NEbraskaCERT Cyber Security Forum

July 16, 2003

Security Assessment Methodologies

Stephen M. Nugen, CISSP

Presenter

NEbraskaCERT

- Steve Nugen
- Affiliations: CISSP, NEbraskaCERT, NuGenSoft, CSM, InfraGard, etc.
- Contact
  - smnugen@nugensoft.com
  - 402.505.7691
- Style: Talks too fast, mumbles; but never offended if asked to slow down or repeat something

Scope of Presentation

NEbraskaCERT

- Includes
  - Security assessment methodology topics
  - Content from multiple sources, selected and modified according to presenter's prejudices
  - Presenter's own methods

- Structure
  - Part-1: Context: Terms, etc.
  - Part-2: Methodology
  - Part-3: Some discovery activities (time permitting)

Part-1: Terms and definitions

Terms

- Different experts use different terms
  - Some attempts being made to distinguish between them, common understandings still evolving
  - A snapshot...

- Penetration Tests
  - Aka Penetration Analysis, Pen Test, Ethical Hacking, White Hat Hacking, Red Team, Tiger Team
  - Test team plays role of hostile external attacker
  - Done externally to the organization using public Internet connections
  - Probe networks and devices to identify vulnerabilities that could be remotely exploited

Terms cont'd

NEbraskaCERT

- Penetration Tests cont'd
  - Oftentimes covert
    - Management authorized
    - No notification to IT staff...
    - Zero knowledge (no inside knowledge, no support)
  - May include testing the organization's capability to detect and react to penetration activities
  - May include social engineering
  - May not be comprehensive
    - Like attacker, only need to find one good vulnerability
    - Sometimes a vivid wake-up call for management

Terms cont'd

NEbraskaCERT

- Audits
  - Independent team
  - Overt
    - Coordinated with organization
    - Full-knowledge and organizational support, including interviews
  - Mostly internal
  - Measure current practices/implementations against some set of standards
    - External standards defined by government, business partners, etc.
    - Organization's own policies and procedures
  - May include an evaluation of the standards themselves
  - May include physical security

Terms cont'd

NEbraskaCERT

- Assessments
  - Aka security diagnostic
  - Internal or external team
  - Test team assumes multiple roles, including insiders
  - Overt
    - Full cooperation of organization, participation as required
    - Full-knowledge, including sensitive knowledge (network diagrams, etc.)
  - External and internal access
  - More comprehensive than penetration tests
    - Goal is to find all the most-critical vulnerabilities so that the associated risk can be managed

Terms cont'd

NEbraskaCERT

- Formal verifications
  - Ideal
    - Complete and convincing mathematical argument that proves the absence of vulnerabilities
    - Preconditions specify constraints on the system state when software executes
    - Postconditions specify the effect of executing the software
  - Trusted product verification
    - Compares two levels of system specification for proper correspondence
      - Ex: Security policy model to top-level specification
      - Ex: Top-level specification to source code
      - Ex: Source code to object code

Terms cont'd

NEbraskaCERT

- Common practice: Combinations, tailored to organizational requirements

Motivations

NEbraskaCERT

- Part of the security process
  - Between awareness and countermeasures
  - Periodic evaluations in a changing environment
    - Changing assets
    - Changing threats
- Component of risk management
  - Identification
  - Analysis (likelihood of compromise, cost of compromise)
  - Mitigation
  - Informed acceptance

Motivations cont'd

NEbraskaCERT

- Goals
  - Avoid the consequences of misuse/compromise
    - Discover weaknesses before they are exploited
    - Measure how well the organization resists misuse/compromise
  - Discover actual performance against what the organization believes it has implemented
    - Analogy: Using an proofreader to detect mistakes not visible to the author
    - Universal finding: Discovering protocols, services, etc. that were not thought present by Exec/IT management
    - Common finding: Key restrictions not enforced or monitored by technical means

Motivations cont'd

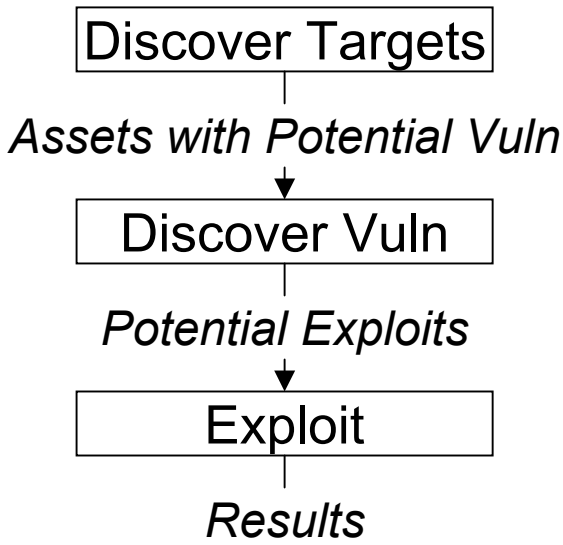
NEbraskaCERT

- Goals cont'd
  - Evaluate the actual system for compliance with plans, policies, etc. defined by the organization or others (audit)
  - Use a methodology/process which is repeatable, supporting
    - Validation, confidence
    - Re-use

Constraints

NEbraskaCERT

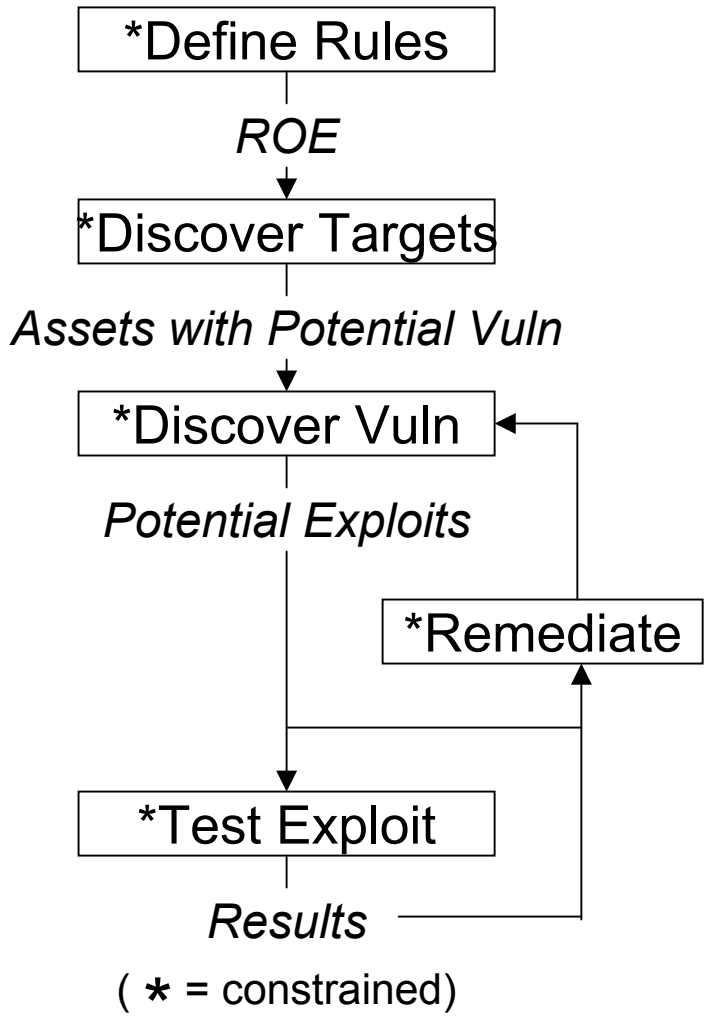
- True Attacks
  - Not constrained by need to maintain business continuity
  - Success: Discovery and exploitation of any single vulnerability



Constraints cont'd

NEbraskaCERT

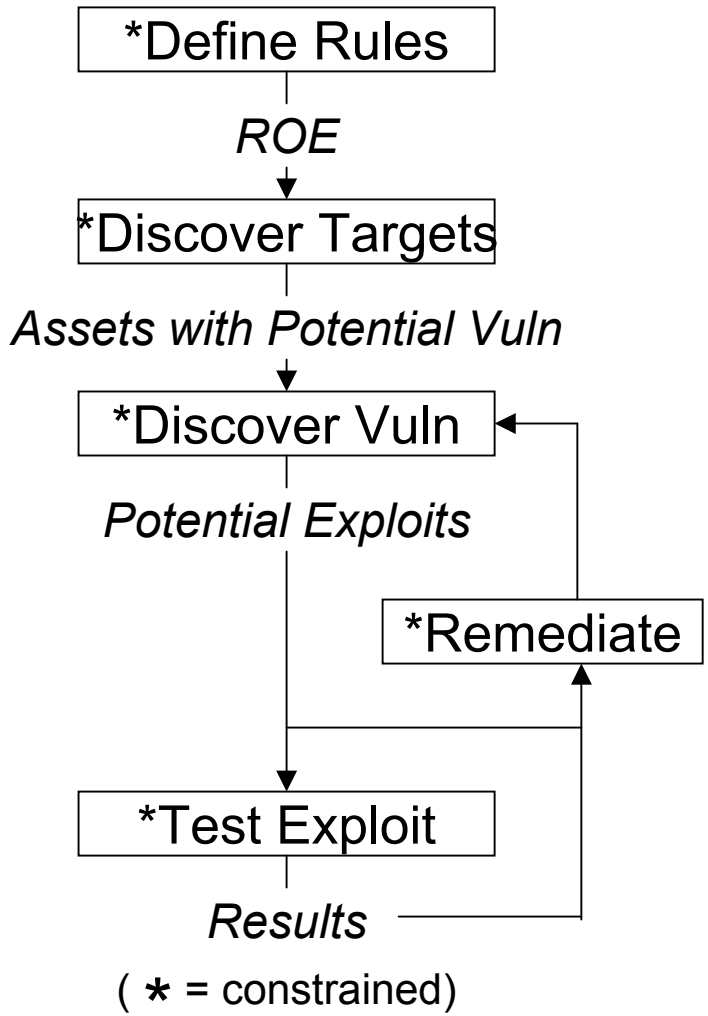
- Ethical Discovery
  - Needs to discover same vulnerabilities as unconstrained malicious actor
  - Constrained by need to maintain
    - Business continuity
    - Availability, confidentiality, and integrity of information and information assets
    - Good records of activities and findings



Constraints cont'd

NEbraskaCERT

- Ethical Discovery cont'd
  - Ideal success: Discovery and remediation of every vulnerability
    - Not possible
    - Testing only proves the existence of vulnerabilities, not their absence
  - Realistic success: Discovery and mitigation of most critical vulnerabilities



Part-2: Methodologies

Methodologies

NEbraskaCERT

- Some defined formally, such as
  - Flaw Hypothesis Methodology (FHM)
  - Attack Tree (AT) Methodology
  - InfoSec Assessment Methodology (IAM)
- Some defined less formally by vendors and best practices
- Development continues
  - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
  - Others... research institutions, vendors

Knowledge

NEbraskaCERT

- Three approaches with respect to how much insider knowledge provided to test team: Zero, Partial, Full

- Zero Knowledge
  - Aka Black Box
  - Testers not given any company-private information about target networks and systems
  - Most realistic simulation of external intrusion
  - Tester not biased by security architecture
  - Requires independent testers
  - Takes longer, costs more

Knowledge cont'd

NEbraskaCERT

- Full Knowledge
  - Aka Crystal box
  - Testers provided with network diagrams, system configurations, etc.
  - Simulates internal attacks
  - Quicker, costs less
  - Coordinated tests less likely to harm system
  - Testers can be employees or independent
- Partial Knowledge
  - More than zero, less than full...

Flaw Hypothesis Methodology

NEbraskaCERT

- Overview
  - System analysis and penetration techniques
  - Specifications and documentation for the system are analyzed
  - Flaws in the system are hypothesized
  - Hypothesized flaws prioritized based on
    - Probability that flaw actually exists
    - Ease and impact of exploiting the flaw
  - Prioritized list used to direct penetration attack

InfoSec Assessment Methodology

NEbraskaCERT

- IAM: InfoSec Assessment Methodology
- Developed by NSA in response to PDD-63
- Phased approach
  - Pre-Assessment
  - On-Site Visit
  - Post-Assessment

IAM cont'd

NEbraskaCERT

- Addresses 18 areas
  - InfoSec Documentation
  - Identification/Authentication
  - Session Controls
  - Telecommunications
  - Virus Protection
  - Maintenance
  - Back-ups
  - Media Sanitation/Disposal
  - Personnel Security
  - Roles and Responsibilities
  - Account Management
  - External Connectivity
  - Auditing
  - Contingency Planning
  - Configuration Management
  - Labeling
  - Physical Environment
  - Training and Awareness
- Training...

OCTAVE

NEbraskaCERT

- Context
  - OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation
  - Developed by SEI (Software Engineering Institute at Carnegie Mellon University)
  - Funded by
    - U.S. Department of Defense
    - U.S. Department of State
  - Two flavors
    - OCTAVE: For large-scale organizations
    - OCTAVE-S: For small organizations (still under development)
  - Src: CERT (www.cert.org)

OCTAVE cont'd

NEbraskaCERT

- Motivation
  - Observed deficiencies in evaluations
    - Technology-only focused
    - Conducted without site's direct participation
    - Precipitated by an event (reactive rather than proactive)
    - Using undefined or inconsistent criteria
  - Need
    - Expand the organizational involvement beyond IT
    - Include security policies, practices, procedures
    - Be proactive rather than reactive
    - Provide a foundation for continuous security improvement

OCTAVE cont'd

NEbraskaCERT

- Philosophy
  - Cannot mitigate all risks... cannot prevent all determined, skilled incursions
  - Budget and other resources limited
  - So, need to focus limited resources on ensuring the survivability of the enterprise

OCTAVE cont'd

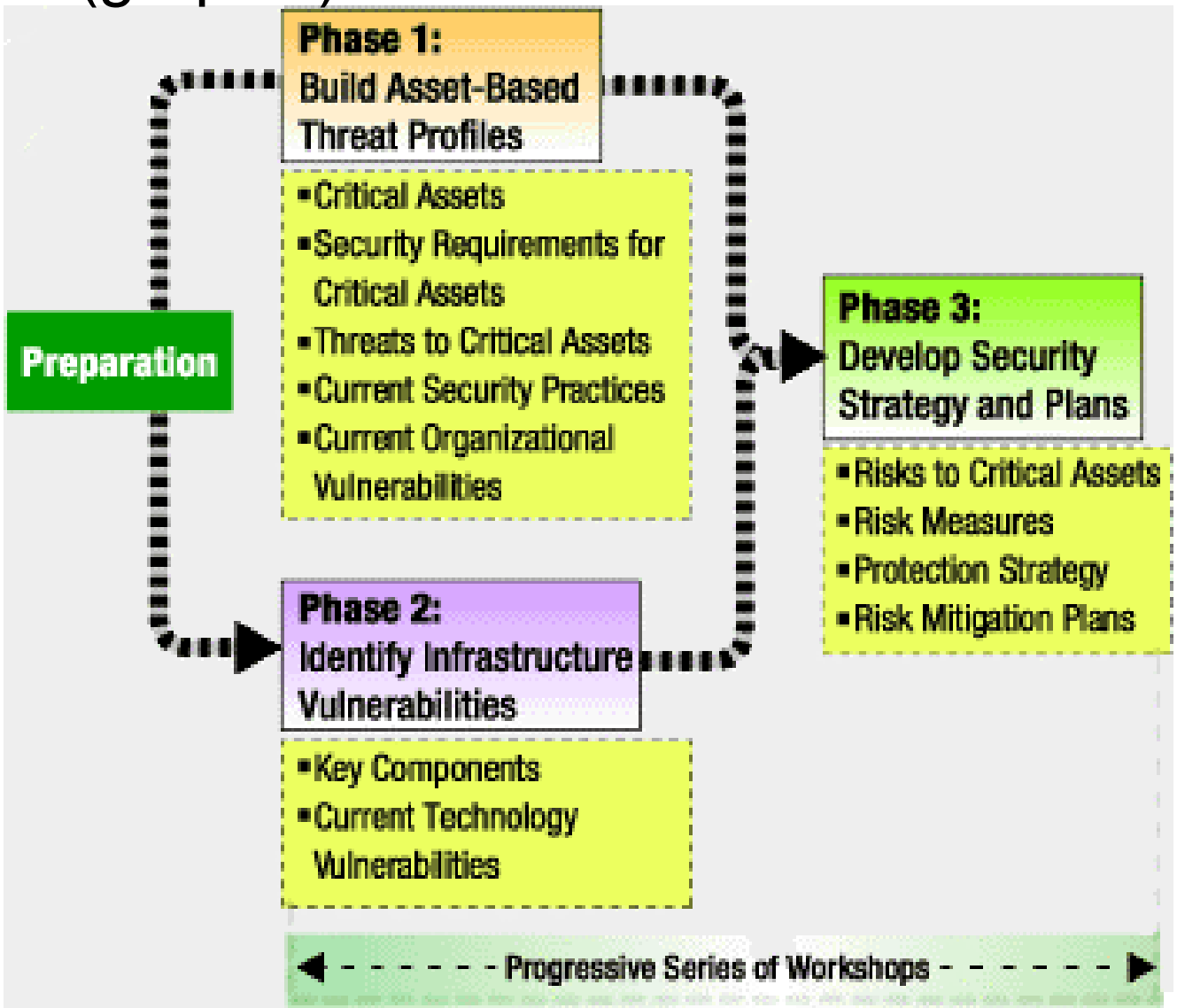
NEbraskaCERT

- Approach
  - Uses organization's own expertise and resources, not outsourced
    - Organization self-directs the assessment
  - Full-knowledge
  - Uses a workshop-based approach for gathering information and making decisions
    - At least 12 workshops, each a half or full-day
    - Durations vary from few weeks to more than 6-months depending on scope and scheduling complications
  - Organizations tailor the OCTAVE approach to their own needs

OCTAVE cont'd

NEbraskaCERT

- Phases (graphic)



OCTAVE cont'd

NEbraskaCERT

- Phases cont'd
  - Preparation
    - Senior management sponsorship
    - Selecting team members
    - Training
    - Planning: scope, etc.
  - Phase-1: Organizational view
    - Identify organization's self-knowledge of its assets in terms of
      - Criticality
      - Threats
      - Security requirements
      - What organization is currently doing to protect those assets
    - Includes senior management, operational area, and staff knowledge
    - Build asset-based threat profiles

OCTAVE cont'd

NEbraskaCERT

- Phases cont'd
  - Phase-2: Technological View
    - Identify key components of shared information infrastructure
    - Evaluate key components for technology vulnerabilities that could be exploited
  - Phase-3: Strategy and Plan Development
    - Analyze information collected/generated by Phase-1 and Phase-2
    - Develop protection strategy. including
      - Organizational direction
      - Mitigation plans to reduce risk
      - Near-term actions

OCTAVE cont'd

NEbraskaCERT

- Uses catalogs of information
  - Practices: collection of good practices
    - Used in Phase-1 as a benchmark to compare current practices against
    - Used in Phase-3 to develop organization's protection strategy
  - Threat Profile: range of threats organizations need to consider
    - Used at the end of Phase-1
  - Vulnerabilities: collection of vulnerabilities based on platform and application
    - Used in Phase-2
    - OCTAVE does not include tools

OCTAVE cont'd

NEbraskaCERT

- OCTAVE licensing
  - Not required for internal use
  - License from SEI required for external users, including
    - Individual advisors/trainers
    - Transition partners: organizations that help other organizations with OCTAVE
    - Developers of derivatives or automated tools supporting OCTAVE

Process

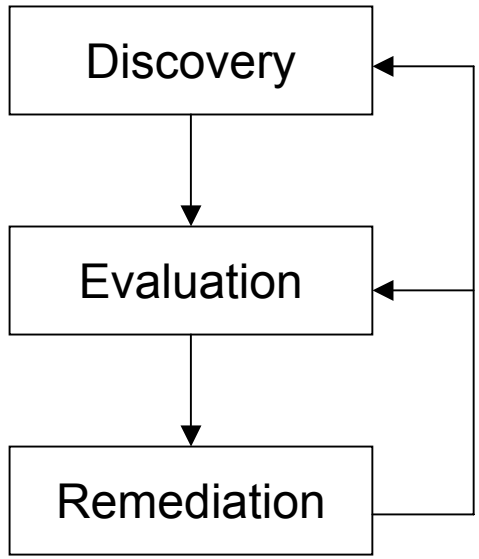
NEbraskaCERT

- Presenter's viewpoint
  - With
    - Credit to multiple sources
    - Blame to none
  - Unconstrained by cost and schedule...

- Overall process defined by the intersection of
  - Phase (e.g., discovery, evaluation, remediation)
  - Role (outsider, associate, insider)
  - Scope (e.g., subnet-x, location-y)
  - Activity (planning, collection, analysis, reporting)

Process cont

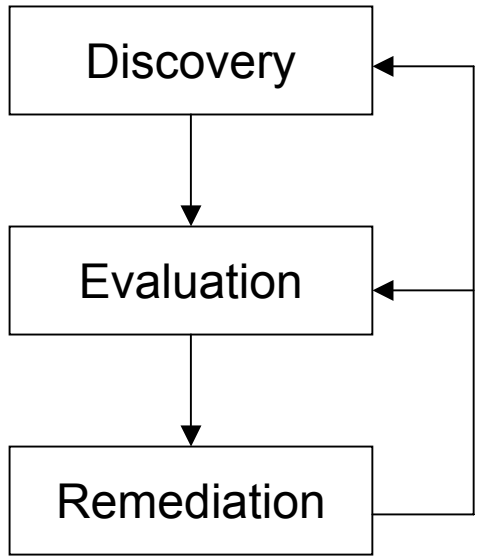
- Phases
  - Discover potential targets of misuse
    - Information
    - Information assets
  - Discover vulnerabilities in those potential targets
    - Possible exploits
    - Differences in observed performance versus
      - Expected performance
      - Required/specified performance
  - Evaluate vulnerabilities
    - Confirm/demonstrate the existence of vulnerability
    - May include controlled intrusions, exploits



Process cont

NEbraskaCERT

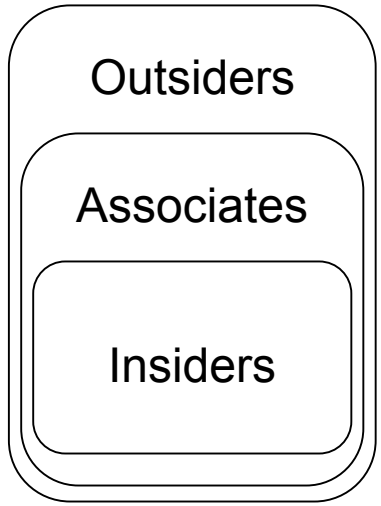
- Phases cont'd
  - Remediation... from viewpoint of security diagnostics:
    - Does include recommendations to reduce risk
    - Does not include corrective measures
  - After remediation, may repeat subset of Evaluation and Discovery phases to measure the effectiveness of the corrective measures



Process cont

NEbraskaCERT

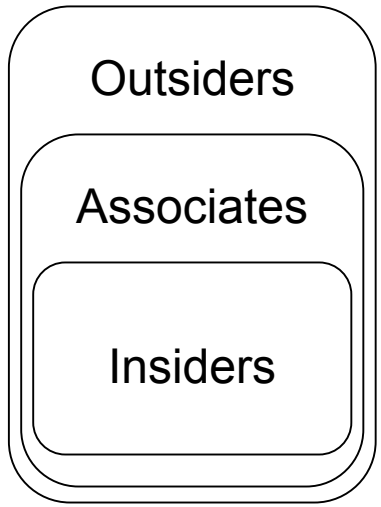
- Roles
  - Defined by access and insider knowledge
  - Outsiders
    - Internet access to company information and assets: Yes
    - Physical access to company facilities, and networks: No
    - Employee account and/or knowledge: No
    - Examples
      - Anyone, anywhere, anytime
      - Script kiddies ranging from curious to malicious
      - Expert hackers motivated by recognition, hactivism, money



Process cont

NEbraskaCERT

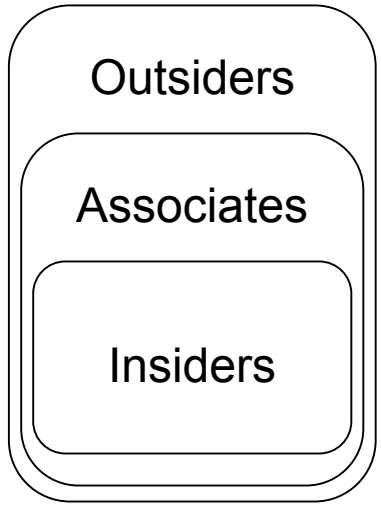
- Roles cont'd
  - Associates
    - Internet access to company information and assets: Yes
    - Physical access to company facilities, and networks: Yes
    - Employee account and/or knowledge: No
    - Specified by some as external intruder with physical access
    - Examples
      - Outsourced cleaning, security, maintenance, service staff, etc.
      - Short-term visitors, vendors, consultants, temporary employees
      - Any outsider who has compromised any client or server inside the organization



Process cont

NEbraskaCERT

- Roles cont'd
  - Insiders
    - Internet access to company information and assets: Yes
    - Physical access to company facilities, and networks: Yes
    - Employee account and/or knowledge: Yes
    - Examples
      - Employees... users, manager, system administrators
      - Longer-term visitors, vendors, consultants, temporary employees
      - Ex-employee with Associate access (directly or indirectly via compromised client or server)



Process cont

NEbraskaCERT

- Scope defined by
  - Networks, subnets, domains, etc.
  - Facility locations
  - And, so forth
  - Constraints
    - Ex: Network infrastructure only
    - Ex: No Web Applications
    - Ex: No Denial of Service

Process cont

NEbraskaCERT

- Activities include
  - Planning
    - Rules of Engagement
    - Success criteria
    - Configuring systems and tools for
      - Collection and analysis
      - Secure storage of sensitive information
    - Research specific to organization's assets
  - Data collection
    - External, Internal
    - May be witnessed
    - May be scheduled outside of production

Process cont

NEbraskaCERT

- Activities include
  - Analysis
    - Common: One hour of collection requires 2-6 hours of analysis
  - Reporting
    - Executive summary for CxO level
    - Management report for IT Directors
    - Technical report for system/network administrators

Tools Source

NEbraskaCERT

- Opinions differ...
- Commercial
  - Include technical support
  - May have lower probability of hidden harm
  - Not what hackers use
  - Costly
- Freeware (including Open Source and non-sourced freeware)
  - Useful tool may include an unknown malicious component
  - Closer match to hacker attacks
  - Free

Part-3: Some Discovery Activities

Planning: Rules of Engagement

NEbraskaCERT

- Overview
  - Aka ROE, Rules of Behavior
  - Outlines the framework for external and internal testing
  - Usual goals... all of them simultaneous
    - Minimize impact to operations
    - Maximize test effectiveness (minimize cost)

- Includes
  - Identifying the scope of the assessment in terms of
    - Which networks... which systems
    - What kinds of tests... DoS for example?
    - Shared hosting environment?
  - What process to use if evidence of previous attack discovered

Planning: ROE cont'd

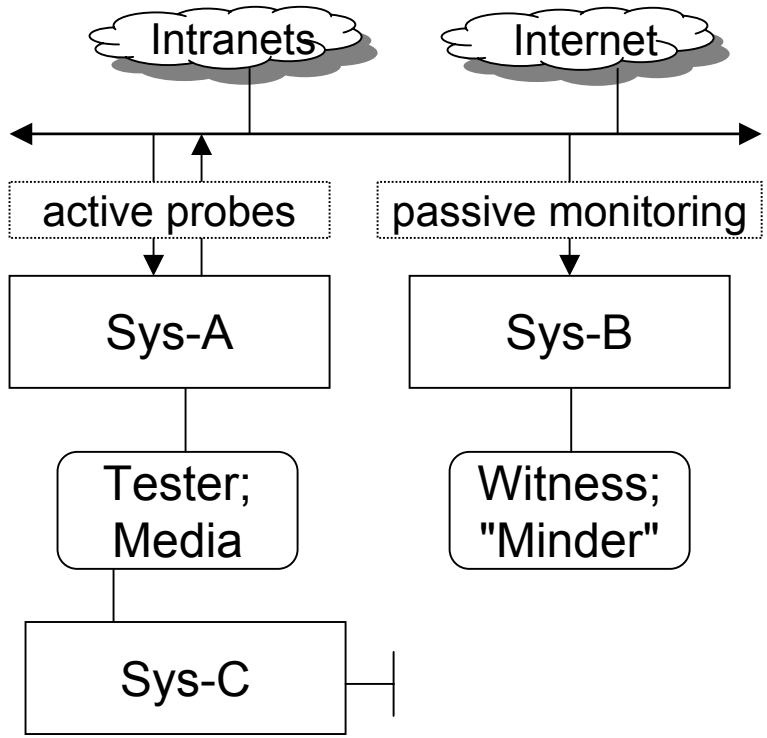
NEbraskaCERT

- Includes cont'd
  - Points of contact
  - Witnesses
    - Who does testing
    - Minder/Witness/Observer
  - Criteria for success
  - How work products are secured
  - May include
    - Formal release stating testing organization will be held harmless and not not liable for unintentional
      - Disruption to operations... e.g., interruptions in service
      - Loss or damage to information and/or information resources

Discovery: Collection

NEbraskaCERT

- Technical collection may require multiple systems
  - Illustration
    - Sys-A: Active
      - Multiple tools
      - Networked
      - OS not hardened
    - Sys-B: Passive
      - Packet sniffer
      - Semi-networked
      - OS not hardened
    - Sys-C: Secure
      - Secure storage, analysis
      - Standalone
      - OS hardened



Discovery: Public Information

NEbraskaCERT

- Done off-site using Internet

- Discover Domains
  - Identify all the domains registered-to/used-by target organization
  - For each domain, discover
    - Contact information
    - DNS servers
  - Query each DNS server to learn about
    - Related domains
    - Exposed servers/services (web, mail, etc.)

Discovery: Public Info cont'd

NEbraskaCERT

- Discover public information about the target
  - Search engines, etc.
  - What are they saying?
    - Are they disclosing too much information with respect to security?
  - What are others saying about them?
    - Identify vendors, partners, etc.
    - Who links to them?
  - What are their employees saying?
  - Are sensitive/vulnerable file types indexed by search engines?

Discovery: Public Info cont'd

NEbraskaCERT

- Discover exposed (public and dmz) subnets and devices
  - Tools include ping, traceroute, IP allocation DBs, etc.
    - IPs may be allocated to hosting provider
  - Identify perimeter routers, firewalls, DMZ servers, etc.
  - Requires caution...

Discovery: External Entry Points

NEbraskaCERT

- Done off-site using Internet
  (or inside, but outside perimeter firewall)

- Use port scanners and related tools to characterize (fingerprint) each device
  - What operating system, version?
  - What services and applications are accessible?

Discovery: Ext Entry Points cont'd

NEbraskaCERT

- Fingerprinting includes
  - Identifying the operating system by small differences in their implementation of TCP/IP, including
    - Response to TCP control messages (RST, FIN, etc.)
    - TTL
    - Initial window size
    - And, so forth
  - Retrieving login prompts for Telnet, FTP, etc to identify the vendor, version, etc.
  - SNMP reads... using "Public" community string to identify vendors, model numbers, etc.

Discovery: Ext Entry Points cont'd

NEbraskaCERT

- Fingerprinting cont'd
  - Examining HTTP (web) servers to identify the vendor, version, tools used to generate the HTML, etc.
    - Response to HEAD and OPTIONS requests
    - Response to GET requests for specific file types
    - Meta content in returned source
  - Note: Target devices/services can tweak the information they provide to deny, frustrate, or deceive this type of discovery

Discovery: Ext Entry Points cont'd

NEbraskaCERT

- Modems
  - Aka War Dialing
  - Find modems connected (even if only occasionally) to
    - Workstations, servers, network
    - PBX
    - Building controls
  - May require auto-dialing range of numbers to detect rogue modems
    - May be obnoxious or even illegal in some states
    - Oftentimes done during different time periods to detect occasional-use modems
      - Normal work hours
      - Nights
      - Weekends

Discovery: Ext Entry Points cont'd

NEbraskaCERT

- WLANs
  - Aka war driving
  - External/Internal activities include
    - Discover rogue access points
    - Discover access points broadcasting their SSID
    - Evaluate WLAN communication encryption, etc.
      - Susceptibility to crack?
    - Evaluate range of access points... accessible from outside the facility?
    - Evaluate connectivity between access points and LAN
      - Where are they connected in relation to firewalls and IDS?

Discovery: Ext Entry Points cont'd

NEbraskaCERT

- Web Applications
  - Scope includes
    - Authentication vulnerabilities
    - Active content
    - Session hijacking
    - Information leakage (under error conditions for example)
  - External/Internal activities include
    - Evaluate web server
      - Fingerprint
      - Susceptibility to vulnerabilities such as path traversal, non-standard encodings, etc.

Discovery: Ext Entry Points cont'd

NEbraskaCERT

- Web Applications cont'd
  - External/Internal activities cont'd
    - Examine source for
      - Script languages, sources
      - Hidden forms, values
      - Client-side validation
      - Authentication methods
    - Examine session management mechanisms
      - Session cookies
      - Parameters
    - Examine persistent cookies

Discovery: Ext Entry Points cont'd

NEbraskaCERT

- Web Applications cont'd
  - Optional external/internal activities
    - Preferably done on non-production testbed environment
    - Done carefully, so not to cause unintentional DoS
    - Manipulate inputs to cause client-side errors
      - Client-side validation
      - Cross-site scripting
      - And, so forth

Discovery: Ext Entry Points cont'd

NEbraskaCERT

- Web Applications cont'd
  - Optional external/internal activities cont'd
    - Manipulate inputs to cause server-side errors
      - May require defeating client-side checks via
        - Direct GETs and POSTs
        - Tester-controlled proxy
        - Edit client-side source
      - Watch for DoS
      - Probe for meaningful error codes
      - Evaluate potential for SQL injection
    - Examine session management
      - Can use in-line proxy to manipulate session cookies, parameters, etc.

Discovery: Internal Entry Points

NEbraskaCERT

- Done on-site with LAN connection (or externally via VPN tunnel)

- Degree of logical access depends on the role
  - Associate: No account
  - Insider: Accounts typical of different classes of insiders

Discovery: Int Entry Points cont'd

NEbraskaCERT

- Internal Infrastructure
  - Tools and activities: Similar to external discovery
  - Additional activities include
    - Evaluating physical access to restricted areas
    - Fingerprint DMZ servers from inside
    - Test outbound firewall/router rules
    - Test extranets to connected partners
    - Searching all subnets via ping sweeps, etc.
    - Testing router configurations, including
      - Passwords
      - Services
      - And, so forth

Discovery: Int Entry Points cont'd

NEbraskaCERT

- Internal Infrastructure cont'd
  - Additional activities cont'd
    - Packet sniffing
      - if switched, use
        - Uplink port
        - ARP poisoning
      - Identify key servers
      - Identify workstations acting as servers
    - Common findings
      - Privacy concerns
      - Unexpected (by organization staff) traffic
        - Protocols
        - Destinations
        - Servers

Discovery: Int Entry Points cont'd

NEbraskaCERT

- Windows domains
  - Tools include MS resource kits, etc.
  - Map domains and trust relationships
  - Identify devices not in IT-controlled domains as potential targets
    - Default WORKGROUP
    - Special-purpose... marketing, building controls, etc.

Discovery: Int Entry Points cont'd

NEbraskaCERT

- Hosts (Server/Workstations)
  - Tools include
    - Port scanners, enumerators, etc.
    - Patch-level analyzers
    - Host-level analyzers, templates
    - Checklists...
  - Evaluation areas include
    - Evaluating OS configuration (hardening)
      - Security settings for anonymous access, etc.
      - Exposed services, shares, etc.
      - Authentication policies
      - Access permissions
      - Installed utilities, applications, etc.

Discovery: Int Entry Points cont'd

NEbraskaCERT

- Hosts cont'd
  - Evaluation areas cont'd
    - Browser and email client configurations
      - Proxies
      - Preview panes
      - Scripting, etc.
    - Audit configuration
      - How are the logs configured
      - Which events logged
      - Which resources monitored
    - Installed versus needed patches... for OS, Browser, Server Apps, Client Apps, etc.

Discovery: Int Entry Points cont'd

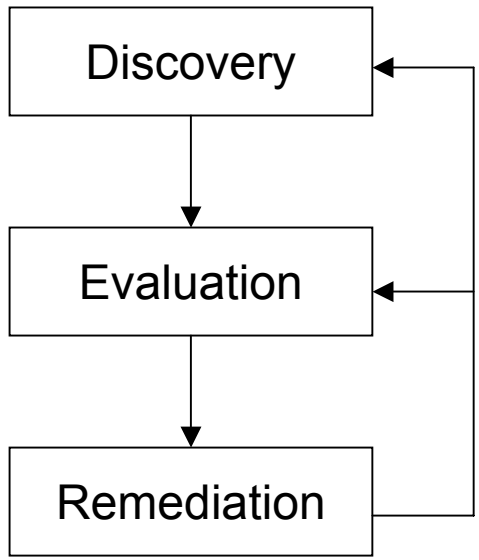
NEbraskaCERT

- Hosts cont'd
  - Evaluation areas cont'd
    - User accounts
      - Dummy Administrator
      - Administrators
        - Shared local administrator
        - Local and domain accounts with administrator rights
      - Other... particularly shared accounts where the password is likely to be simple
      - Comments that may identify the password
      - Note: Password cracking may done during this activity, or as part of off-site analysis

Next Steps

NEbraskaCERT

- Vulnerability Discovery
  - Define (hypothesize) probable vulnerabilities, focusing on the most critical
  - Evaluate...
- Remediation
- Re-test



Questions

Comments

Contributions