VulnerabilityAssessment.co.uk

Kevin Orrey

Expand - Collapse

- Report Template
    - Introduction
        - Date carried out
        - Testing Team details
            - Name
            - Contact Nos.
            - Relevant Experience if required.
        - Network Details
            - Peer to Peer, Client-Server, Domain Model, Active Directory integrated
            - Number of Servers and workstations
            - Operating System Details
            -

  - Major Software Applications
  - Hardware configuration and setup
  - Interconnectivity and by what means i.e. T1, Satelite, Wide Area Network, Lease Line Dial up etc.
  - Encryption/ VPN's utilised etc.
  - Role of the network or system
- Scope of test
  - Constraints and limitations imposed on the team i.e. Out of scope items, hardware, IP addresses.
  - Constraints, limitations or problems encountered by the team during the actual test
  - Purpose of Test
    - Deployment of new software release etc.
    - Security assurance for the Code of Connection
    - Interconnectivity issues.
  - Type of Test
    - Complaince Test
    - Vulnerability Assessment
    - Penetration Test
  - Test Type

        - White-Box
            - The testing team has complete carte blanche access to the testing network and has been supplied with network diagrams, hardware, operating system and application details etc, prior to a test being carried out. This does not equate to a truly blind test but can speed up the process a great deal and leads to a more accurate results being obtained. The amount of prior knowledge leads to a test targeting specific operating systems, applications and network devices that reside on the network rather than spending time enumerating what could possibly be on the network. This type of test equates to a situation whereby an attacker may have complete knowledge of the internal network.
        - Black-Box
            - No prior knowledge of a company network is known. In essence an example of this is when an external web based test is to be carried out and only the details of a website URL or IP address is supplied to the testing team. It would be their role to attempt to break into the company website/ network. This would equate to an external attack carried out by a malicious hacker.
        - Grey-Box
            - The testing team would simulate an attack that could be carried out by a disgruntled, disaffected staff member. The testing team would be supplied with appropriate user level privileges and a user account and access permitted to the internal network by relaxation of specific security policies present on the network i.e. port level security.
- Executive Summary (Brief and Non-technical)
    - OS Security issues discovered with appropriate criticality level specified
        - Exploited
            -

Causes

      - Hardware failing
      - Software failing
      - Human error
  - Unable to exploit - problem area
    - Causes
      - Hardware failing
      - Software failing
      - Human error
- Application Security issues discovered with appropriate criticality level specified
  - Exploited
  - Unable to exploit - problem area
- Physical Security issues discovered with appropriate criticality level specified
  - Exploited
  - Unable to exploit - problem area
- Personnel Security issues discovered with appropriate criticality level specified
  -

  - Exploited
  - Unable to exploit - problem area
- General Security issues discoveredwith appropriate criticality level specified
  - Exploited
  - Unable to exploit - problem area

- Technical Summary
  - OS Security issues discovered
    - File System Security
      - Details of finding
        - Example: A FAT partition was found. FAT by default does not give the ability to set appropriate access control permissions to files. In addition moving files to this area removes the protection of the current acls applied to the file.
      - Recommendation and fix
        - Example: Format the file system to NTFS.
    - Password Policy
      - Details of finding

Example: LM Hashes found still being utilised on the network.

  - Recommendation and fix
    - Example: Ensure NTLM2 is enforced by means of the correct setting in Group Policy.
- Auditing Policy
  - Details of finding
    - Example: Logon success adn failure was not enabled
  - Recommendation and fix
    - Example: Ammend appropriate Group Policy Objects and ensure it is tested and then applied to all relevant Organisational Units etc.
- Patching Policy
  - Details of finding
    - Example: Several of the latest Microsoft patches were found to be missing
  - Recommendation and fix
    - Example: Ensure a rigorous patching policy is instigated after first being tested on a development LAN to ensure stability. Review the settings on the WSUS server and ensure that it is regularly updated and an appropriate update strategy is instigated for the domain.
- Anti-virus Policy

    - Details of finding
      - Example: Several workstations were found to have out of date anti-virus software. In addition where it was found to be installed the actual product was found to be mis-configured and did not provide on-access protection.
    - Recommendation and fix
      - Example: Ensure all workstations are regualrly updated and configured correctly to ensure maximum protection is afforded
  - Trust Policy
    - Details of finding
      - Example: Users from one domain were unable to access resources on another tree.
    - Recommendation and fix
      - Example: Review transitive and non-transitive trusts and ensure that all relevant trusts have been established.
- Web Server Security
  - File System Security
    - Details of finding
      - Example: i.e. Incorrect permission on www root
    -

    - Recommendation and fix
        - Example: Apply more stringent permissions or remove various users/groups that currently have access to this area.
- Password Policy
    - Details of finding
        - Example: Areas of the website that should be Protected did not have any password mechanism enforced.
    - Recommendation and fix
        - Example: Ensure areas that require access to be limited are password protected.
- Auditing Policy
    - Details of finding
        - Example: Web server logs were not being reviewed for illicit behavious.
    - Recommendation and fix
        - Example: Regulalrly review all audit logs.
- Patching Policy
    - Details of finding
        - Example: The latest patch was not applied to the server leaving it susceptible to a Denial of Service Attack.

    - Recommendation and fix
      - Example: Apply the latest patch after testing on a development server to ensure compatibility with installed applications and stability of the server is maintained.
  - Lockdown Policy
    - Details of finding
      - Example: The IIS lockdown tool has not been applied to the web server.
    - Recommendation and fix
      - Example: Apply the IIS lockdown tool to the server after first testing on a development server to ensure compatibility with installed applications and stability of the server is maintained.
- Database Server Security
  - File System Security
    - Details of finding
      - Example: Loose access control permissions were found on directories containing important configuration files that govern access to the server.
    - Recommendation and fix
      - Example: Ensure stringent access control permissions are enforced.

Password Policy

  - Details of finding
    - Example: Clear text passwords were found stored within the database.
  - Recommendation and fix
    - Example: Ensure all passwords, if required to be stored within the database are encrypted and afforded the maximum protection possible.
- Auditing Policy
  - Details of finding
    - Example: Reviewing the audit logs from the TNS Listener were not being carried out.
  - Recommendation and fix
    - Example: Ensure all relevant audit logs are regularly inspected. Audit logs may give you the first clue to possible attempts to brute force access into the database.
- Patching Policy
  - Details of finding
    - Example: The latest Oracle CPU was not installed, leaving the system susceptible to mutilple buffer and heap overflows and possible Denail of Service attacks.
  - Recommendation and fix

      - Example: Install the latest Oracle CPU after first trsting on a development server to ensure adequate compatibility and stability.
  - Lockdown Policy
    - Details of finding
      - Example: Numerous extended stored procedures were directly accesible by the public role.
    - Recommendation and fix
      - Example: Ensure the public role is revoked from all procedures that direct access is not required or utilised.
  - Trust Policy
    - Details of finding
      - Example: Clear text Link passwords were discovered.
    - Recommendation and fix
      - Example: Ensure all Link passwords are encrypted, review the requirement to utilise these Links on a regualr basis.
- General Application Security
  - File System Security
    - Details of finding

    - Recommendation and fix
- Password Policy
    - Details of finding
    - Recommendation and fix
- Auditing Policy
    - Details of finding
    - Recommendation and fix
- Patching Policy
    - Details of finding
    - Recommendation and fix
- Lockdown Policy
    - Details of finding
    - Recommendation and fix
- Trust Policy
    - Details of finding
    - Recommendation and fix

Business Continuity Policy

- Backup Policy
  - Details of finding
  - Recommendation and fix
- Replacement premises provisioning
  - Details of finding
  - Recommendation and fix
- Replacement personnel provisioning
  - Details of finding
  - Recommendation and fix
- Replacement software provisioning
  - Details of finding
  - Recommendation and fix
- Replacement hardware provisioning
  - Details of finding
  - Recommendation and fix

Replacement document provisioning

- Details of finding
- Recommendation and fix

- Annexes
  - Glossary of Terms
    - Buffer Overflow
      - Normally takes the form of inputting an overly long string of characters or commands that the system cannot deal with. Some functions have a finite space available to store these characters or commands and any extra characters etc. over and above this will then start to overwrite other portions of code and in worse case scenarios will enable a remote user to gain a remote command prompt with the ability to interact directly with the local machine.
    - Denial of Service
      - This is an aimed attacks designed to deny a particular service that you could rely on to conduct your business. These are attacks designed to say overtax a web server with multiple requests which are intended to slow it down and possibly cause it to crash. Traditionally such attacks emanated from one particular source.
    - Directory Traversal
      - Basically when a user or function tries to "break" out of the normal parent directory specified for the application and traverse elsewhere within the system, possibly gaining access to sensitive files or directories in the process.
    - Social Engineering
      -

        Normally uses a limited range of distinct subject matter to entice users to open and run an attachment say.
        Usually associated with phishing/E-mail type attacks. The main themes are:
        • Sexual - Sexual ideas/pictures/websites,
        • Curiosity - Friendly themes/appealing to someone's passion or obsession,
        • Fear - Reputable sources/virus alert,
        • Authority - Current affairs/bank e-mails/company e-mails.

    - SQL Injection etc.
        - Basically when a low privileged user interactively executes PL/SQL commands on the database server by adding additional syntax into standard arguments, which is then passed to a particular function enabling enhanced privileges.

- Network Map/Diagram
- Accompanying Scan Results - CD-ROM
- Vulnerability Definitions
    - Critical
        - A vulnerability allowing remote code execution, elevation of privilege or a denial of service on an affected system.
    - Important
        - A security weakness, whose exploitation may result in the compromise of the Confidentiality, Integrity or Availability of the company’s data.
    - Information Leak
        - Insecure services and protocols are being employed by the system allowing potentially allowing unrestricted access to sensitive information i.e.:
          a. The use of the Finger and Sendmail services may allow enumeration of User IDs.

b. Anonymous FTP and Web based services are being offered on network devices or peripherals.
c. Disclosure of Operating System, Application version details and personal details of system administration staffs.

- Concern
  - The current systems configuration has a risk potential to the network concerned though the ability to exploit this is mitigated by factors such as default configuration, auditing, or the difficulty level or access level required to carry out an exploit. This includes the running of network-enabled services that are not required by the current business continuity process.
- Unknowns
  - An unknown risk is an unclear response to a test or an action whose impact can be determined as having minimal impact on the system. The test identifying this risk may or may not be repeatable. While the results do not represent a security risk per see, they should be investigated and rectified where possible. Unknowns may also be due to false positives being reported, however, do require follow up response.

- Details of Tools Utilised.
- Methodology Utilised.
  - Reconnaissance
    - The tester would attempt to gather as much information as possible about the selected network. Reconnaissance can take two forms i.e. active and passive. A passive attack is always the best starting point as this would normally defeat intrusion detection systems and other forms of protection etc. afforded to the network. This would usually involve trying to discover publicly available information by utilising a web browser and visiting newsgroups etc. An active form would be more intrusive and may show up in audit logs and may take the form of an attempted DNS zone transfer or a social engineering type of attack.
  - Enumeration
    - The tester would use varied operating system fingerprinting tools to determine what hosts are alive on the

network and more importantly what services and operating systems they are running. Research into these services would then be carried out to tailor the test to the discovered services.

- Scanning
    - By use of vulnerability scanners all discovered hosts would be tested for vulnerabilities. The result would then be analysed to determine if there any vulnerabilities that could be exploited to gain access to a target host on a network.
- Obtaining Access
    - By use of published exploits or weaknesses found in applications, operating system and services access would then be attempted. This may be done surreptitiously or by more brute force methods. An example of this would be the use of exploit engines i.e. Metasploit or password cracking tools such as John the Ripper.
- Maintaining Access
    - This is done by installing a backdoor into the target network to allow the tester to return as and when required. This may be by means of a rootkit, backdoor trojan or simply the addition of bogus user accounts.
- Erasing Evidence
    - The ability to erase logs that may have detected the testing teams attempts to access the network should ideally not be possible. These logs are the first piece of evidence that may prove that a possible breach of company security has occurred and should be protected at all costs. An attempt to erase or alter these logs should prove unsuccessful to ensure that if a malicious attacker did in fact get access to the network then their every movement would be recorded.
- See Penetration Test Framework for more details

- Sources of Information
    -

National Security Agency

- Microsoft
  - Microsoft Windows 2000 Security Configuration Guide.
  - Windows Server 2003 Security Guide.
  - Windows XP Security Guide.
  - The Threats and Countermeasures guide.
- Auscert
- CISSecurity
- ISO27001/2
- Sorbanes Oxley
- HIPAA