Final presentation

Steven Lemaire

Idea of the problem

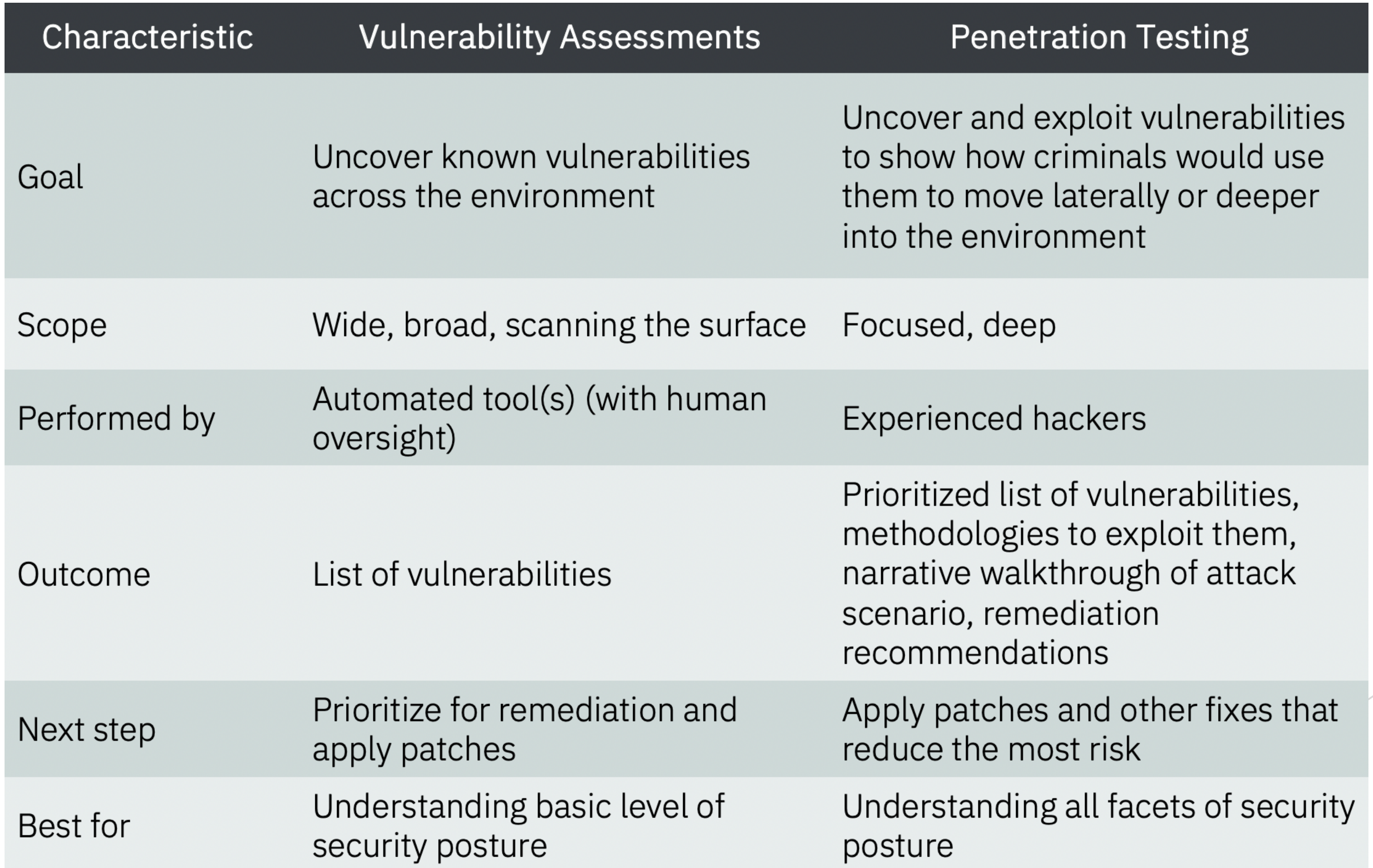
- Security PROBLEMS in Telecommunication Networks may concern 3 points
  - Confidentiality : Access to the only people permitted
  - Integrity : No change of the information
  - Availability : Data always available when we need

ISECOM

- To protect your system there are 2 ways, first one is manually
- The Open Source Security Testing Methodology Manual is a complete methodology for the testing, analysis and measurement of operational security towards building the best possible security defenses. This company makes penetration testing :
  - Reconnaissance
  - Scanning and enumeration
  - Exploitation (gaining access)
  - Post-exploitation (maintaining access)
  - Covering tracks

Penetration test

- Discover other users of the network, list them, obtain data from users by observing the exchanges.



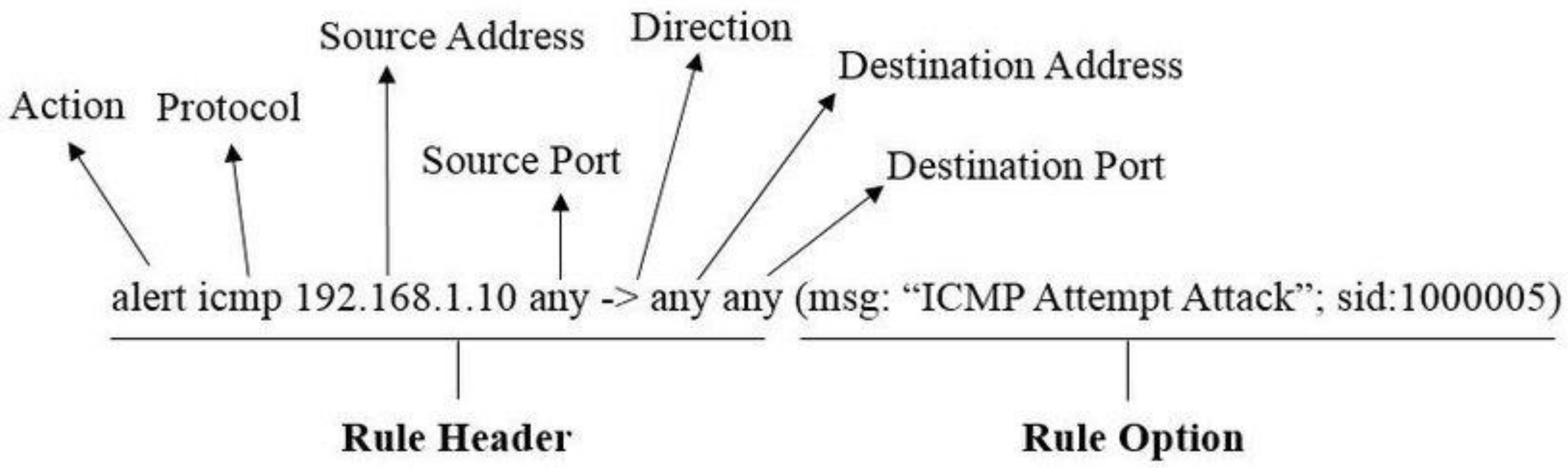
Characteristic	Vulnerability Assessments	Penetration Testing
Goal	Uncover known vulnerabilities across the environment	Uncover and exploit vulnerabilities to show how criminals would use them to move laterally or deeper into the environment
Scope	Wide, broad, scanning the surface	Focused, deep
Performed by	Automated tool(s) (with human oversight)	Experienced hackers
Outcome	List of vulnerabilities	Prioritized list of vulnerabilities, methodologies to exploit them, narrative walkthrough of attack scenario, remediation recommendations
Next step	Prioritize for remediation and apply patches	Apply patches and other fixes that reduce the most risk
Best for	Understanding basic level of security posture	Understanding all facets of security posture

Kali Linux

- Automatic tool
- The Kali Linux penetration testing platform contains a vast array of tools and utilities, from information gathering to final reporting, that enable security and IT professionals to assess the security of their systems.

Work to be done

- Install and configure Snort on Ubuntu on a VM
- Snort is one of the best / most used tool for Intrusion Detection System



Source Address

Direction

Destination Address

Action

Protocol

Source Port

Destination Port

```
alert icmp 192.168.1.10 any -> any any (msg: “ICMP Attempt Attack”; sid:1000005)
```

Rule Header

Rule Option

Source

- https://tools.kali.org/
- https://www.hitachi-systems-security.com/blog/penetration-testing-vs-vulnerability-assessment/
- https://linuxhint.com/configure-snort-ids-create-rules/
- https://www.google.com/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwim6KWokavmAhVFr4sKHT3RDLAQjhx6BAgBEAI&url=https%3A%2F%2Fwww.researchgate.net%2Ffigure%2FExample-of-Snort-IDS-Rule-The-rule-options-of-Snort-consist-of-two-parts-a-keyword-and_fig1_281564631&psig=AOvVaw2OqjdKmpvx6ONCHLbMnVtj&ust=1576069021539993