Penetration Testing

#week7

Powerful tool for analysing IT security but must be:

- Properly Commissioned
- Correctly Scoped
- Integrated with routine security measures
- Used as part of a comprehensive security strategy

It's primary function is to be viewed as a method for gaining assurance in your vulnerability assessment and management process

It is not a primary method for identifying vulnerabilities, essentially think of it as quality assurance for your security processes.

In an ideal scenario you should know what a pen tester will find before they find it, this means having good understanding of vulnerabilities, effective internal assessment processes, and using third-party tests for verification

Highly experienced testers finding unknown vulner abilities is the EXCEPTION not the rule. You should instead expect:

- To find known issues
- Occasional discovery of minor issues

Pen testers typically identify

- Technical risk levels from software vulnerabilities
- Hardware vulnerability exposure
- Configuration compliance
- Known vulnerabilities in tested components
  It's important to note results are only valid at the time of testing

A properly scoped test provides assurance that:

- Products tester are configured to best practices
- Security controls are properly implemented
- No common vulnerabilities exist in tested components
- No publicly known vulnerabilities are present

It's important to remember that tests are only valid at time of testing, normally tests have 12+ months between tests. New threats emerge constantly and systems are always change and evolve.

Test need to be performed by qualified an experience staff, this is because:

- Tests cant be entirely procedural
- No exhaustive test case exists
- Expertise determines what gets discovered
- Quality directly linked to tester abilities

Testing

Test basis

How much information is provided

Black box testing:

- Testers have minimal prior knowledge
- Simulates external attacker and tests what an outside could discover
- Advantage of this is its the most realistic external threat simulation

White box testing

- Testers have full system knowledge, meaning access to architecture, code, credentials
- As such can test more thoroughly and is a more efficient use of time
- The advantage of this is that it's a more comprehensive coverage of potential issues.

Test Types

Bespoke Software Vulnerability Testing

- Focused on vulnerability identification in customer or niche software
- Is most commonly applied to web applications
- It's critical that feedback is provided to developers

Scenario-Driven Vulnerability Testing

- Focused on exploring specific scenarios to discover defense vulnerabilities
- For example, lost laptop with company details, insider threat simulation
- The key is to choose scenarios based on your organisations risk profile and previous incidents.

Detection and Response Testing

- Tests vulnerabilities AND organisational response capabilities
- Evaluates detection capability effectiveness, response process efficiency, coverage of security controls, Incident handling procedures

Sometimes standard tests aren't enough

Penetration testing does NOT replace normal security testing, you still need regular internal testing

Model Engagement

Pen tests typically follow the structure:

1. Initial engagements, selecting team
2. Scoping, defining tests
3. Testing, conducting assessments
4. Reporting, documenting findings
5. Follow-up, remediation and improvement

This model assumes:

- You want to know the impact of exploitation
- How likely the vulnerabilities is to be exploited
- If you have an internal vulnerability

Each finding should have a severity rating that demonstrates the:

- Ease of exploitations
- Required attacker skills
- Available exploits
- Potential damage

It your responsibility to act on the risk assessment

Common pitfalls of pen testing are:

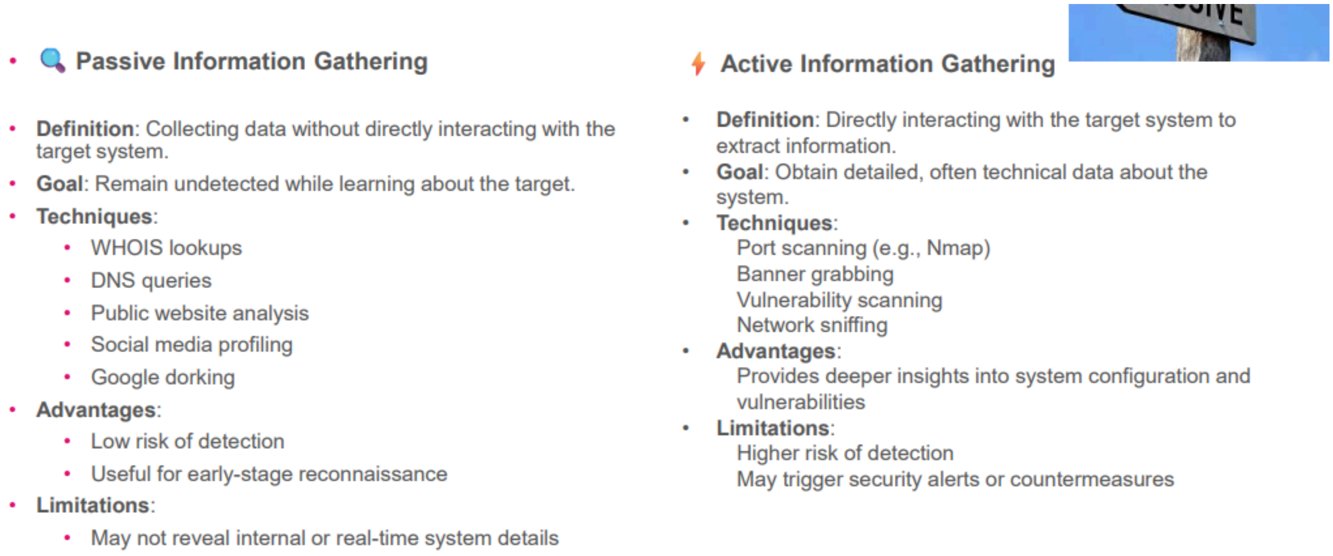
- Treating pen testing as a one time thing
- Ignoring

Test Methodology

What steps do pen testers take?

- Reconnaissance: Gathering information about target organisation
- Scanning & Enumerations: Identifying live hosts, ports, and services
- Vulnerability Assessment, Detecting weaknesses in systems
- Exploitation, Attempting to compromise identified vulnerabilitites
- Post-Exploitation, Maintaining access and expanding control
- Reporting, documenting findings

Penetration Testing Tools



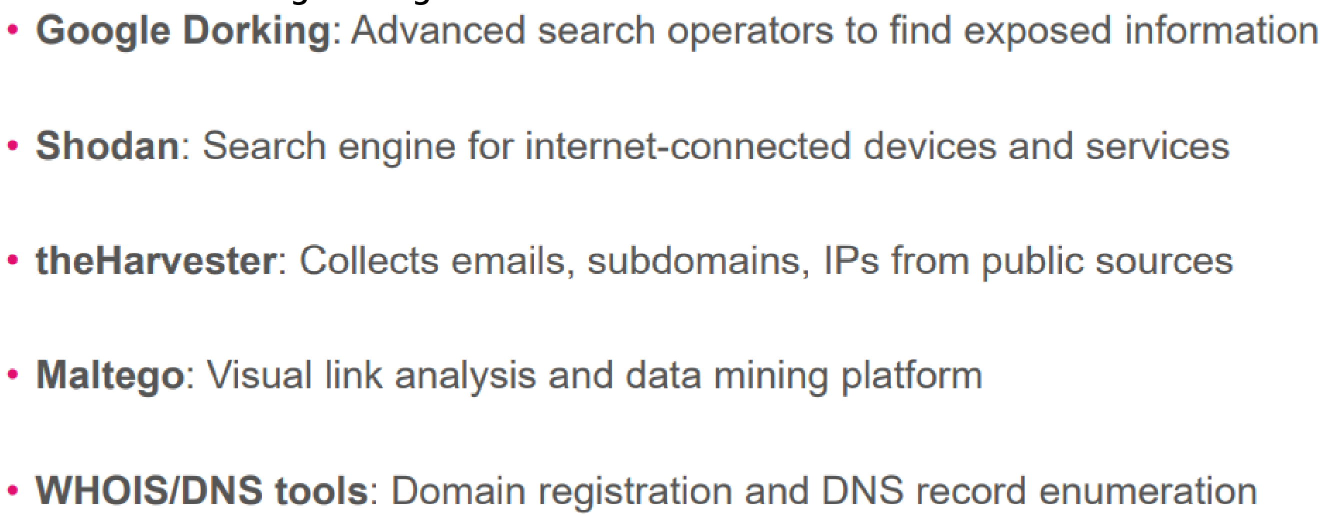
- 🔍 **Passive Information Gathering**

- **Definition**: Collecting data without directly interacting with the target system.
- **Goal**: Remain undetected while learning about the target.
- **Techniques**:
  - WHOIS lookups
  - DNS queries
  - Public website analysis
  - Social media profiling
  - Google dorking
- **Advantages**:
  - Low risk of detection
  - Useful for early-stage reconnaissance
- **Limitations**:
  - May not reveal internal or real-time system details

⚡ **Active Information Gathering**

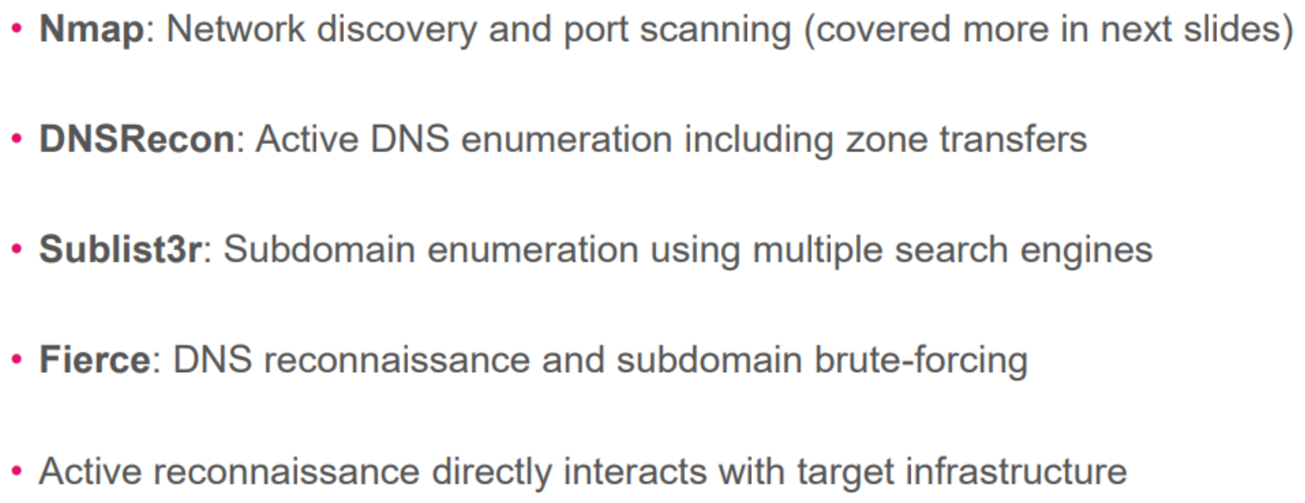
- **Definition**: Directly interacting with the target system to extract information.
- **Goal**: Obtain detailed, often technical data about the system.
- **Techniques**:
  Port scanning (e.g., Nmap)
  Banner grabbing
  Vulnerability scanning
  Network sniffing
- **Advantages**:
  Provides deeper insights into system configuration and vulnerabilities
- **Limitations**:
  Higher risk of detection
  May trigger security alerts or countermeasures

Passive information gathering



- **Google Dorking**: Advanced search operators to find exposed information
- **Shodan**: Search engine for internet-connected devices and services
- **theHarvester**: Collects emails, subdomains, IPs from public sources
- **Maltego**: Visual link analysis and data mining platform
- **WHOIS/DNS tools**: Domain registration and DNS record enumeration

Active information gathering

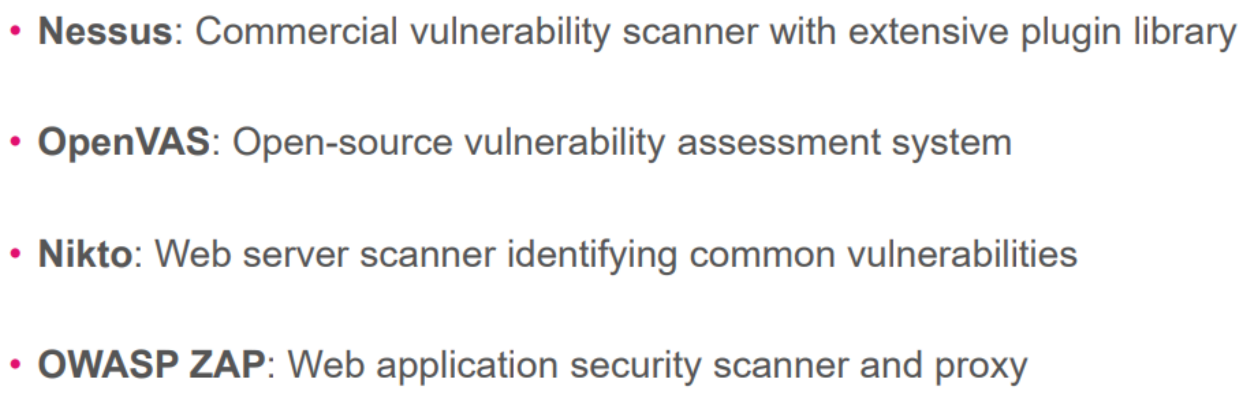


- **Nmap**: Network discovery and port scanning (covered more in next slides)
- **DNSRecon**: Active DNS enumeration including zone transfers
- **Sublist3r**: Subdomain enumeration using multiple search engines
- **Fierce**: DNS reconnaissance and subdomain brute-forcing
- Active reconnaissance directly interacts with target infrastructure

NMAP

Industry standard network scanner
Supports multiple scan types
Essential syntax `nmap -sV -sC -oA output target`
Note that random network scanning is illegal

Vulnerability Scanning Tools



- **Nessus**: Commercial vulnerability scanner with extensive plugin library
- **OpenVAS**: Open-source vulnerability assessment system
- **Nikto**: Web server scanner identifying common vulnerabilities
- **OWASP ZAP**: Web application security scanner and proxy

Exploitation Frameworks

- **Metasploit Framework**: Comprehensive exploitation and post-exploitation platform
- Contains hundreds of exploit modules for various vulnerabilities
- Payload generation, encoding, and delivery mechanisms
- Integrates with scanning tools for automated exploitation
- Caution: Only use against authorised targets with proper scope

Password Cracking Tools

- **John the Ripper**: Fast password hash cracking with multiple attack modes
- **Hashcat**: GPU-accelerated password recovery supporting many hash types
- **Hydra**: Network login cracker for various protocols (SSH, FTP, HTTP, etc.)
- **CeWL**: Custom wordlist generator from website content
- **Dictionary**, brute-force, and rule-based attack strategies

Post-Exploitation Tools

- **Mimikatz**: Windows credential extraction from memory
- **BloodHound**: Active Directory attack path mapping
- **PowerSploit**: PowerShell-based post-exploitation framework
- **Empire/Starkiller**: Post-exploitation agent and C2 framework

Social Engineering Tools

- **Social Engineering Toolkit (SET):** Framework for social engineering attacks
- **GoPhish**: Phishing campaign management and tracking
- **King Phisher**: Phishing campaign toolkit with analytics
- **Email templates**, credential harvesting, and reporting features

Network Traffic Analysis Tools

- **Wireshark**: Industry-standard packet capture and analysis tool
- **tcpdump**: Command-line packet analyzer for quick captures
- **Bro/Zeek**: Network security monitoring framework
- **NetworkMiner**: Network forensics analysis tool