

COURSE: SECURITY+ SY0-401

MODULE 3: THREATS AND VULNERABILITIES

Part B

- 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

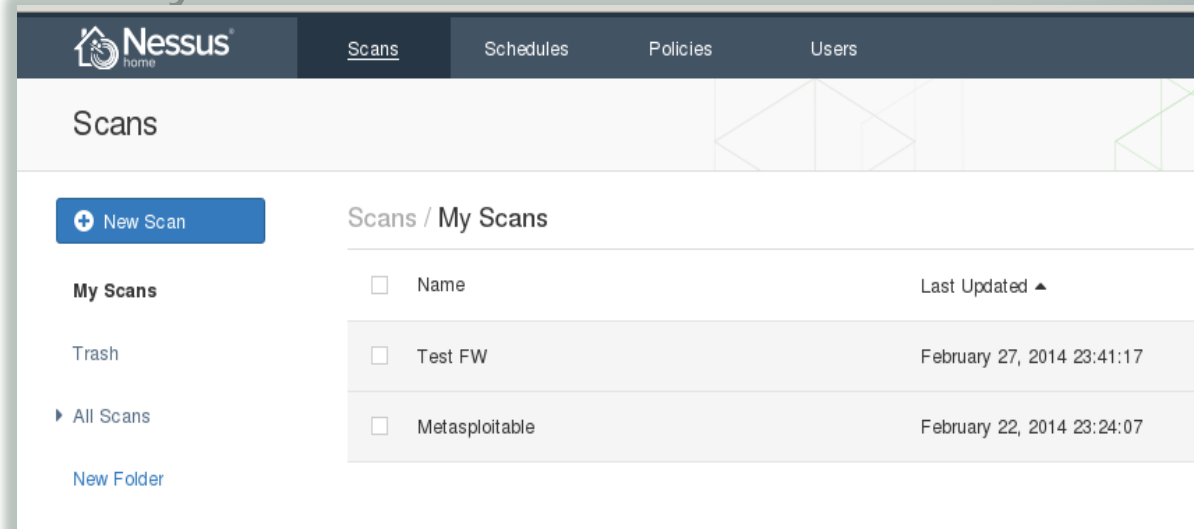
		LIKELIHOOD				
		1	2	3	4	5
I M P A C T	1	Low	Low	Medium	Medium	High
	2	Low	Medium	Medium	High	Critical
	3	Medium	Medium	High	Critical	Critical
	4	Medium	High	Critical	Critical	Critical
	5	High	Critical	Critical	Critical	Critical

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

```
ffffffffffffffffffffffffffff
fffffffff
ffffffffffffffffffffffffffff
fffffffff.....
fffffffff.....
fffffffff.....

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N4 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

Using notepad to track pentests? Have Metasploit Pro report on hosts,
services, sessions and evidence -- type 'go_pro' to launch it now.

      =[ metasploit v4.9.0-2014032601 [core:4.9 api:1.0] ]
+ -- --=[ 1283 exploits - 698 auxiliary - 202 post ]
+ -- --=[ 332 payloads - 33 encoders - 8 nops      ]

msf > ?

Core Commands
=====

Command      Description
-----
?            Help menu
back         Move back from the current context
banner       Display an awesome metasploit banner
cd           Change the current working directory
color        Toggle color
connect      Communicate with a host
edit         Edit the current module with $VISUAL or $EDITOR
exit         Exit the console
go_pro       Launch Metasploit web GUI
```



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
