



Using Security Tools



Information Assurance and Network Security

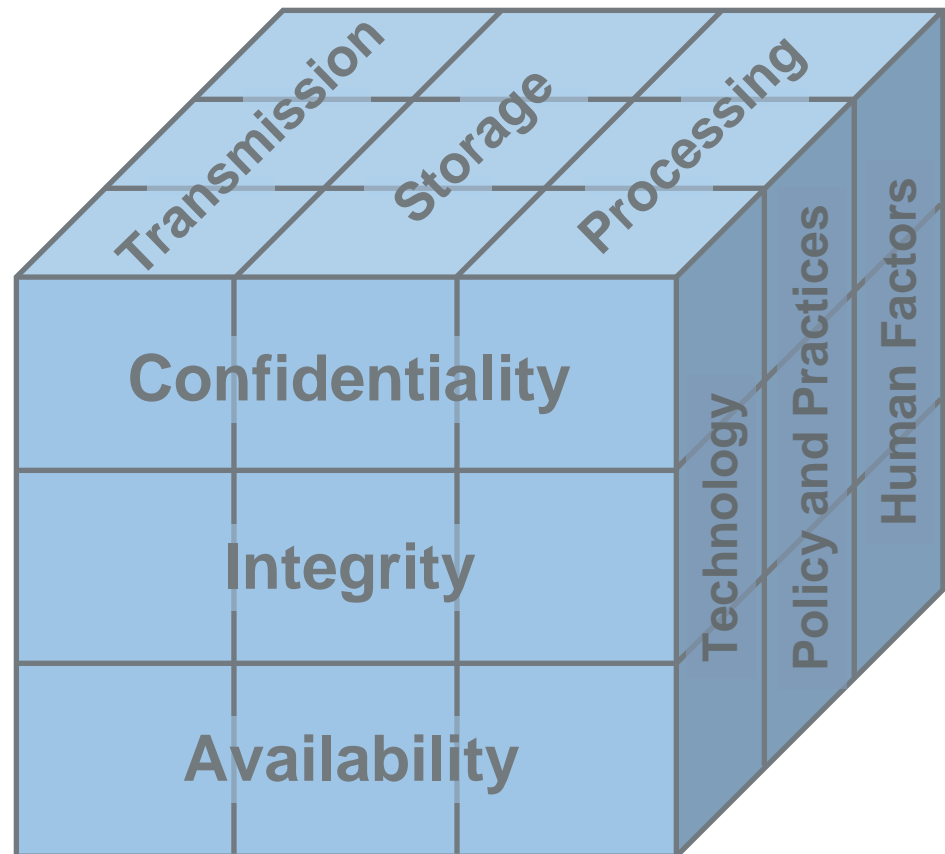
John Sands and Erich Spengler

Cisco | Networking Academy®
Mind Wide Open™

Overview of Information Assurance and Network Security

Foundations

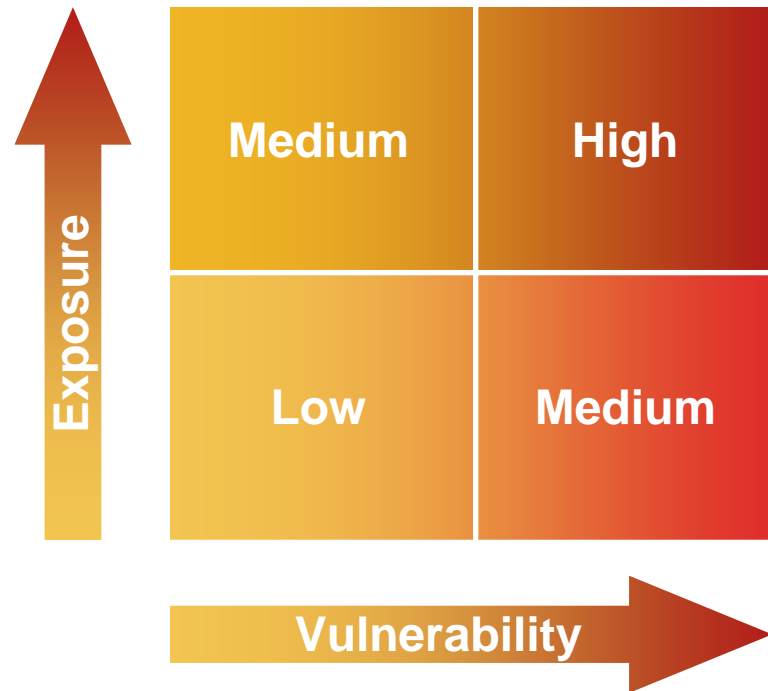
1. Confidentiality
2. Data Integrity
3. System Availability



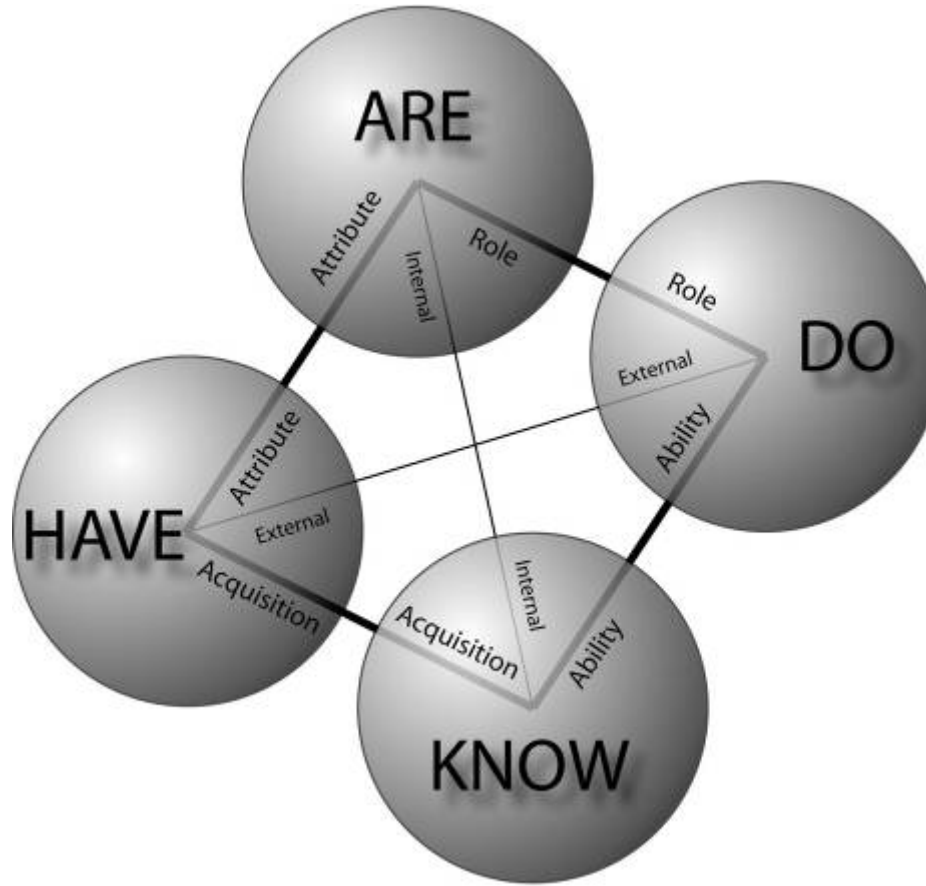
Terms to Review

1. Vulnerability
2. Threat
3. Risk
4. Countermeasure
5. Authentication
6. Non-repudiation

Risk: With Known Threats, Risk Becomes Proportional to the Amount of Exposure to Any Vulnerability



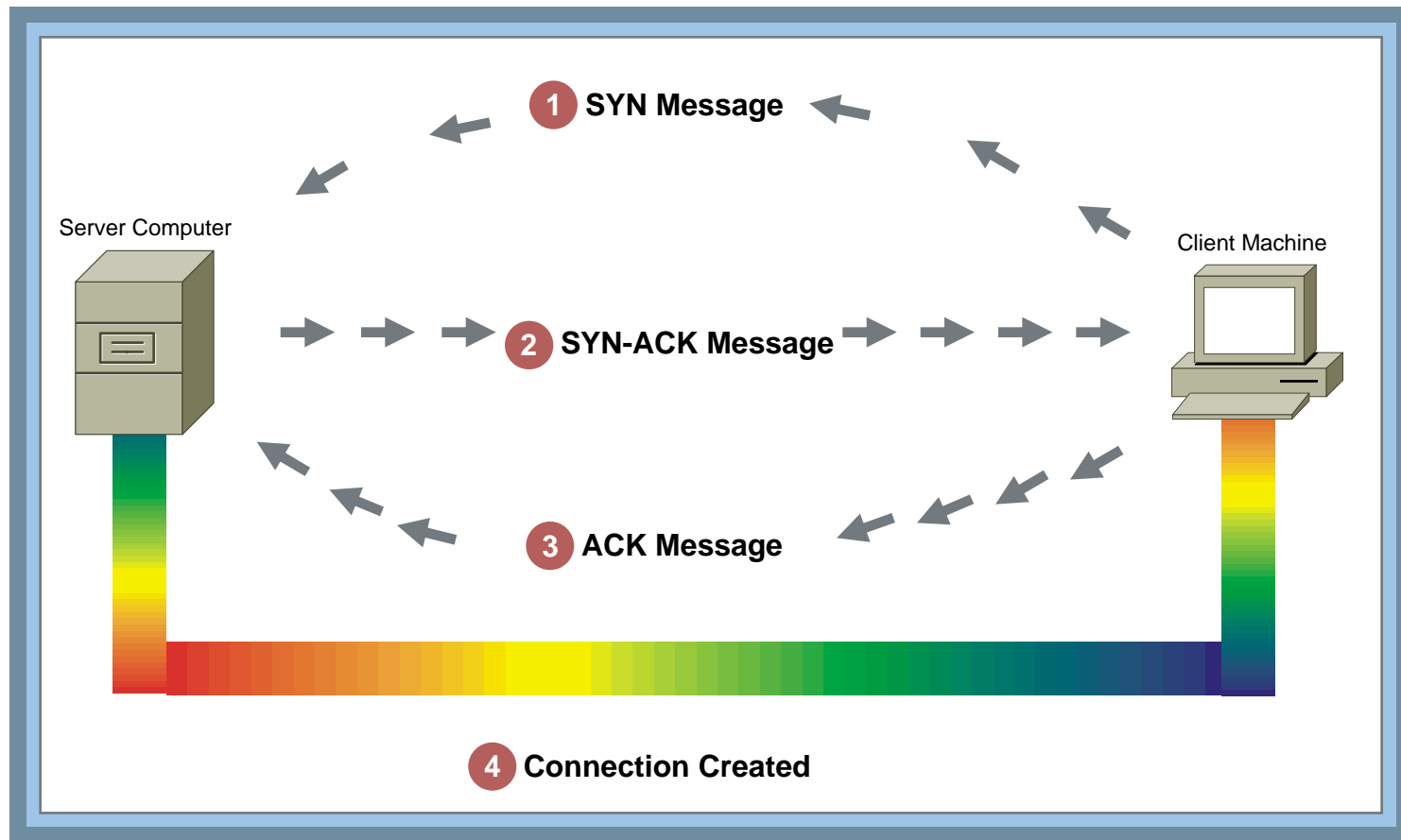
Authentication



Using a Keyboard Logger



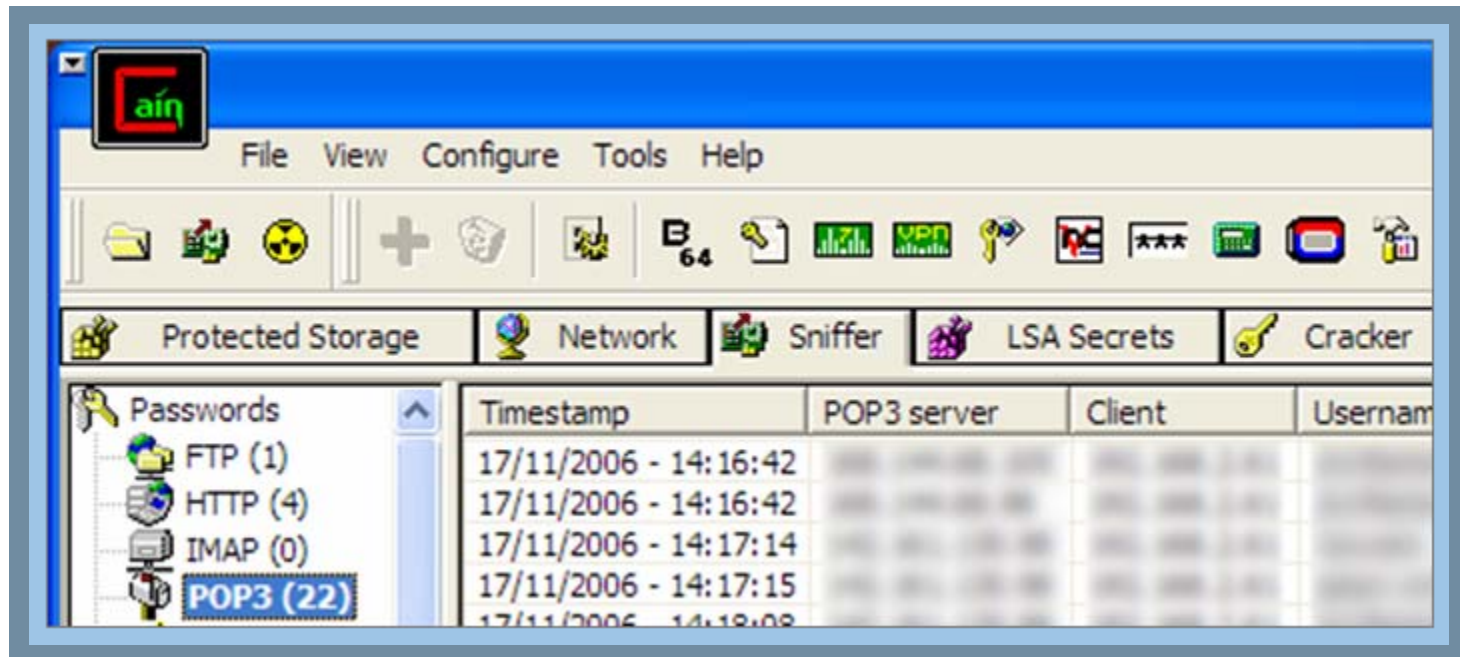
Using Syn Attack



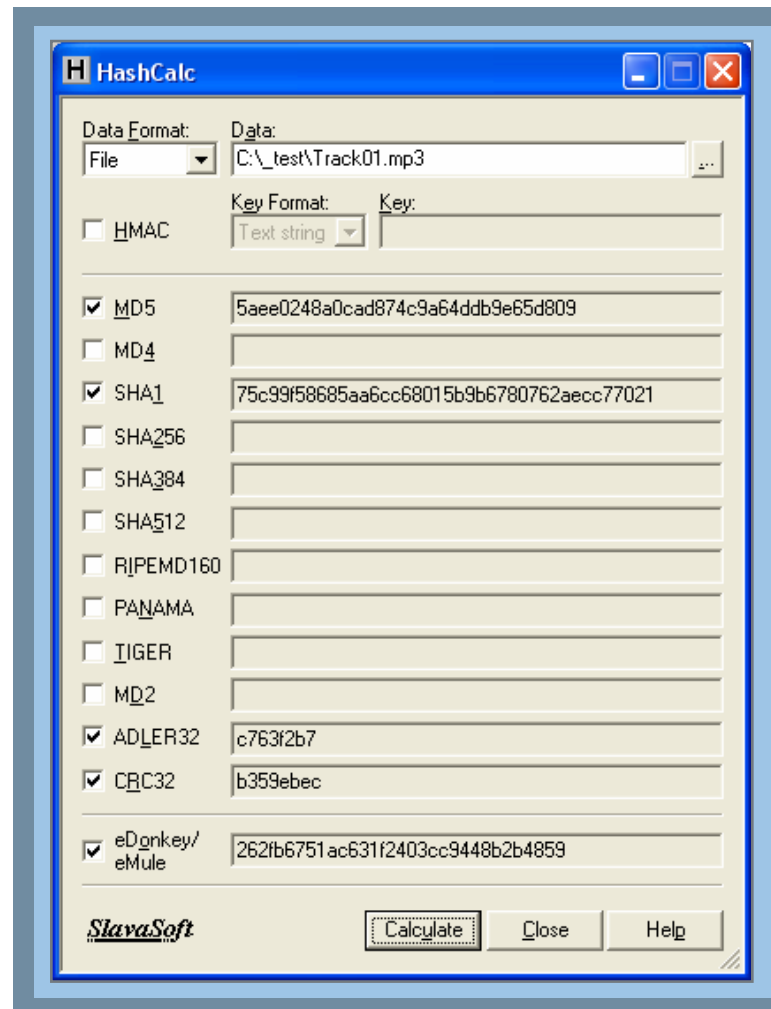
Using AngerIP Network Scanner



Using Cain and Able



Using HashCalc



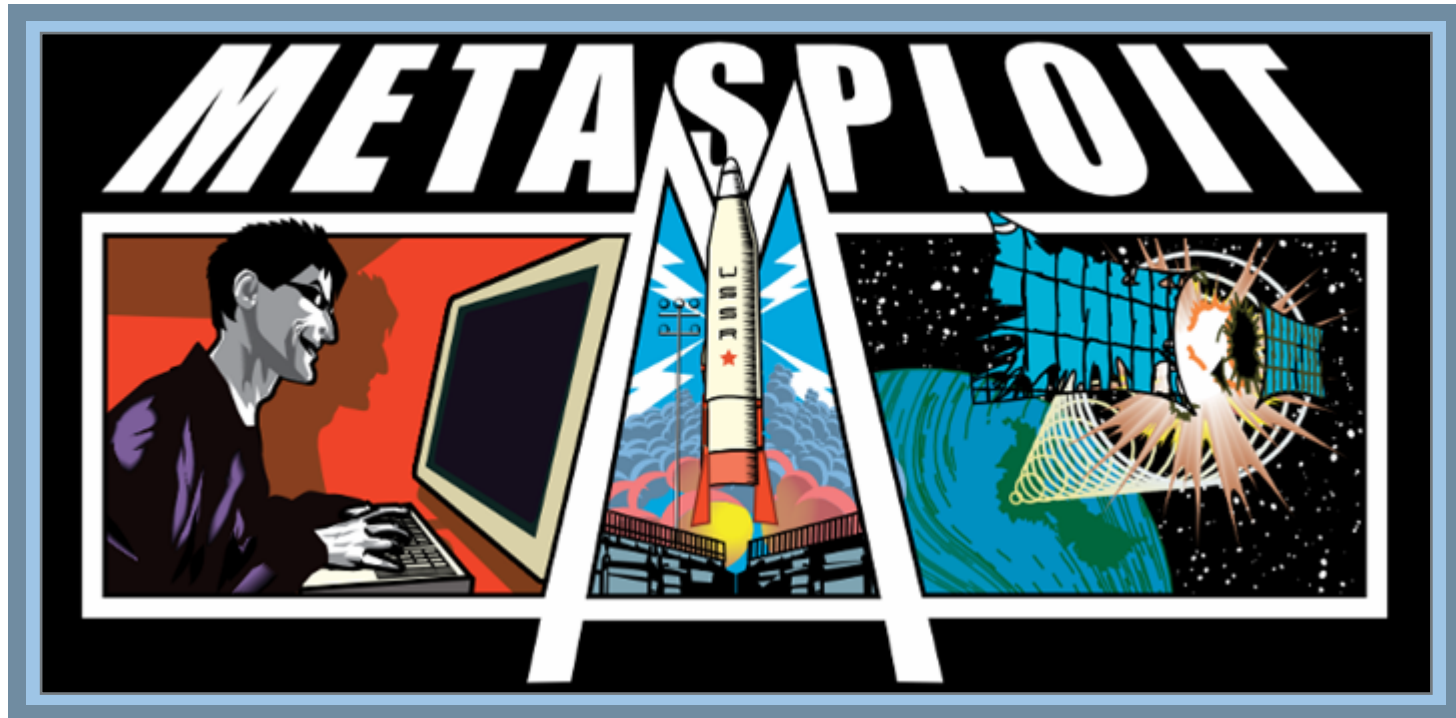
Using NetCat



Nessus Scan



Using MetaSploit



Using Bandwidth Limiter

The screenshot displays the Mikrotik WinBox interface. The top window shows the configuration for the 'bandwidth limiter' service, with a table of bandwidth limits for various connections.

Connection	Incoming		Outgoing	
	Speed	Limit	Speed	Limit
ETHER1	10.01	5.00		5.00
Internet Explorer	10.01	10.00		5.00
Process (3844)	10.01	5.00		5.00
127.0.0.1:1288	0.00	5.00	0.00	5.00
192.168.100.10:80	10.01	5.00		5.00
Generalized Process for WinBox		5.00		5.00
Yahoo Messenger		5.00		5.00
system		5.00		5.00
WinBox 2 service		5.00		5.00
USA Shell (Expert Version)		10.00		5.00
Skype.exe		5.00		5.00
Application Layer Delivery Ser.		5.00		5.00
WinBox Client		5.00		5.00
MyWinView		5.00		5.00

The bottom window, titled 'Zabbix View', shows traffic monitoring data:

Flow	Received	Sent
My Computer	4,822	4,822
Local Network	30.7	39.1
Internet	31,800,430	30,803
Public		

Two traffic graphs are visible, showing data over time. The top graph shows a peak in traffic, and the bottom graph shows a more sustained flow.

Using Net Stumbler

The screenshot shows the Network Stumbler application window titled "Network Stumbler - [20021206125750.ns1]". The interface includes a menu bar (File, Edit, View, Device, Window, Help), a toolbar with various icons, and a main display area. On the left, there is a tree view with categories: Channels (1, 3, 6, 11), SSIDs (101, HeideofTegaCay, linksys, tburnslaptop), and Filters (Encryption Off, Encryption On, ESS (AP), IBSS (Peer), CF Pollable, Short Preamble, Default SSID). The main display area shows a table of detected wireless networks.

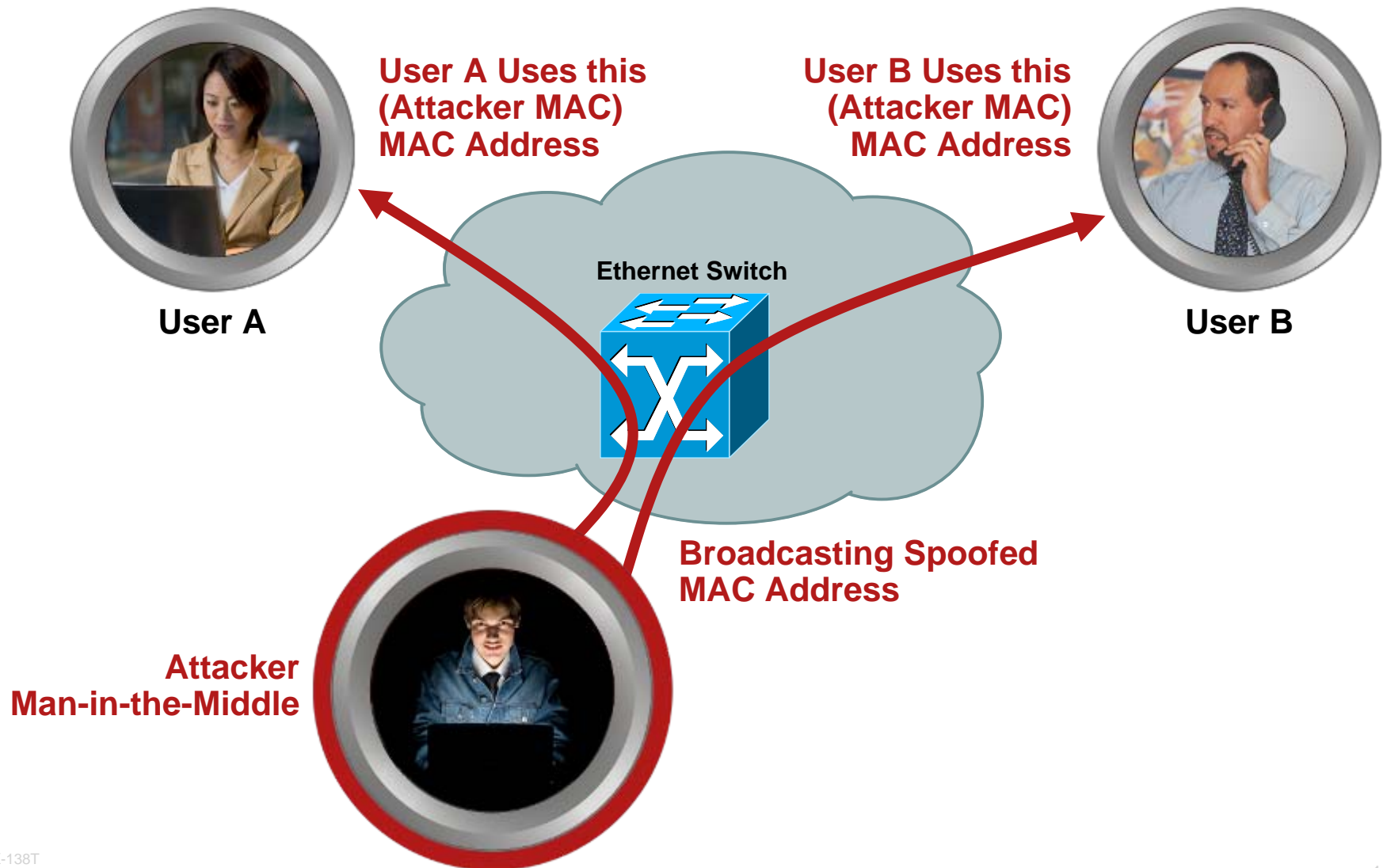
MAC	SSID	Ch...	Vendor	Ty...
000124F08C...	HeideofTegaCay	11	Acer	AP
00045A0C5338	linksys	6	Linksys	AP
0030AB1F74...	tburnslaptop	1	Delta (...)	AP
008048E4BC...	101	3		AP

At the bottom of the window, the status bar shows "Ready", "1 AP active", and "GPS: Disabled".

Using Microsoft Baseline Security Analyzer



Using XARP



For More Information About CSSIA

- CSSIA.ORG
- ftp://64.107.8.176/_Information%20Assurance%20I/IA%20Labs%20and%20Tools%202006/IA-I_V2/
- sands@morainevalley.edu
- spengler@morainevalley.edu

Q and A



Cisco | Networking Academy[®]

Mind Wide Open[™]



CISCO