Chapter 1

Planning and Engagement

Episode 1.01 - Planning a Pen Test

Objective

1.1 Compare and contrast governance, risk, and compliance concepts

1.2 Explain the importance of scoping and organizational/customer requirements

1.0 PLANNING AND SCOPING

- Get permission
- Know how much work you have to do
  - Don’t do more than that
- Watch out for scope creep

PLANNING A PEN TEST

- Penetration Testing Execution Standard
  - http://www.pentest-standard.org/
  - Defines seven sections of a penetration test
- Pen test sections
  - Pre-engagement interactions
  - Intelligence Gathering
  - Threat Modeling
  - Vulnerability Analysis
  - Exploitation
  - Post Exploitation
  - Reporting

THE IMPORTANCE OF PLANNING

- Each section of a pen test is important
- Each step is important
- Don’t skip steps
  - You might miss an exploit
  - You might scope the test improperly

THE IMPORTANCE OF PLANNING

- Lots of options in each step
- Each pen test often conducted differently
- Easy to waste time and effort
  - Experience helps avoid this
- Project management skills are important here

QUICK REVIEW

- Above all else, get written permission
- Clearly define scope to avoid scope creep
- Project management skills will help keep pen tests on track

Episode 1.02 – Rules of Engagement

Objective 1.1 Compare and contrast governance, risk, and compliance concepts

TARGET AUDIENCE AND ROE

- Know your target audience
  - Who is sponsoring the pen test?
  - What is the purpose for the test?
- Rules of engagement – governs the pen tester's activities
  - Schedule - start, stop, temporal restrictions
  - Team composition, location, access

TARGET AUDIENCE AND ROE

- Test scope
  - Technical/physical/ personnel
  - Target limits (inclusion, invasiveness, etc.)

COMMUNICATION ESCALATION PATH

- Risks of pen testing
  - Crashing devices, services, whole servers
  - Corrupting data
  - Degrading performance
  - Terms of Service (TOS)/regulation/legislation violation
- Communication escalation path
  - Who to contact if things go wrong
  - Communication expectations (content, trigger, frequency)

QUICK REVIEW

- Know who is sponsoring the pen test and why
- What kind of tests can you execute and what is off limits?
- Understand pen test risks
- Plan to communicate and know who to call and when

Episode 1.03 – Regulatory Compliance

Objective 1.1 Compare and contrast governance, risk, and compliance concepts

REGULATORY COMPLIANCE CONSIDERATIONS

- Payment Card Industry Data Security Standard (PCI DSS)
  - Industry standard of security requirements for payment card processing
  - PCI DSS requirement 11
    - Internal and external testing
      - Annually
      - After significant infrastructure changes
- https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

REGULATORY COMPLIANCE CONSIDERATIONS

- General Data Protection Regulation (GDPR)
  - European Union (EU) regulation
  - Data protection and privacy for all individuals in the EU
  - Give control to individuals over their personal data
  - Article 32(1) requires “a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing”

QUICK REVIEW

- Regulation compliance requirements impact pentesting scope
- PCI-DSS is an industry standard for any organization that accepts payment cards
- GDPR regulates data security for the European Union

Episode 1.04 - Resources and Budgets

Objective

1.1 Compare and contrast governance, risk, and compliance concepts

1.2 Explain the importance of scoping and organizational/customer requirements

RESOURCES AND REQUIREMENTS

- What does each party provide?
- At what point does the engagement begin?
- Confidentiality of findings
- Known vs. unknown
  - Is the test a secret?

BUDGET

- How much will each section of the test cost?
- Every task in the test should have a value
  - Want to add more tests? It’ll cost more
- One of the most important factors
  - Directly impacts available resources and time

QUICK REVIEW

- What do you provide and what does the client provide?
- Are your activities known or secret?
- Determine the value of each part of the test
- Don't underestimate the impact of an accurate budget

Episode 1.05 - Impact and Constraints

Objective 1.3 Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity

SET EXPECTATIONS

- Impact
  - The result of testing
  - Report vulnerabilities
  - Remediation
    - How should client respond?

SET EXPECTATIONS

- Disclaimers
  - Point-in-time assessment
    - Only valid now
  - Comprehensiveness
    - Enterprise/division/department, etc.

TECHNICAL CONSTRAINTS

- Any technical limitations that reduce test scope
- Production (live) components
- Out-of-service devices
- Can’t access
  - Physical/geographic access limitations
  - Legal/regulatory/out of scope

QUICK REVIEW

- Document expected impact of pen tests
- Provide estimate of remediation activities
- Specify any technical constraints

Episode 1.06 - Support Resources

Objective 1.2 Explain the importance of scoping and organizational/customer requirements

SUPPORT RESOURCES

- WSDL/WADL
  - Web services/application description language
  - XML file with lots of info about web service/application and its interface requirements
    - Input/output specs

SUPPORT RESOURCES

- SOAP project file
  - Not exposed to public
  - Used by developers in development environment

SUPPORT RESOURCES

- SOAP project file
  - Simple Object Access Protocol – used to exchange info for web services
  - Project file provides low level web service interface details (input/output/server info)

SUPPORT RESOURCES

- SDK documentation
  - Software Development Kit (SDK) docs help provide info on tools used to develop software
  - Reveals software libraries in use

SUPPORT RESOURCES

- Swagger document
  - Popular open-source framework for developing REST services
  - REST is a light weight API
  - Document can provide internal info on REST services exposed to clients

SUPPORT RESOURCES

- XSD
  - XML Schema Definition – defines XML document content

SUPPORT RESOURCES

- Sample application requests
  - Well-formed requests, generally to web services
  - Useful when testing web services/applications of all types

SUPPORT RESOURCES

- Architectural diagrams
  - Diagrams of networks and connected devices
  - Helpful when determining targets to attack

QUICK REVIEW

- Find out if any internal resources are available
- Look for artifacts from application development
- Also look for any deployment or support documents

Episode 1.07 - Legal Groundwork

Objective 1.1 Compare and contrast governance, risk, and compliance concepts

LEGAL CONCEPTS

- Statement of work (SOW)
  - Clearly states what tasks are to be accomplished
- Master Service Agreement (MSA)
  - Specifies details of the business arrangement
- Non-Disclosure Agreement (NDA)
  - Agreement that defines confidentiality, restrictions and/or sharing information

ENVIRONMENTAL DIFFERENCES

- Export restrictions – restrictions on shipment or transfer of technology or services outside the U.S.
  - See U.S. State Department resource - https://www.state.gov/strategictrade/overview/
- Local and national government restrictions – laws and regulations differ among countries
  - A legal action in one country may be illegal in another
- Corporate policies – differ between most organizations

ENVIRONMENTAL DIFFERENCES

- National or local restrictions
  - Differ among countries
  - Local customs differ
- Corporate policies
  - Differ between most organizations

WRITTEN AUTHORIZATION

- Obtain signature from proper signing authority
  - Pen tests can reveal sensitive or confidential information
  - Activities may be illegal without proper permission
  - Signed permission makes you a white hat
- Third-party provider authorization when necessary
  - Get permission for any outside resources you use in tests
  - Internet, Cloud, and distributed resource that isn’t owned by the entity sponsoring the pen test

QUICK REVIEW

- Understand common contract types
- Pay attention to localization restrictions
- Always get written permission
- Find out if you need third-party permission as well

Episode 1.08 - Service Provider Agreements

Objective 1.1 Compare and contrast governance, risk, and compliance concepts

SERVICE PROVIDER AGREEMENTS

- Service-level agreement (SLA)
  - Legal agreement between a service provider and a client
  - Quality
  - Availability
  - Responsibilities
- Some SLAs may include penetration testing
  - Requirements
  - Limitations

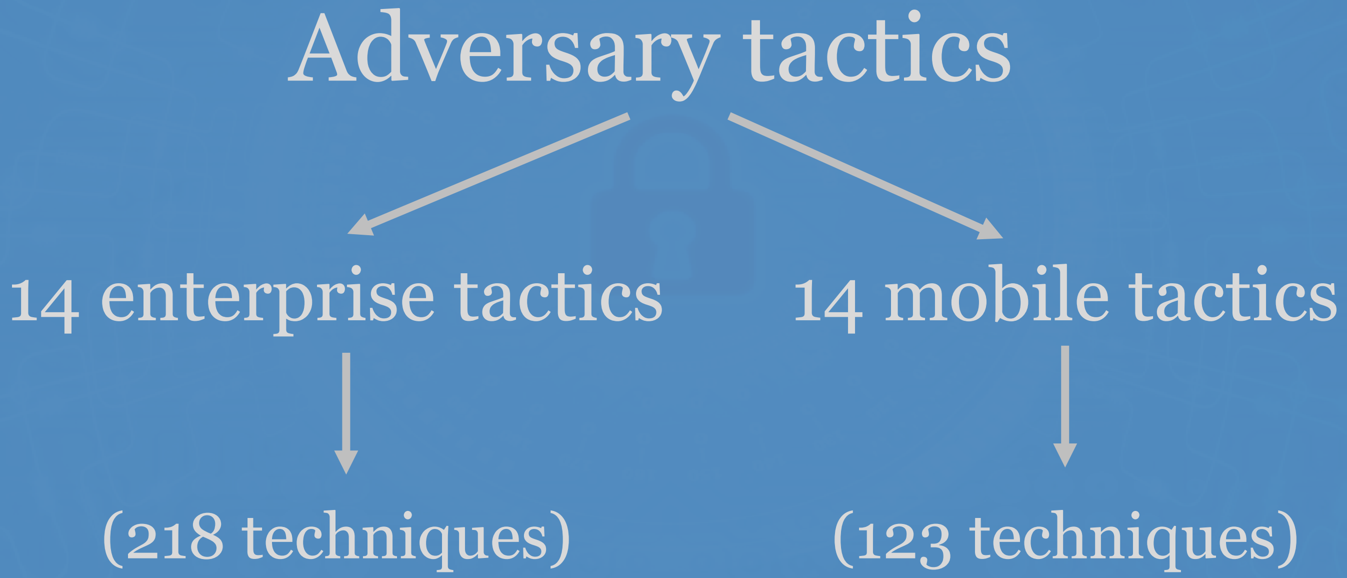
QUICK REVIEW

- A service level agreement (SLA) sets expectations between a service provider and client
- SLAs may require control testing
- SLAs may limit the scope or type of tests

Episode 1.09 - Standards and Methodologies, Part 1

Objective 1.2 Explain the importance of scoping and organizational/customer requirements

MITRE ATT&CK



Adversary tactics

14 enterprise tactics

(218 techniques)

14 mobile tactics

(123 techniques)

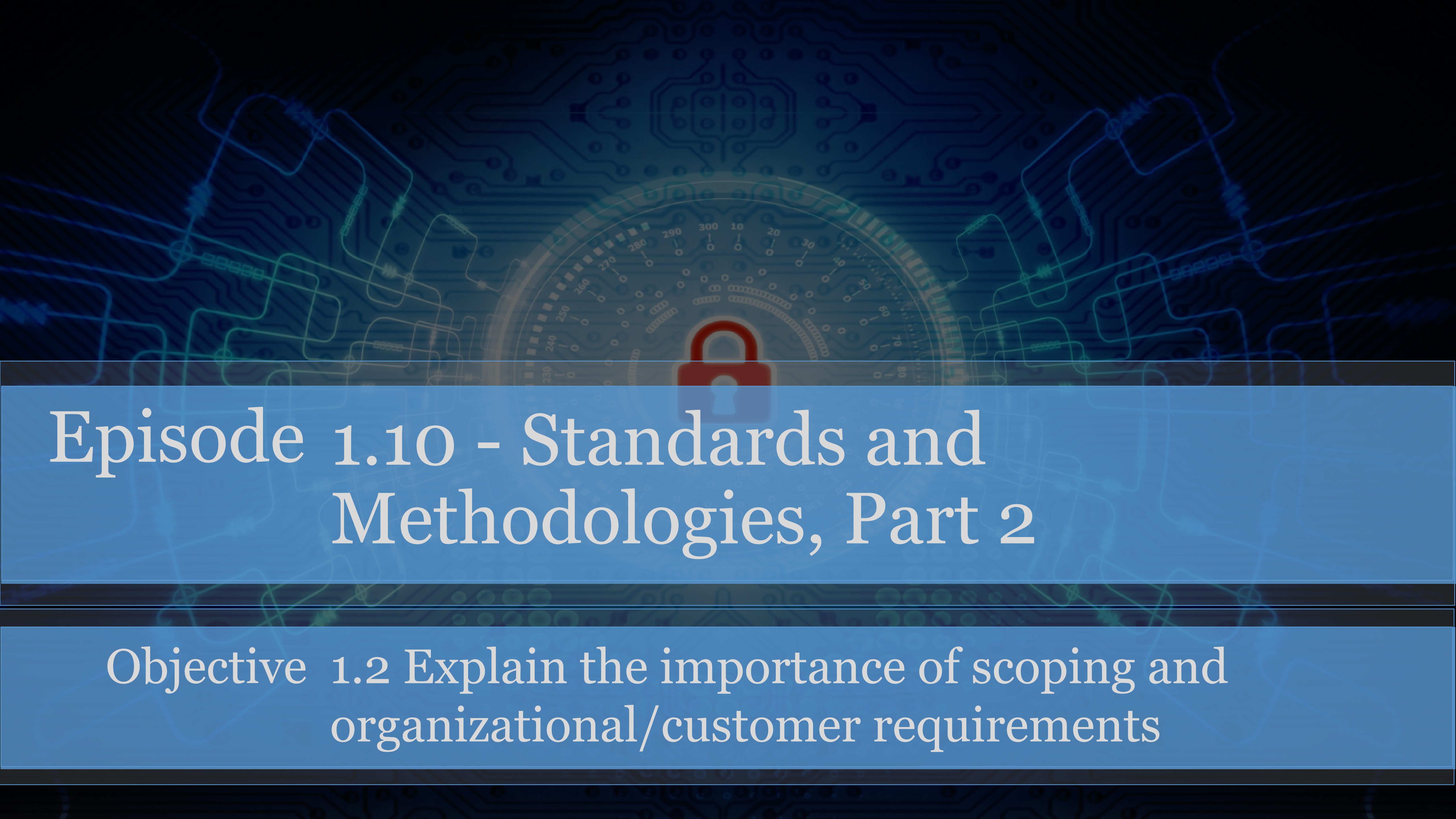
https://attack.mitre.org

STANDARDS AND METHODOLOGIES

- Open Web Application Security Project (OWASP)
  - Nonprofit resource to help make web applications more secure
  - OWASP Top 10
  - https://owasp.org

QUICK REVIEW

- Attack standards and methodologies document standardized attack phases
- MITRE ATT&CK organizes activities into 12 tactics and 196 techniques
- OWASP Top 10 tracks the most commonly encountered software risks



Episode 1.10 - Standards and Methodologies, Part 2

Objective 1.2 Explain the importance of scoping and organizational/customer requirements

STANDARDS AND METHODOLOGIES

- National Institute of Standards and Technology (NIST)
  - U.S. standards authority
    - https://www.nist.gov
  - NIST Cybersecurity Framework (CRF)
    - https://www.nist.gov/cyberframework
  - NIST Special Publication (SP) 800-171 - 3.11.2, 3.11.3
    - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
  - NIST SP 800-53 Rev 5
    - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

STANDARDS AND METHODOLOGIES

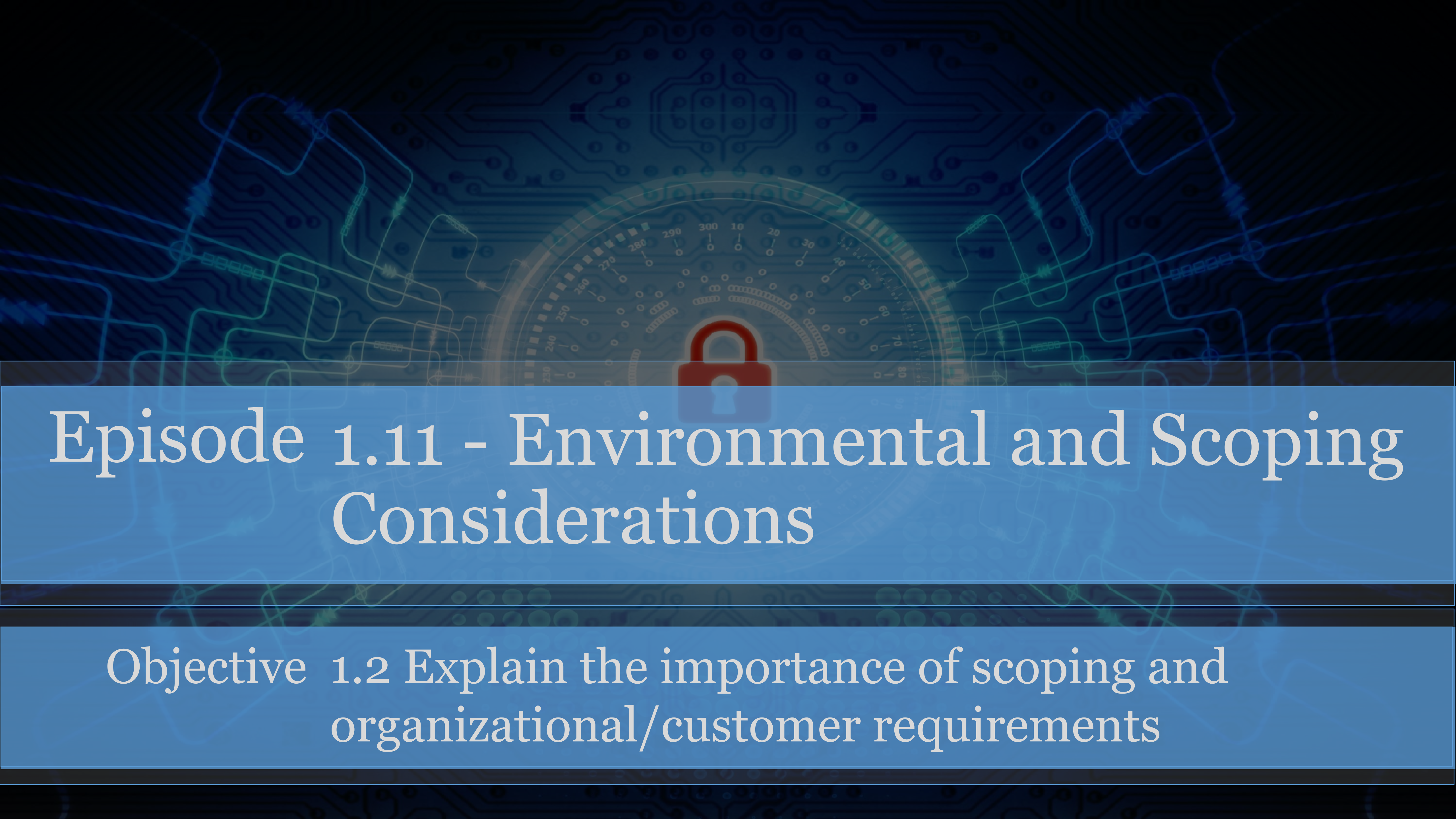
- Open-source Security Testing Methodology Manual (OSSTMM)
  - Dated, open-source manual for testing security controls
  - https://untrustednetwork.net/files/osstmm.en.2.1.pdf
- Penetration Testing Execution Standards (PTES)
  - http://www.pentest-standard.org

STANDARDS AND METHODOLOGIES

- Information Systems Security Assessment Framework (ISSAF)
  - Comprehensive security assessment framework
  - Dated, but open-source and extensive
  - https://untrustednetwork.net/files/issaf0.2.1.pdf

QUICK REVIEW

- NIST publishes many technical standards
- OSSTMM is an open-source manual for testing security controls
- PTES documents the seven phases of pentesting
- ISAAF is an open-source security assessment framework



Episode 1.11 - Environmental and Scoping Considerations

Objective 1.2 Explain the importance of scoping and organizational/customer requirements

ENVIRONMENTAL CONSIDERATIONS

- Network
  - Physical vs. virtual segmentation
  - Wired vs. wireless
  - Media
  - LAN vs. MAN vs. WAN

ENVIRONMENTAL CONSIDERATIONS

- Application
  - Nature of application(s) in use
  - Third-party or internally developed
  - Architecture

ENVIRONMENTAL CONSIDERATIONS

- Cloud
  - Private vs. public vs. hybrid
  - On-premises vs. cloud distribution

IN-SCOPE ASSETS

- Wireless networks
- IP ranges
- Domains, forests, organizational units (OUs) in Active Directory
- Application programming interfaces (APIs)
- Domain Name System (DNS)

SCOPING THE ENGAGEMENT

- Types of assessment
  - Goals-based/objectives-based
    - Goals-based – Goals set up front, testers work to fulfill goals
    - Objective-based – Assets to protect are defined and testers use all angles to attack protected objectives
  - Compliance-based
    - Used to show compliance (i.e. PCI-DSS)
  - Red team
    - Ongoing team that acts like attackers to use any means to access objective(s)
    - A single compromise is success

QUICK REVIEW

- Consider the target environment when planning a pentest
- The type of assessment directs your activities
- Goal-based assessments set the goals up first and the tester(s) work to fulfill goals
- Objective-based assessments define specific assets for testers to attack

Episode 1.12 – Ethical Mindset

Objective 1.3 Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity

ETHICAL MINDSET

- Start with a trusted team
  - Team members are entrusted with substantial authority
  - Background checks of Pentesting team
- Immediately report breaches/criminal activity
  - Don’t wait until the reporting phase
  - Define a reporting process
  - Preliminary info releases are acceptable

ETHICAL MINDSET

- Limit the use of tools to a particular engagement
  - Avoid scope and/or authorization creep
  - Do not run tests that cross engagement boundaries
- Limit invasiveness based on scope
  - Don’t overdo it
  - Pay attention to limitations defined by scope
  - Watch out for long running test and redirects
- Risks to the professional
  - Fees/fines
  - Criminal charges

QUICK REVIEW

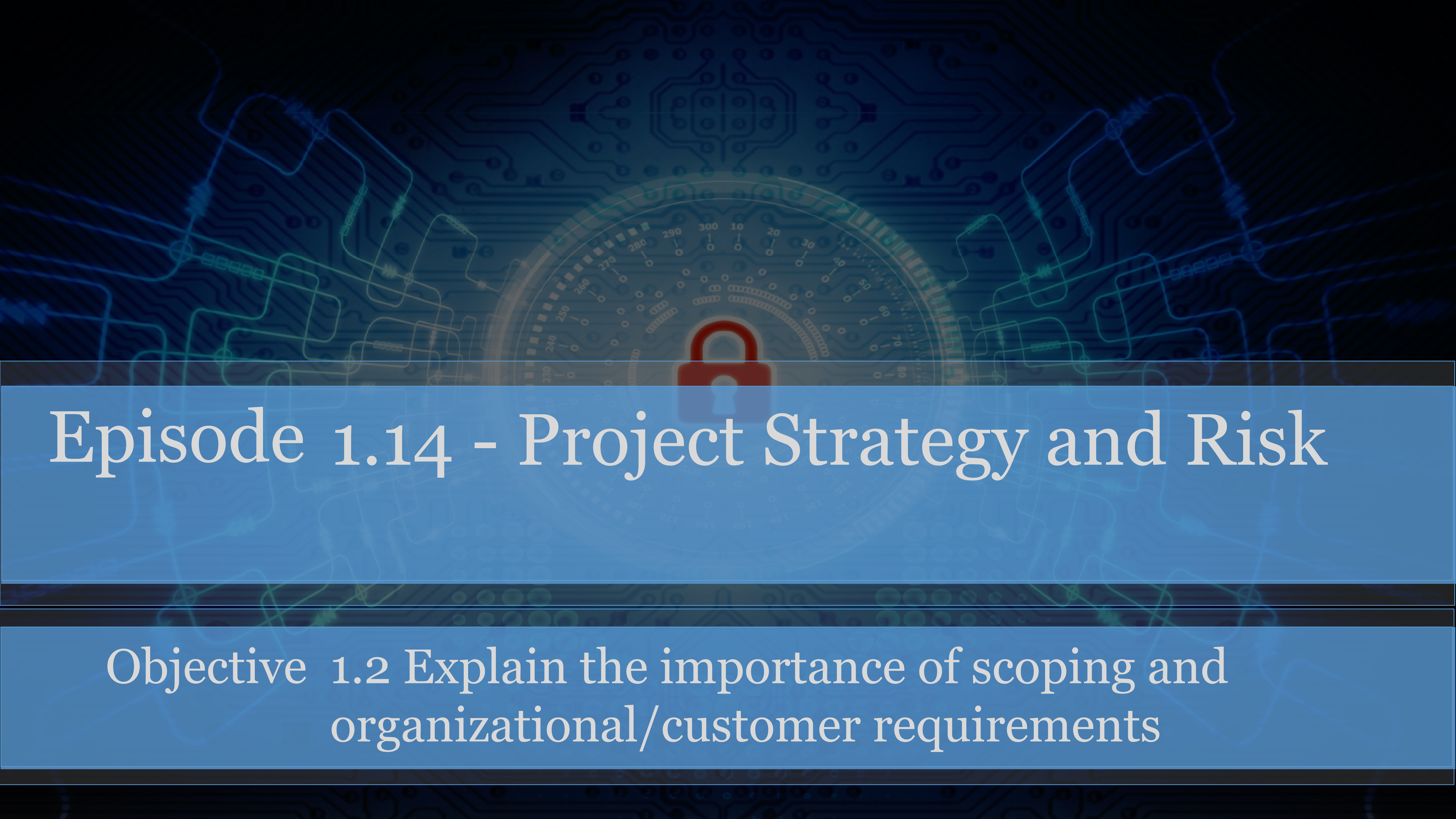
- Carry out pentesting ethically
- Build a trusted team
- Immediately report critical findings
- Limit tool use and scope
- Avoid risks to pentesters

Episode 1.13 Lab Environment Setup

Objective (none)

Demo

- Introduction to class environment
- Download VirtualBox, run Windows VM, Metasploitable, and DVWA



Episode 1.14 - Project Strategy and Risk

Objective 1.2 Explain the importance of scoping and organizational/customer requirements

CONSIDERATIONS

- White-listed
  - No one can access resources unless specifically granted
- Black-listed
  - Everyone can access unless specifically blocked

CONSIDERATIONS

- Security exceptions
  - IPS (Intrusion Prevention System)/WAF (Web application firewall) whitelist
  - NAC (Network Access Control)
  - Certificate pinning (public key pinning)
- Explore company policies to learn about security considerations

STRATEGY

- Black box
  - Zero prior information
  - Most similar to real attacker
  - Test is generally a surprise to all internal personnel
- White box
  - Full access to internal information
  - Simulates insider attack
- Gray box
  - Some internal information available
  - Consistent with an insider attack with limited access

RISK ACCEPTANCE

- Pen tests can be risky
  - Service can be interrupted
  - Devices/servers can become unresponsive
- How much risk is the client willing to accept?
  - Client has identified risks
  - Acceptance: willing to accept risks, based on likelihood and impact
- Tolerance to impact
  - If risk is realized, what is client’s tolerance to the result?
  - How much disruption is tolerable?

QUICK REVIEW

- Are your tests Black box, White box, or Gray box?
- Discuss risk acceptance with your client
- Agree on the tolerance to impact if tests affect the client's environment

Episode 1.15 – Scope Vulnerabilities

Objective 1.2 Explain the importance of scoping and organizational/customer requirements

SCHEDULING AND SCOPE CREEP

- Scheduling
  - When can/should tests be run?
  - Who should be notified?
  - When must tests be completed?
- Scope creep – common in nearly all projects
  - Client requests additional tasks after SOW is signed
  - Many may seem “doable”
  - Takes resources away from core SOW tasks
  - Must get authorization for any SOW modifications

THREAT ACTORS

- Adversary tier – what role should the pen tester assume?
  - APT (Advanced Persistent Threat)
  - Script kiddies
  - Hacktivist
  - Insider threat
- Capabilities
  - What resources does the attacker(s) have?
  - Organized and sponsored attackers have more equipment and sophistication

THREAT ACTORS, cont’d

- Intent
  - Power/revenge
  - Status/validation
  - Monetary gain
  - Ideology
- Threat model
  - Gather information and identify assets
  - Rank pertinent threats
  - Map threats to assets

QUICK REVIEW

- Agree on days and times that are available for testing
- Develop a scope management plan and stick to it
- Assume an adversary role for tests
- Realistically determine the technical capabilities based on adversary role

Episode 1.16 - Compliance-Based Assessments

Objective 1.1 Compare and contrast governance, risk, and compliance concepts

COMPLIANCE-BASED ASSESSMENT

- Rules to complete assessment
- Password policies
- Data isolation
- Key management
- Limitations
- Clearly defined objectives based on regulations

QUICK REVIEW

- Define any compliance requirements for each test
- Define test objectives based on regulations or mandated minimums