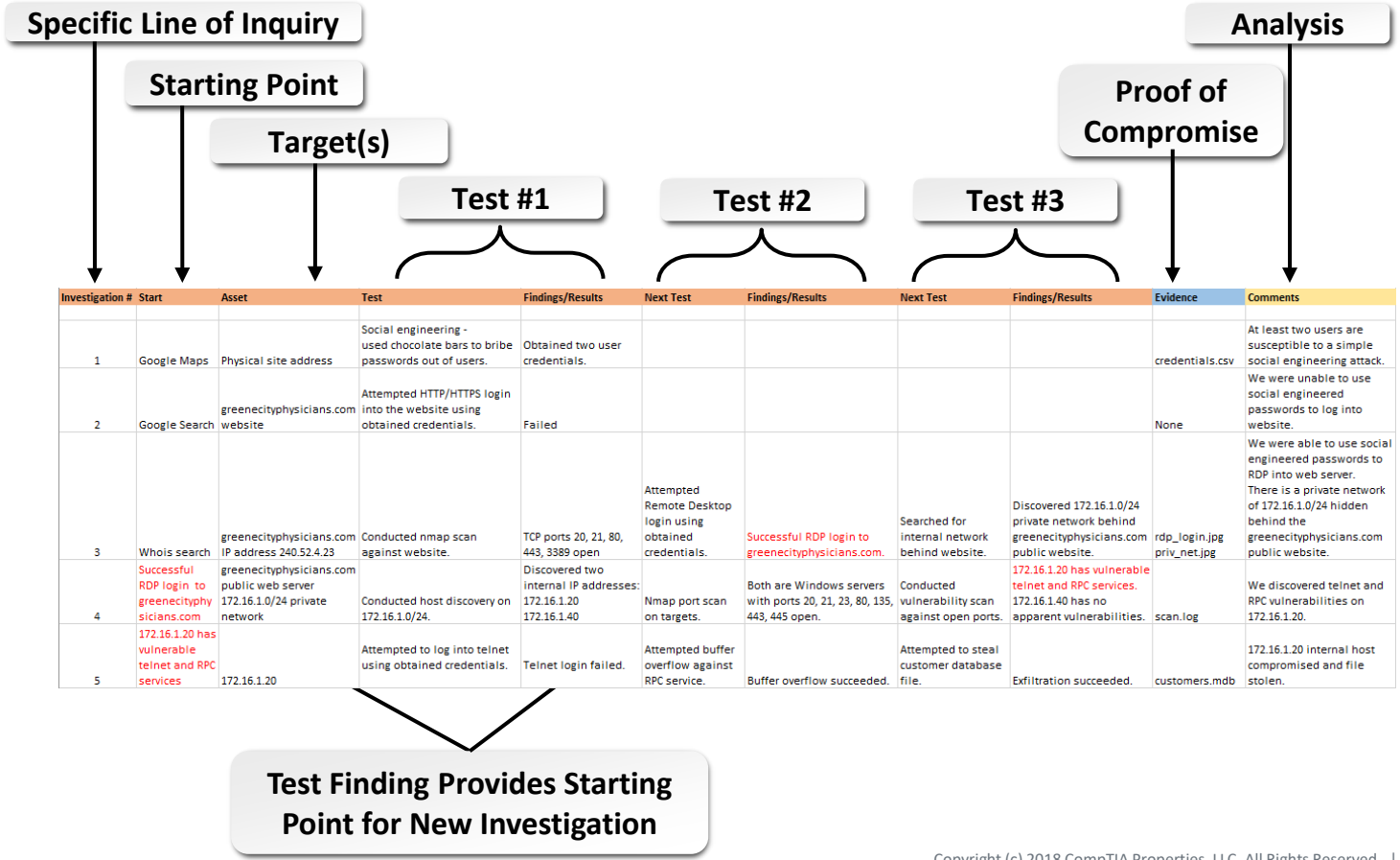
Guidelines for Preparing for a Pen Test Engagement (Slide 1 of 2)

- Verify the team members are trained for their roles.
- Establish a clear chain of command and communication path.
- Train team members to consult their supervisors when unexpected situations occur.
- Pair up less experienced testers with veteran testers when feasible.
- Verify client IT management team is aware of the test.
  - Backups available
  - Contingency plans
- Train team members to stay within the established scope of the engagement unless otherwise directed.

Guidelines for Preparing for a Pen Test Engagement (Slide 1 of 2)

- Train team members to log evidence of prior or existing malicious activity.
  - Continue with the task at hand.
  - Communicate findings up the chain of command.
- Ensure the team fully documents each portion of the engagement.
  - Steps taken.
  - Maximum data collection.
  - Central repository for storage.

Activity: Preparing to Go Live (Slide 2 of 2)



Investigation #	Start	Asset	Test	Findings/Results	Next Test	Findings/Results	Next Test	Findings/Results	Evidence	Comments
1	Google Maps	Physical site address	Social engineering - used chocolate bars to bribe passwords out of users.	Obtained two user credentials.					credentials.csv	At least two users are susceptible to a simple social engineering attack.
2	Google Search	greenecityphysicians.com website	Attempted HTTP/HTTPS login into the website using obtained credentials.	Failed					None	We were unable to use social engineered passwords to log into website.
3	Whois search	greenecityphysicians.com IP address 240.52.4.23	Conducted nmap scan against website.	TCP ports 20, 21, 80, 443, 3389 open	Attempted Remote Desktop login using obtained credentials.	Successful RDP login to greenecityphysicians.com.	Searched for internal network behind website.	Discovered 172.16.1.0/24 private network behind greenecityphysicians.com public website.	rdp_login.jpg priv_net.jpg	We were able to use social engineered passwords to RDP into web server. There is a private network of 172.16.1.0/24 hidden behind the greenecityphysicians.com public website.
4	Successful RDP login to greenecityphysicians.com	greenecityphysicians.com public web server 172.16.1.0/24 private network	Conducted host discovery on 172.16.1.0/24.	Discovered two internal IP addresses: 172.16.1.20 172.16.1.40	Nmap port scan on targets.	Both are Windows servers with ports 20, 21, 23, 80, 135, 443, 445 open.	Conducted vulnerability scan against open ports.	172.16.1.20 has vulnerable telnet and RPC services. 172.16.1.40 has no apparent vulnerabilities.	scan.log	We discovered telnet and RPC vulnerabilities on 172.16.1.20.
5	172.16.1.20 has vulnerable telnet and RPC services	172.16.1.20	Attempted to log into telnet using obtained credentials.	Telnet login failed.	Attempted buffer overflow against RPC service.	Buffer overflow succeeded.	Attempted to steal customer database file.	Exfiltration succeeded.	customers.mdb	172.16.1.20 internal host compromised and file stolen.

Test Finding Provides Starting Point for New Investigation

Reflective Questions

1. Do you have pen testing experience? How do the standards, frameworks, and processes discussed in this lesson map to your experiences?

2. Have you ever experienced scope creep? What were the circumstances and outcomes?