FIT5037: Network Security
Computer system vulnerabilities and penetration testing

Faculty of Information Technology
Monash University

May 16, 2019

Copyright Notice

Lecture 10: Computer system vulnerabilities and penetration testing

Lecture Topics:

- Symmetric key cryptography
- Asymmetric key cryptography
- Pseudorandom Number Generators and hash functions
- Authentication Methods and AAA protocols
- Security at Network layer (IPsec)
- Security at Network layer (firewalls and wireless security)
- Security at Transport layer
- Security at Application layer
- Computer system security and malicious code
- **Computer system vulnerabilities and penetration testing**
- Intrusion detection
- Denial of Service Attacks and Countermeasures / Revision

Outline

- Security Assessment
  - Methodology
  - Techniques
    - Examination
    - Testing
- Vulnerability Categories
  - NIST SP 800-115
  - NVD
  - OWASP Top 10 2017
- Common Vulnerability Scoring

Security Assessment[1]

NIST SP 800-115: Technical Guide to Information Security Testing and Assessment

- *assessment object*: host, system, network, procedure, person
- *assessment*: the process of determining how effectively the object meets specific security objectives
- types of assessment methods
  - *Testing*: exercising one or more assessment objects under specified conditions to compare actual and expected behaviour
  - *Examination*: checking one or more assessment objects to understand, clarify, or obtain evidence
  - *Interviewing*: conducting discussions with individuals or groups within an organisation to understand, clarify, identify the location of evidence
- benefits of security assessment methodology
  - consistency and structure in security testing
    - reduce time required to perform the security testing
    - allow reuse of resources
  - faster transition and training of new staff
  - address resource constraints

[1] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Security Assessment Methodology: Phases[2]

- Planning
  - gather information needed
    - assets to be assessed
    - threats of interest against the assets
    - security controls to mitigate the threats
    - assessment approach
  - have a project management plan
    - goals and objective
    - scope
    - requirements
    - team roles and responsibilities
    - limitations
    - success factors
    - assumptions
    - resources
    - timeline
    - deliverables

- Execution
  - identify vulnerabilities
    - system
    - network
    - organisational process

- Post-Execution
  - analyse identified vulnerabilities
    - determine root causes
  - establish mitigation recommendations
  - develop a final report

[2] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Technical Assessment Techniques[3]

NIST SP 800-115 groups assessment techniques as:

Review Techniques

- evaluate to discover vulnerabilities
  - systems,
  - applications,
  - networks,
  - policies and procedures
- review:
  - documentation,
  - log,
  - ruleset,
  - system configuration
  - network packet capture
  - file integrity check
- usually conducted manually

Target Identification and Analysis Techniques

- identify
  - systems
  - open ports
  - services
  - potential vulnerabilities
- automated tools are generally used
  - e.g. `nmap`, `Nesus`, `openvas` etc.
  - may also be conducted manually

Target Vulnerability Validation Techniques

- corroborate existence of vulnerability
  - may be conducted using automated tools or manually
  - password cracking
  - penetration testing
  - social engineering
  - application security testing

[3] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Assessment Methods: Examination[4]

Examination

- primarily involves review of documents
  - policies, procedures, security plans and requirements, standard operating procedures, architecture diagrams, asset inventories, system configurations, rulesets, system logs
- documentation identifies intended:
  - design, installation, configuration, operation and maintenance of systems and networks
- review and cross checking **ensures conformance and consistency**
  - e.g. review of firewall ruleset to ensure compliance with organisation policy
- generally has no (active) impact on the actual systems or networks
  - one example of a passive impact is network sniffing

[4] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Assessment Methods: Testing[5]

Testing

- involves hands-on work with systems and networks
  - identify vulnerabilities
  - can provide information on likelihood of an adversary exploiting the assets
  - measure level of compliance in
    - patch management
    - password policy
    - configuration management etc.
- may provide a more accurate picture of an organisation security posture
  - however often has a narrow scope due to limitations of resources
- more intrusive compared to examination
  - can impact systems and networks
    - each interaction could potentially lead to unexpected results e.g. system halts or denial of service
    - limit the extent of tests which the adversary is not bound to

Combining Examination and Testing provides a more accurate view of security

[5] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Testing Viewpoints: External[6]

- conducted from outside
  - usually from Internet
- begins with reconnaissance techniques
  - public registration data
  - Domain Name System (DNS) server information
  - newsgroup, social media postings
  - IP addresses
  - operating systems
  - technical points of contact
  - any other public information
- next is network discovery and scanning techniques
  - determine external hosts
  - provided services by each host
  - evasion techniques are used against firewalls and ACLs in perimeter routers
- externally accessible hosts are tested for vulnerabilities

[6] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Testing Viewpoints: Internal[7]

- conducted from inside organisation network
  - assume the identity of a trusted insider
    - a general user
    - provided with information a general user will have
    - same privilege as the general user
  - depending on the test and its goals may include privilege of a system or network administrator
    - e.g. testing privilege separation for data custodians and system/network admins
  - goal is to gain more access than given
    - use of privilege escalation techniques
- less limited compared to external
  - conducted behind perimeter defences
    - there may be internal firewalls to pose limitations for internal users
  - network sniffing can be used

[7] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Testing Viewpoints: Overt[8]

- conducted with the knowledge and consent of organisation's IT staff
- also known as white hat testing
- IT staff can provide guidance to limit the impact
- testing provides a training opportunity for IT staff
  - gives context to security requirements
  - may help teach how to perform testing
- less expensive
  - does not require stealth
  - carries less risk

[8] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Testing Viewpoints: Covert[9]

- conducted without the knowledge of IT staff but **with** the full knowledge and permission of upper management
- a trusted third party may be involved as an agent of the assessors, the management, the IT staff and security staff
  - make sure a response measure is not initiated against the assessor for conducting the test
  - mediates activities
  - facilitates communications
- useful in testing IT staff response to perceived security incidents
- purpose is to examine the damage or impact an adversary can cause
  - focus is not on identifying vulnerabilities
    - not all systems and security controls are tested
  - examines the organisation from an adversarial perspective
    - exploiting the most rudimentary vulnerability to gain access
- usually has a defined boundary
  - when to stop
  - prevent damage while showing it could be done
- often time-consuming and expensive
- ovides a better indication of the everyday security due to level of stealth

Examination: Review Techniques[10]

- Document Review
  - technical aspects of policies and procedures are current
    - security policies, architectures, standard operating procedures, incident response plans
  - can discover gaps and weaknesses
    - missing or misconfiguration of security control
  - examples: OS security procedures, protocols that are no longer used, new OS and its protocols
- Log Review
  - proper information is being logged
    - adherence to log management policies
  - reveal problems e.g. misconfiguration, unauthorised access, intrusion attempts
    - examples of useful logs: authentication server, firewall, IDS/IPS, application, patch management
- Ruleset Review
  - collection of rules or signatures to compare against network traffic or system activity
    - forwarding or rejecting a packet, creating an alert, allowing a system event
  - identify gaps and weaknesses on security devices
  - uncover inefficiencies

[10] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Examination: Review Techniques[11] (continued)

- Ruleset Review ...
  - examples
    - Firewalls: each rule is still required, only authorised traffic is permitted, least privilege is enforced
    - IDS/IPS: unnecessary signatures are disabled
- System Configuration Review
  - identifying weaknesses in security configuration controls
    - examples: identifying unnecessary services and applications, improper user accounts and password settings
  - Manual: assessors rely on security configuration guides or check-lists (NIST: National Checklist Program Repository)
  - Automated: NIST Security Content Automation Protocol (SCAP)
- Network Sniffing
  - identify unauthorised and inappropriate activities
    - unsecured protocols
    - unauthorised protocols
  - deployed at
    - the perimeter: assess traffic entering and exiting the network
    - behind firewall: assess rulesets
    - behind IDS/IPS: assess signatures
    - in front of critical system: assess protocols and activities
- e Integrity Checking: identify file modifications

Target Identification and Analysis: Network Discovery[12]

- discover active and responding hosts on a network
  - passive: network sniffing
    - IP addresses, ports, and protocols
    - relationships between hosts: peers, frequency, type of traffic
    - no probe is sent
    - takes more time than active discovery
    - usually conducted inside the organisation network
  - active: several techniques
    - Internet Control Message Protocol: ping
    - OS fingerprinting: a mix of normal, abnormal, and illegal traffic is sent
    - sending packets to common port numbers: TCP SYN request, UDP protocol messages
    - aggressive scans may be detected by firewalls and IDS/IPS
    - can be conducted external to the organisation network
- identify weaknesses
- learn how the network operates
- may detect rogue or unauthorised devices
  - unauthorised OS
  - open ports/active services where there should be none

[12] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Target Identification and Analysis: Network Port and Service Identification[13]

- conducted separately if Network Discovery has not provided the information
  - a tool may provide both Network Discovery and Port/Service Identification
    - e.g. `nmap`
- port scanner to identify: network ports, services running, application that runs the service
- OS fingerprinting
  - the way a host responds to requests
  - collection of open ports
    - e.g. TCP 135, 139, 445 Windows or Unix system running Samba
  - may identify OS incorrectly
    - OS may be configured to respond in a non-standard way
    - firewalls may block certain ports
- application identification
  - communications with the open port is analysed to determine the application
    - comparing the responses with a database
  - version scanning: may also identify application version
    - e.g. banner grabbing
  - may identify application or version incorrectly
- port scanning consumes network bandwidth
- rt scanning does not identify vulnerabilities

[13]

Target Identification and Analysis: Vulnerability Scanning[14]

- attempts to identify vulnerabilities rather than relying on interpretation of network and port scans
- vulnerability scanning tools can usually use the output of network/port scanners
- can identify
  - outdated OS and applications
  - missing patches
  - misconfiguration
  - compliance or deviations from security policy
- provide information for penetration testing
- provide information on how to mitigate discovered vulnerabilities
- host-based
  - vulnerability scanner is installed and run on local hosts
  - is primarily done to identify host OS and application misconfiguration and vulnerabilities
  - vulnerabilities could be either locally or network-exploitable
  - can detect vulnerabilities with higher level of detail
- network-based
  - scanner is run from the network (internally or externally)
  - administrator credentials can be used to extract vulnerability information

[14] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Target Identification and Analysis: Vulnerability Scanning[15] (continued)

- identifying the risk of combined vulnerabilities is a challenge
  - e.g. several low-risk vulnerabilities presenting a higher risk when combined
  - may lead to false level of confidence in security measures in place
  - more reliable: performing a penetration test (may aggregate vulnerabilities)
- a potential difficulty of identifying risk of vulnerabilities is the reported level by scanners
  - each tool may use a different method to define levels
  - makes it difficult to compare findings
  - the risk assigned by the tool may not reflect the actual risk
  - Common Vulnerabilities and Exposure is a list of publicly known vulnerabilities
    - each entry has a CVE ID of the form CVE-YYYY-NNNNN
    - a brief description
    - it also provides a score for the level of each vulnerability (0.0-10.0)
- network-based scanning only identifies vulnerability of active systems during scan
  - only covers surface scan and not the overall risk
  - may have false positives
  - results should be interpreted by experts
- relies on a repository of vulnerability signatures
  - must be updated before scan

[15] T SP 800-115 Technical Guide to Information Security Testing and Assessment

Target Identification and Analysis: Wireless Scanning[16]

- the organisation's wireless environment must be actively tested and made secure
- wireless security assessment considerations:
  - physical location of the facility
    - proximity to public area
  - security level of data transmitted by wireless network
  - connection rate and traffic levels for wireless devices
  - deployment of Wireless IDS (WIDS)
- scanning should be performed using a mobile device
- all IEEE standards and channels should be scanned
- a Radio Frequency (RF) spectrum analyser can assist identifying non-standard or outside frequency range devices
  - determine wireless activity not traffic

[16] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Target Identification and Analysis: Wireless Scanning[17] (continues)

- passive scanning: no data is sent and device is not impacted
  - identify potentially rogue devices
  - identify unauthorised and ad-hoc networks
  - analyse captured traffic for anomalies
- each channel should be scanned for enough amount of time
  - not to miss a node
  - still be efficient
- active scanning
  - can build on information gathered in passive scans
  - attempts to connect to discovered devices
    - perform penetration or vulnerability scanning
  - cautious not to scan neighbouring devices (other organisations)
  - cautious with devices appear to be rogue
    - may belong to visitors to organisation and inadvertently have wireless enabled
- location tracking
  - wireless scanning tools should be used to locate suspicious devices
- Bluetooth scanning: passive scan to evaluate potential presence and activity in compliance with Bluetooth security requirements

[17] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Target Vulnerability Validation: Password Cracking[18]

- process of recovering passwords from stored hashes (one-way functions) or over the network
  - hashes intercepted by a network sniffer
  - retrieved from target system
- dictionary attack: try passwords in a dictionary file
- hybrid attack: use combination rules and additional characters to the dictionary file
  - e.g. John the Ripper password cracker
- brute force: all possible passwords up to certain length
- use of *rainbow tables*
  - lookup tables of pre-computed password hashes
  - require large amount of storage
  - may be ineffective when *salt* is used
- can be performed off-line
  - little or no impact

[18] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

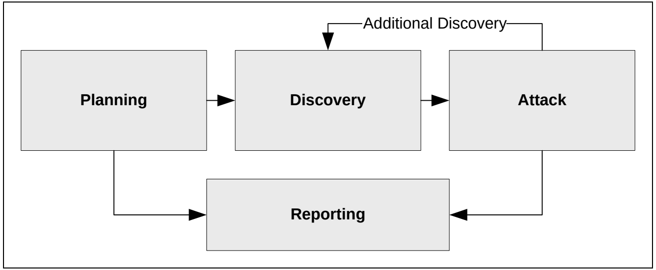
Target Vulnerability Validation: Penetration Testing[19]

- testing in which assessors mimic real-world attack
- identify methods to circumvent security measures of
  - application
  - system
  - network
- involves launching real attacks against real systems
  - data and tools used by the attacker
- often involves looking and using vulnerabilities in one or more systems to gain access
- can be used to
  - determine the system tolerance against real-world attacks
  - the level of sophistication required for an attacker
  - additional countermeasures to mitigate the threat
  - defender's ability to detect attacks and respond

[19] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Target Vulnerability Validation: Penetration Testing Phases[20]

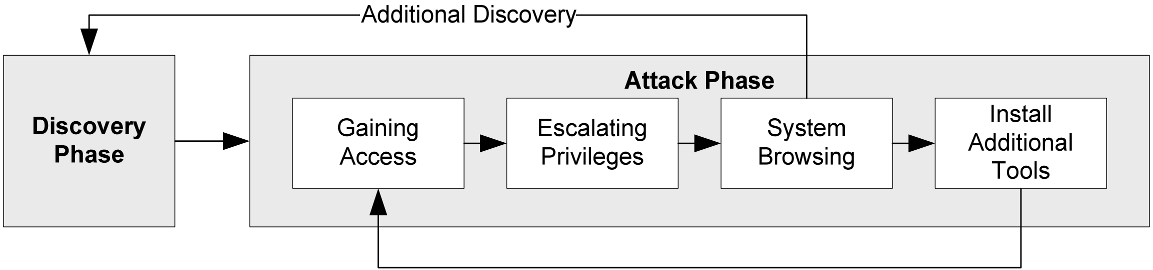
NIST SP 800-115 defines the following four phases



- Planning: rules are identified, management approval is finalised and documented, testing goals are set
- Discovery: two parts
  - information gathering and scanning
  - vulnerability analysis

[20] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Target Vulnerability Validation: Penetration Testing Phases[21] (continued)



- Attack: the heart of penetration test
  - verify previously identified potential vulnerabilities by attempting to exploit them
  - may lead to additional discovery in target network and potential vulnerabilities
  - may allow to escalate privilege
  - if exploitation is successful additional tools can be installed to gain access to additional systems or resources on the network

[21] NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Vulnerability Categories: NIST SP 800-115

- Misconfiguration
  - misconfigured security settings
  - insecure defaults
- Kernel Flaws
  - security flaws in the kernel of OS
    - OS enforces the overall security of a system
- Buffer Overflow
  - unchecked length of input
  - leads to arbitrary code execution
    - shell code injection (heap or stack)
    - return to library (bypass non-executable memory: NX or DEP)
    - ROP (bypass capability checks)
- Insufficient Input Validation
  - user input in a web application to database query
  - operating system commands
- Symbolic Links
  - can be used to trick programs run with higher privilege to modify or list critical system files
- File Descriptor Attacks
  - used to keep track of files instead of file name
  - inappropriately assigned file descriptor to a file could lead to compromise of that file
- Race Conditions
  - if occurred during the time a process is in privileged mode can allow privilege escalation
- Incorrect File and Directory Permissions
  - allow various types of attack
    - reading or writing of password files
    - additions to the list of trusted remote hosts
    - upload of scripts to writable directories with execution permission

- NIST National Vulnerability Database (NVD) based on Common Weakness Enumeration:
  - NVD Categories
  - CWE Layout

Vulnerability Categories: OWASP Top 10 2017[22]

Open Web Application Security Project (OWASP) Top 10 2017

1. Injection
   - vulnerability in web to SQL, LDAP, XPath (navigation through an XML document), OS commands, NoSQL, XML parsers, SMTP headers, expression languages, ORM (Object-Relational Mapping, converting data between incompatible type systems)
   - user-supplied data is not validated, filtered or sanitised
   - dynamic queries are not context aware and used directly in the interpreter
   - hostile data is used directly or concatenated with structured data
2. Broken Authentication
   - default administrative accounts
   - credential attacks
     - allows brute force or dictionary attacks
     - cleartext or weak hashing of passwords
   - session management attacks
     - exposed session IDs
     - session IDs or authentication tokens not properly invalidated

[22] OWASP Top 10 2017

Vulnerability Categories: OWASP Top 10 2017[23] (continued)

3. Sensitive Data Exposure
   - data transmitted in cleartext
   - data stored in cleartext
   - weak cryptographic algorithms used
   - default cryptographic keys are used
4. XML External Entities (XXE)
   - exploitation of vulnerable XML processors
     - accepts XML directly or uploaded XML files parsed by an XML processor
     - vulnerable SAML identity processing and federated identity management
5. Broken Access Control
   - bypassing AC checks through modified URL, internal application state, or the HTML page
   - changing the primary key to another users allowing to view/edit someone else's account
   - metadata manipulation e.g. tampering with JSON Web Token (JWT) access control token, a cookie, or a hidden field
6. Security Misconfiguration
   - missing security hardening in application stack
   - improperly configured permissions on cloud services
   - unnecessary features are enabled or installed
   - error handling reveals information

Vulnerability Categories: OWASP Top 10 2017[24] (continued)

7. Cross-Site Scripting (XSS)
   - allows attacker to execute arbitrary HTML or JavaScript in victim's browser
   - user input is not escaped or sanitised
   - **Reflected XSS**
     - requires the victim to visit a malicious web site or click on a link crafted by attacker
     - works by reflecting the malicious content off of a vulnerable (trusted by user) web site
   - **Stored XSS**
     - the injected script is permanently stored and is executed in visitor's browser of the vulnerable web site
   - **DOM XSS**
     - Document Object Model (DOM) environment in victim's browser is modified so the client side script runs in an unexpected manner
8. Insecure Deserilization
   - works if application or API deserialise hostile or tampered objects supplied by attacker
9. Using Components with Known Vulnerabilities
   - outdated OS, web/application server, DBMS, applications, APIs, runtime environment, libraries
10. Insufficient Logging and Monitoring
    - login, failed login, high-value transactions not logged
    - warnings and errors generate no, inadequate or unclear log messages
    - logs of applications and APIs are not monitored for suspicious activity

[24] OWASP Top 10 2017

References

- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
- OWASP Top 10 2017
- OWASP Cross-Site Scripting (XSS)
- Common Vulnerability Scoring v3.0: Specification Document

Appendix (non-examinable) - Common Vulnerability Scoring v3.0[25]

- composed of three metric groups
  - Base Metric
    - represents characteristics that are constant over time and across user environment
  - Temporal Metric
    - represents characteristics that may change over time but not across user environment
  - Environmental Metric
    - represents characteristics that are relevant and unique to a particular user's environment
- provides a standardised vulnerability scores
- can be translated into a qualitative representation
  - e.g. low, medium, high, and critical
  - help prioritise vulnerability management

[25] Common Vulnerability Scoring v3.0: Specification Document

Appendix (non-examinable) - Common Vulnerability Scoring v3.0: Base Metric Group[26]

Exploitability metrics

- Attack Vector
  - Network: exploitable with network access (OSI layer 3)
  - Adjacent: bound to the same shared physical or logical subnet
  - Local: not exploitable through network access, attacker path is via read/write/execute capabilities
  - Physical: require physical access to device/component
- Attack Complexity
  - Low
  - High: successful attack depends on conditions beyond attacker's control
- Privileges Required
  - None
  - Low: attacker is authorised with basic user privilege
  - High: attacker is authorised with significant privilege
- User Interaction
  - None
  - Required: successful exploitation requires a user to take some action

[26] Common Vulnerability Scoring v3.0: Specification Document

Appendix (non-examinable) - Common Vulnerability Scoring v3.0: Base Metric Group[27] (continued)

Scope

- Unchanged: only affects resources managed by the same authority
  - vulnerable component and the impacted component are the same
- Changed: affects resources beyond the authorisation privileges
  - vulnerable component and the impacted component are different

Impact Metrics

- Confidentiality
  - High: total loss
  - Low: some loss
  - None: no loss
- Integrity (H, L, N)
- Availability (H, L, N)

[27] Common Vulnerability Scoring v3.0: Specification Document

Appendix (non-examinable) - Common Vulnerability Scoring v3.0: Temporal Metrics[28]

Exploit Code Maturity

- Not Defined: does not affect the score
- High: functional autonomous code exists or no exploit is required (manual trigger)
- Functional: functional exploit code is available
- Proof-of-Concept: proof-of-concept exploit code is available
- Unproven: no exploit code is available or an exploit is theoretical

Remediation Level

- Not Defined
- Unavailable: either no solution is available or it is impossible to apply
- Workaround: unofficial, non-vendor solution is available
- Temporary Fix: an official but temporary fix is available
- Official Fix: a complete vendor solution is available

[28] Common Vulnerability Scoring v3.0: Specification Document

Appendix (non-examinable) - Common Vulnerability Scoring v3.0: Temporal Metrics[29] (continued)

Report Confidence

- Not Defined
- Confirmed: detailed report exists, or functional reproduction is possible
- Reasonable: significant details are published without full confidence in root cause (or no access to source code to confirm)
- Unknown: reports of impact that indicate vulnerability is present but he cause is unknown or reports differ

[29] Common Vulnerability Scoring v3.0: Specification Document

Appendix (non-examinable) - Common Vulnerability Scoring v3.0: Environmental Metrics[30]

Security Requirements

- Not Defined
- High: Loss of CIA is likely to have a catastrophic adverse effect on organisation or individuals
- Medium: serious adverse effect
- Low: limited adverse effect

Modified Base Metrics

- allows analyst to adjust the Base metrics when an environment has made general changes for the affected software that changes
  - exploitability
  - scope
  - or impact

[30] Common Vulnerability Scoring v3.0: Specification Document