COURSE: SECURITY+ SY0-401

MODULE 3: THREATS AND VULNERABILITIES

Part B

Overview

- Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities

- Explain the proper use of penetration testing versus vulnerability scanning

Tools and Techniques to Discover Security Threats and Vulnerabilities

- Assessment types
  - Risk
  - Threat
  - Vulnerability
- Assessment technique
  - Baseline reporting
  - Code review
  - Determine attack surface
  - Review architecture
  - Review designs

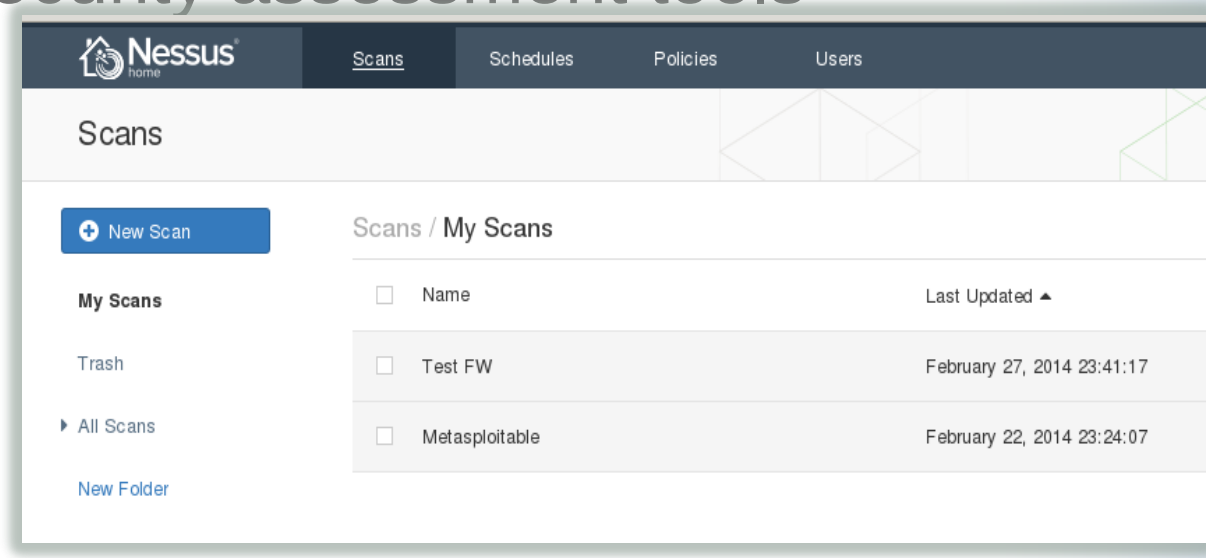
Tools and Techniques to Discover Security Threats and Vulnerabilities

- Risk calculations
  - Threat vs. likelihood

		LIKELIHOOD				
		1	2	3	4	5
IMPACT	1	Low	Low	Medium	Medium	High
	2	Low	Medium	Medium	High	Critical
	3	Medium	Medium	High	Critical	Critical
	4	Medium	High	Critical	Critical	Critical
	5	High	Critical	Critical	Critical	Critical

Tools and Techniques to Discover Security Threats and Vulnerabilities

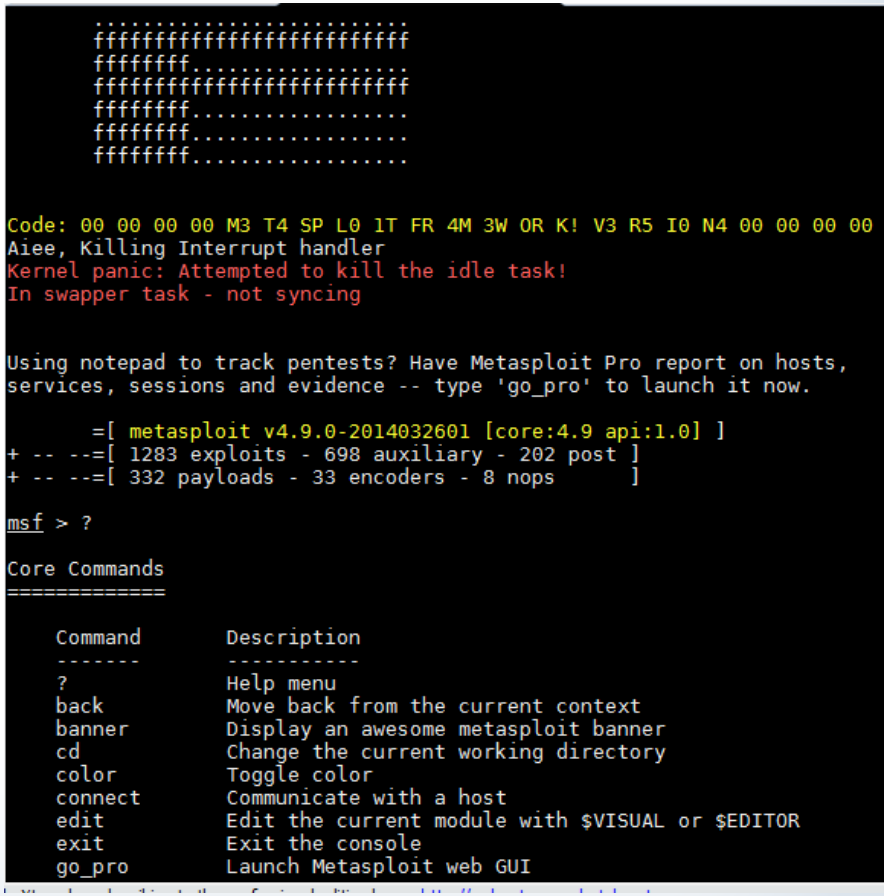
- Interpret results of security assessment tools
- Tools
  - Protocol analyzer
  - Vulnerability scanner
  - Honeypots
  - Honeynets
  - Port scanner
  - Passive vs. active tools
  - Banner grabbing



Penetration Testing versus Vulnerability Scanning

Penetration testing

- Verify a threat exists
- Bypass security controls
- Actively test security controls
- Exploiting vulnerabilities



Penetration Testing versus Vulnerability Scanning

- Vulnerability scanning
  - Passively testing security controls
  - Identify vulnerability
  - Identify lack of security controls
  - Identify common misconfigurations
  - Intrusive vs. non-intrusive
  - Credentialed vs. non-credentialed
  - False positive
- Black box
- White box
- Gray box

Demonstration

Penetration Testing

Vulnerability Scanning

THANK YOU