

## Principles of Cyber Security

Lecture 13: Vulnerability Scanning





#### **Objectives**

**10.1** To describe the Vulnerability Scanning and Data Management Tools.





### **Vulnerability Scanning**

- Vulnerability scanning in some ways complements
  - pen testing
- Studying vulnerability scanning involves
  - understanding:
  - What it is
  - How to conduct a scan
  - How to use data management tools
  - How threat hunting can enhance scanning



#### **Conducting a Vulnerability Scan**

 A penetration test is a single event using a manual process often performed only after a specific amount of time has passed.

• A vulnerability scan is a frequent and ongoing process that continuously identifies vulnerabilities and monitors cybersecurity progress.



#### **Conducting a Vulnerability Scan**

- Conducting a vulnerability scan involves:
  - Knowing what to scan and how often
  - Selecting a type of scan
  - Interpreting vulnerability information
- When and What to Scan
  - Two primary reasons for not conducting around-the-clock vulnerability scans:
    - Workflow interruptions
    - Technical constraints
  - A more focused approach is to know the location of data so that specific systems with high-value data can be scanned more frequently



#### **Conducting a Vulnerability Scan**

O/EC270	000: Asse	t Manager	nent									Bwitch Dashboard	• • 0;	tions +
CSF - Top Opending Systems					Discovery Scan - Horlis Par Assat Lat				CSF - Software Applications and Database Servers					
<ul> <li>Biolitana Mary In Barry To Hannes (B)</li> <li>Biolitana Mary In Hannes (B)</li> <li>Biolitan</li></ul>			Asset			Total	Actobe Acrobe			DB2 Barver				
			Gysta vis that ha	ve been Scanse	d (	710	Adaba Photosh MS Office		1	MySQL Server	15			
			Systems Seimned Within Last 90 Days			210	MS Office 38		0 De	aie Database Servor	8			
			Systems Scanned Wilhim Last 7 Days				MS Office for M	80	U	MB BQL Berver	15			
			Sustains General Within Last 10 Days 181				Last Optime: 12 minutes ago							
			About a strong and on the strong stro				ABD Top 4 Mitigation Bivatigies - List of Bothware							
				Systems Scattood Ter Compliance in Bard 60 Days 558				1210			0	Part of the local division of the		
Manage Party					Bad Credentain			487	Nare .			CON	Outpools M	4900
Last Updated 8 minutes ago					Exploration (Denand)				1bids-1.16-2.48	(mark)		191	Active	
Network Mapping - Braindown of Daviosa Detected on Network					SSE. or TLS Sorvers 445				Isososystem 10.0-4.4HB/weed			120	Active	
Posters Evelstes Franklis			Leel Updated 9 minutes ago											
Pinina Wata Ital			Host Discovery - Hosts Per Class C			checkpolicy-0.032-1.4 (5)hone			125	Active				
Making Desirem Happeneters SCHOA Sectors														
art brand *2 made on				IP Address Total			rota	diffed to-2.3.1-28.arX(yerw)			125	Active		
or opening it. I make the				172.94.04.0594			226							
kan Shiff and Log - Coverage				172.26.25.0524			205	and the set of the set			115	Active		
Total Syste	tal Systems 3437			170.58.29.0494			238	gamin-0.1.10-0.a/E(\$1014)			125	Active		
Ecanned Systems 1488		200 M (0 100)			174									
Sniffed Systems 1923 42 6			14				Last Updated: Less than a minute ego							
Copped Systems				172,36.22,024 130				CRE. How constant there are						
al Upsaties 12 mil	ston of				Last Updated : 9 m	rutes ago			0.000		•			
CHEC2/000 - Mo	telis Devices				Network Mapping	- Hanta Not O	perrord in Last 7 Days		Physic ID	Namé		Family	Security	
	Davicon.	Mark en Viene	High Volta	Disting Water	IP Address	NERCE	DNR	MAC Access	33850	Unsupport	ed Unix Operating Syste	en Ganeral	Orlical	65
Scanned .	0	0.	0	0									_	
Managed			- A.		112.99.0.5				2024	Mancoof) In Version Dat	nforrest Explores Uneaso locition	parted Weidowe	Ortical	
asl Upsatini. 12 minutes ago				122.26.0.8				77754	Married 1	NT Demande Line of	unter Warber	Contract of	-	
CSF - Wireless Access Daviors					179.26.0.21		retainvices Lists .						and the second	
1984P Down! New WAP Last 7 Days					172.20.0.20		lab-Res-501/ids		62750	Marceoft A	ML Parser (MEDML) an	d Windows	Orlivel	17
		100	Novi	×	172,24.0.63		idron-s520.000.10			MELCOR!	version or supported		-	
					Loci Decistat: 8 m	0.430.300			84720	Marcoult	Weeksen Rover 2023	Windows	Ortical	74



Figure 2-5 Nessus software asset management



Figure 2-4 Nessus hardware asset management

#### **Data Management Tools**

- Two data management tools are used for collecting and analyzing vulnerability scan data:
  - Security Information and Event Management (SIEM)
  - Security Orchestration, Automation, and Response (SOAR)
- Security Information and Event Management (SIEM)



#### **Data Management Tools**



#### Figure 2-8 SIEM dashboard



#### Summary

 Two data management tools are used for collecting and analyzing data: the Security Information and Event Management (SIEM) tool and a Security Orchestration, Automation, and Response (SOAR) tool.





# Thank you

