Obligatory reading
Network security
Unit 2

Obligatory reading
Network security
Unit 2

Penetration Testing

NCSC
https://www.ncsc.gov.uk/guidance/vulnerability-scanning-tools-and-services

Automated process to scan a security system for defects.
This covers areas such as the patch management process, hardening procedures and the Software Development Lifecycle (SDLC). Services or products that offer vulnerability scanning are also commonly known as Vulnerability Assessment Systems (VASs).

Why scanning for defects:

- can be automated according to schedule
- speed; hundreds or thousands of checks in a fast pace
- cost effective; its cheapish
- its scalable, so it can be scalable according to the usage of the cloud
- compliance; can be ensured that tests are compliant with organisations desirers and industry standards
- accuracy; reliable results

VMP programs typically include the following processes:

- ***System discovery***: Identifying assets owned by your organisation
- ***Asset classification***: Assigning assets into groups or categories based on common characteristics
- ***Vulnerability detection***: Finding and validating vulnerabilities in assets
- ***Vulnerability triage***: Prioritising vulnerabilities according to technical or business objectives
- ***Vulnerability remediation***: Advising on and verifying the fixing of identified issues
- ***Vulnerability disclosure***: Providing a mechanism for security researchers to disclose relevant vulnerabilities to you. Please refer to the NCSC's Vulnerability Disclosure Toolkit for information on creating your own vulnerability disclosure process.

Appropriate scanner

Vulnerability scanners are usually categorized according to what they scan and on what asset.

Application scanner

- Targets web application
- Targets native applications

Specialist scanner

- More accurate and relevant result for the type of target

- Usually, an organisation system will contain too much for a specialist scanner to provide viable results

You should therefore seek to first establish a foundational level of generalised scanning, to ensure a good level of coverage on the most common infrastructure issues.

Infrastructure scanners
Infrastructure scanning solutions are typically focused on identifying and testing services that are accessible to the rest of the network or the Internet as a whole. For this, they often include host discovery and port scanning functionality.

Whilst some network vulnerability scanners also use more advanced methods than this and can even support checks that first require authentication, they typically aim for breadth instead of depth when it comes to coverage.

Network vulnerability scanners are therefore an excellent choice for monitoring networks with large external footprints for new common vulnerabilities that could be exploited by attacks from the Internet or your internal corporate network

Web application scanners

- Explicitly detect vulnerabilities in applications and web-based services exposed over HTTP/s
- Interacts with applications as a web browser would, but sends requests faster
- Formulated elicit as to expose vulnerabilities
- web application scanners are designed to detect vulnerabilities in custom-built (and often complex) web applications.
- Aligned with OWASP top 10
- *Web application security scanners are an excellent choice when used in conjunction with network vulnerability scanners, or when custom web applications account for most of your external network footprint and therefore present most of the risk to your business or organisation. The NCSC's own Web Check service is an example of such a service, albeit one that can only be offered to the public sector. Web Check is specifically designed to be 'light touch' and aimed towards detecting the most common and widely applicable security issues.*

Decide what to scan, when to scan and which assists. Automate simple tasks, let human focus on complex vulnerabilities.

Obligatory reading
Network security
Unit 2

Penetration Testing – advice on how to get the most from penetration testing

Advice on how to get the most from penetration testing
https://www.ncsc.gov.uk/guidance/penetration-testing

Core tool, not magic bullet.
Finding vulnerabilities by using same tools as adversaries.

- Should not be used as primary tool to *find* vulnerabilities
- Compared to financial audit; ideally, should be a rough idea before starting what will be found

The ideal

A well-scoped penetration test can give confidence that the products and security controls tested have been configured in accordance with good practice and that there are no common or publicly known vulnerabilities in the tested components, ***at the time of the test.***

- Appropriate method for identifying risk present on a **specific, operational system** that consist of products from multiple vendors
- Not appropriate for specific product testing

Types of testing

Whitebox testing	Blackbox testing
Full information about the target is shared with the testers. This type of testing confirms the efficacy of internal vulnerability assessment and management controls by identifying the existence of known software vulnerabilities and common misconfigurations in an organisation's systems.	No information is shared with the testers about the internals of the target. This type of testing is performed from an external perspective and is aimed at identifying ways to access an organisation's internal IT assets. This more accurately models the risk faced from attackers that are unknown or unaffiliated to the target organisation. However, the lack of information can also result in vulnerabilities remaining undiscovered in the time allocated for testing.

Can be *either* Blackbox or Whitebox testing:

- **Vulnerability identification in bespoke or niche software**

Most used in web applications. This type of testing must give feedback to developers on coding practices which avoid introducing the categories of vulnerability identified.

- **Scenario driven testing aimed at identifying vulnerabilities** –
  The penetration testers explore a particular scenario to discover whether it leads to a vulnerability in your defences. Scenarios include: Lost laptop, unauthorised device connected to internal network, and compromised DMZ host, but there are many others possible. You should consider, based on previous incidents, which scenarios are most relevant to your organisation.

- **Scenario driven testing of detection and response capability**
  In this version of scenario driven testing, the aim is to also gauge the detection and response capabilities your organisation has in place. This will help you understand their efficacy and coverage in the scenario. This is an area of current work by the NCSC, further information will be available shortly, please contact us if you have a particular need in this area.

Functional testing of security controls should still occur.

- Testing plan should always include **positive tests** (for example, logon box lights up or login must be completed)
- Negative testing.
  May be included when skills to perform it are available in the organisation

Model penetration test engagement

1. Initial engagement
2. Scoping
3. Testing
4. Reporting
5. Follow up

Model reports:

- You wish to know what the impact of an attacker exploiting a vulnerability would be, and how likely it is to occur
- You have an internal vulnerability assessment and management process

Scoping

Scoping a penetration test should involve:

1. All relevant risk owners
2. Technical staff knowledgeable about the target system
3. A representative of the penetration test team

Where the goal of the test is to ensure good vulnerability management:

1. Risk owners should outline any areas of special concern
2. Technical staff should outline the technical boundaries of the organisation's IT estate
3. The penetration test team should identify what testing they believe will give a full picture of the vulnerability status of the estate

Assuming you have one, a current vulnerability assessment should be shared with the testers at this stage. Testing can then be designed to support a reasonable opinion on the accuracy and completeness of the internal vulnerability assessment.

Special requirements

During scoping, you should outline any issues which might impact on testing. This might include the need for out-of-hours testing, any critical systems where special handling restrictions are required, or other issues specific to your organisation.

Plan of action

The output of the scoping exercise should be a document stating:

1. The technical boundaries of the test
2. The types of tests expected
3. The timeframe and the amount of effort necessary to deliver the testing - usually given in terms of resource days
4. Depending on the type of approach agreed, this document may also contain several scenarios or specific 'use cases' to test
5. The penetration testing team's requirements. This will allow you to do any necessary preparation before the date of the test. For example, by creating test accounts or simply allocating desk space
6. Any compliance or legislative requirements that the testing plan must meet
7. Any specific reporting requirements, for example the inclusion of CVSS scores or use of CHECK severity levels
8. Any specific time constraints on testing or reporting, that a penetration testing company will need to consider when allocating resources

Testing
Staying in contact

During the test phase, you should ensure that a technical point of contact is available at all times. The point of contact does not need to spend all their time working with the test team but should be available at short notice. This allows the test team to raise any critical issues found during testing, and resolve problems which are blocking their testing (such as network misconfiguration).

Taking care

The testers should make every effort to avoid causing undue impact to the system being tested. However, due to the nature of penetration testing, it's impossible to guarantee that no unexpected reactions to testing will occur.

Changing scope

During a penetration test or security assessment, the testing team may identify additional systems or components which lie outside of the testing scope but have a potential impact on the security of the system(s) which have been defined as in scope.

In this event, the testing team may either suggest a change to the scope, which is likely to alter testing time frames and cost, or they may recommend that the exclusion of such components be recorded as a limitation on testing.

The decision on which would be the preferred option will generally be down to the risk owner, with the penetration team responsible for clearly articulating the factors to consider.

Reporting

The test report should include:

1. Any security issues uncovered
2. An assessment by the test team as to the level of risk that each vulnerability exposes the organisation or system to
3. A method of resolving each issue found
4. An opinion on the accuracy of your organisation's vulnerability assessment
5. Advice on how to improve your internal vulnerability assessment process
6. A debriefing can also be useful. At this meeting the test team run through their findings and you can request further information or clarification of any issues.

Security rating

When rating vulnerabilities it is common for penetration testers (often at customer behest) to use the Common Vulnerability Scoring System which attempts to give a numerical score identifying the severity of a vulnerability.

To simplify this measurement, CHECK reports are required to state the level of risk as HIGH, MEDIUM, LOW or INFORMATIONAL in descending order of criticality. For CHECK reports, scoring systems such as CVSS may be used in addition to (but not in place of) this.

Whilst vulnerabilities are ordinarily categorised at one of these levels in a consistent manner, exceptions can sometimes occur. For example, other mitigating controls in place could minimise the effectiveness of a vulnerability, or the presence of additional vulnerabilities could have a synergistic effect.

Any deviation from associating a vulnerability with its standard rating should be documented and justified by the penetration testing team.

Obligatory reading
Network security
Unit 2

Improving Web application security : threats and countermeasures

Meier, J. D; Microsoft Corporation

https://archive.org/details/improvingwebappl00micr/page/n5/mode/2up

used as a guidebook for assignments as of and when needed.

Obligatory reading
Network security
Unit 2

Getting started with the Threat Modelling Tool

https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

- recommended to use templates if not skilled

Data flow diagram
Analysing threats; SDL approach → STRIDE

Human user as outside entity = square
Human sending commands to web browser = circle
Web browser consulting database = two parallel lines