UWAGA!!! W ramach ćwiczenia są wymagane loginy-hasła dostępu do Kali Linux OS, SSH, OpenVas, IP-adresy skanowanych narzędzi. Ta informacja będzie uzyskana od prowadzącego podczas zajęć.

Skaner podatności OpenVas pozwala na automatyzowaną ocenę podatności (vulnerability assessment) i zarządzanie podatnościami (vulnerability management). OpenVas działa w sposób podobny do działania cyberprzestępcy, co pozwala wykrywać łuki w systemach bezpieczeństwa przed momentem ich wykorzystania przez hackiera.

System pozwala na wykrycie podatności w dwóch generalnych trybach:

- Skanowanie z uwierzytelnianiem
- Skanowanie bez uwierzytelniania

Skanowanie bez uwierzytelniania pozwala na wykrycie hostów w sieci i podatności uruchomionych usług sieciowych.

Skanowanie z uwierzytelnianiem z kolei pozwala sprawdzić wewnętrzną konfigurację hostów i wykrywać podatności w aplikacjach i oprogramowaniu, które nie zostały uruchomione przez administratora hosta.

Generalnie, System OpenVas zawiera:

- Bazy danych
- Klientci
 - OpenVas CLI
 - Greenbone Security Assistant
- Serwisy:
 - OpenVas Scanner
 - OpenVas Manager

W **Bazach danych** są umieszczone testy podatności oraz dane użytkowników i służbowa informacja (wyniki testów, zaplanowane testy, parametry hostów (celi) do skanowania, loginy i t.d.)

OpenVas CLI pozwala zarządzać systemem poprzez złożenie komand w wierszu polecenia (terminału)

Greenbone Security Assistant pozwala zarządzać systemem za pomocą interfejsu webowego

OpenVas Scanner skanuje celi OpenVas Manager na podstawie poleceń przekazanych administratorem poprzez (OpenVas CLI lub Greenbone Security Assistant) zarządza pozostałymi elementami systemu. Organizuje współpracę pomiędzy elementami systemu.

Celi ćwiczenia:

- 1. Zapoznać się z interfejsem OpenVas;
- 2. Nauczyć się konfigurować listy portów dla skanowania;
- 3. Nauczyć się konfigurować parametry celi i skanowania;
- 4. Nauczyć się planować zadania dla OpenVas;
- 5. Zobaczyć różnicę pomiędzy skanowaniem z uwierzytelnianiem i bez uwierzytelnianiem;
- 6. Sprawdzić podatność rzeczywistych systemów (dostępnych w laboratorium 204) za pomocą OpenVas.

Laboratorium odbędzie się w grupach dwuosobowych. Stanowisko laboratoryjne zawiera 2 komputery i 1 przełącznik Cisco.

Jeden komputer i Cisco są wykorzystane dla testów. Drugi komputer będzie spełniał funkcję skanera podatności.

Uruchom OpenVas # openvas-start

Uruchom przeglądarkę internetową i połącz się z portem 9392 na 127.0.0.1 Wpisz nazwę użytkownika i hasło, następnie zaloguj się.



Sprawdź aktualność baz danych. "Extras" -> "Feed Status"

Application	s ▼ Places ▼	😫 Firefox ESR 🕶		Thu 12	:43 •		, #	1 🖌	シロ・
				Greenbone Security Assis	tant - Mozilla Fire	efox		•	• •
i Greenbo	one Security Assis 🗙	: +							
$(\leftrightarrow) \rightarrow c$	÷ ۵	i 🔒 https://127.0.0.1	:9392/omp?cm	d=get_feeds&token=4f6a99	d0-cb1e-4 04	🛡 🏠 🔍 Search		<u>↓</u> III\	▣ ≡
A Most Vis	ited 🛐 Offensive	Security 🥆 Kali Linux	🔨 Kali Docs 📍	🕻 Kali Tools 🛭 🍋 Exploit-DB	📡 Aircrack-ng	🔧 Kali Forums 🔌 NetHunt	er 🛛 👌 Getting Starte	ed	
Gree Secu	enbone urity Assistant					Refresh every 30 Se	ec. 🔻 Logged in a Thu M	s Admin admin Mar 28 17:43:22 2	Logout 019 UTC
Das	hboard	Scans	Assets	SecInfo	Configuration	Extras	Administration	Help	
?									
F e	ed Status								
Туре	Content				Origin		Version	Status	
NVT					Greenbone Comm	unity Feed	201903281128	Current	
SCAP	🥵 CVES, 🚟 CPES	, OVAL Definitions			OpenVAS SCAP Fee	ed	201903280000	Current	
CERT	CERT-Bund Advi	sories, 😬 DFN-CERT Adv	isories		OpenVAS CERT Fee	ed	201903280100	Current	
Backend operati	on: 0.13s				Greenbone	Security Assistant (GSA) Copyright 200	9 - 2018 by Greenbone Netv	works GmbH, www.gre	enbone.net

OpenVas skanuje celi na podstawie znanych list portów sieciowych. Zobacz które listy są dostępne: "Configurations" -> "Port Lists"

Applications \bullet	Places 🔻	🌖 Firefox ESR 🔻		Thu 11	:59 •)**	1	∎)) (°) •
				Greenbone Security Assis	tant - Mozilla Firefox					• •	8
ightarrow Greenbone Sector	urity Assis 🗙	+									
(←) → C' @		(i) 🔏 https://127.0.	0.1:9392/omp?cm	d=get_port_lists&token=3e	53e190-4f9e-4f30	♥ ☆	Q Search		li	\ 🗉	≡
A Most Visited	Offensive	Security 🥆 Kali Linu	ıx 🌂 Kali Docs 🖞	🔪 Kali Tools 🛭 🧟 Exploit-DB	📡 Aircrack-ng 🏾 🌂 Ka	ali Forums 📍	NetHunter	Getting Starte	d		
Greenbo Security A	ne ssistant					Refresh	every 30 Sec.	 Logged in as Thu M 	Admin admi ar 28 16:59:34	n Log 2019 l	out JTC
Dashboard		Scans	Assets	SecInfo	Configuration	Extras	,	Administration	Hei	Þ	
2 🗙 🕇				Filter:						3	•
Port L	ists (10) of 10)									
									K k 1 - 10	of 10 💽	
Name						Port Counts	s		Acti	ons	
						Total	TCP	UDP			
All IANA assigned	TCP 2012-0	2-10			<u> </u>	5625	5625	0			
All IANA assigned	TCP and U	DP 2012-02-10			<u></u>	10988	5625	5363			
All privileged TCF	•				<u> </u>	1023	1023	0			
All privileged TCF	P and UDP				<u> </u>	2046	1023	1023			
All TCP					<u> </u>	65535	65535	0			
All TCP and Nmap	5.51 top 10	00 UDP			6 0	65634	65535	99	à.	″ 🖸 ↓	
All TCP and Nmap	5.51 top 10	000 UDP			<u></u> ₩	66534	65535	999	ì.	∠ 🖸 🖡	
Nmap 5.51 top 20	000 TCP and	top 100 UDP			6 0	2098	1999	99	ì d	2 🔁 🖡	
OpenVAS Default					₩	4481	4481	0	à.	2 🖸 🗜	
TCP dla Cisco						444	444	0	à,	2 🖸 🕸	
								VApply to	page contents 💌		
(Applied filter: rows=10 f	irst=1 sort=nam	ie)							K 🧲 1 - 10	of 10 💽	

Backend operation: 0.02s

Greenbone Security Assistant (GSA) Copyright 2009 - 2018 by Greenbone Networks GmbH, www.greenbone.net

W ramach ćwiczenia będziemy skanowali przełącznik Cisco, komputery pod zarządzaniem OS Windows oraz Ubuntu Linux. Dla tych celów będziemy korzystać z listy "All privileged TCP" oraz właśnie założonej listy.

Sklonuj dowolną listą protów sieciowych (przycisk \Box) i skonfiguruj ją (przycisk Z) w następny sposób:

nazwa: "TCP dla Cisco". Porty: TCP od 1 do 444.

Dla skanowania z uwierzytelnianiem OpenVas korzysta z dostępnych profili logowania. Sprawdź dostępne profili logowania:

"Configurations" -> "Credentials"

Applications $\overline{}$	Places 🔻	🍯 Firefox ESR 🕶		Thu 12:	• 00				1	(1) کر) ()	•
			Green	bone Security Assis	tant - Mozilla Fire	efox				•	Θ	8
ightarrow Greenbone Se	curity Assis 🗙	+										
↔ → ♂ ŵ		1 Attps://127.0.0.1	l:9392/omp?cmd=get_ci	redentials&token=3e	e 53e190-4f9 e-4f	···· 🛡 🏠	ि Q Search			111	1	≡
A Most Visited	Offensive	Security 🌂 Kali Linux	🔪 Kali Docs 🌂 Kali To	ools 🔅 Exploit-DB	📡 Aircrack-ng	🌂 Kali Forums	🔪 NetHunter	🥑 Getting Started	ł			
Greenberg Security	one Assistant					Refresh	n every 30 Sec.	 Logged in as Thu Ma 	Admin a ar 28 17:	admin 00:29 20	Logou 19 UT	ut rc
Dashboard		Scans	Assets	SecInfo	Configuration	Extras		Administration		Help		
? \star			Filter: rows=10	first=1 sort=name				SX?~			- *	0
	entials (1 of 1)										
									K	1 - 1 of	1	2
Name	Туре	3		Allow insec	ure use		Log	in	Actions			
ubuntu	up (us	sername + password)		No			stud	lent	di 🖌 🖸	1		
								VApply to p	age conter	ts 🔻	61	
(Applied filter: rows=10	first=1 sort=nam	ne)								1 - 1 of	1	2
Backend operation: 0.02	S				Greenbone	Security Assistant (GSA) Copyright 2009 - 2	2018 by Greenbone Netwo	orks GmbH,	www.gree	nbone.r	net

Załóż nowy profil: Nazwa: Ubuntu. Obejrzyj Celi do skanowania OpenVas: "Configurations" ->"Targets"

Applications -	Places 🔻	🕑 Firefox ESR 🔻			Thu 12:00) •)	(ا م مر) 🕛 🔻
				Greenbon	e Security Assistar	nt - Mozilla Firefox			•	• •
ightarrow Greenbone Sec	curity Assis ×	< +								
(←) → C'		🛈 🐔 https://127.	0.0.1 :939	2/omp?cmd=get_targe	ts&token=3e53e19	0-4f9e-4f30-b	🛡 🏠 🔍 Search	1	lii\	▣ =
A Most Visited	Offensive	Security 🌂 Kali Li	nux 🌂 I	Kali Docs 🥆 Kali Tools	🍥 Exploit-DB	🖹 Aircrack-ng i 🔨 Ka	ali Forums 🥆 NetHunter	🥑 Getting Started		
Security /	o ne Assistant						Refresh every 30 Sec.	 Logged in as Admi Thu Mar 28 	n admin 17:00:43 20	Logout 19 UTC
Dashboard		Scans	Ass	ets Sec	cinfo	Configuration	Extras	Administration	Help	
? 🗙				Filter:				88?2		
Targe	ts (3 of	3)							a e 1 - 3 of	3
Name	н	losts	IPs	Port List	Crede	ntials - sort by: SSH	 N [2] 		Actions	5
Cisco	1	0.2.60.7	1	TCP dla Cisco					🛅 📶	
sosiad	1	0.1.1.14	1	All privileged TCP					🛅 🗾	
sosiad+SSH	1	0.1.1.14	1	All privileged TCP	SSH:	ubuntu			🛅 📶 🕻	
								VApply to page co	ntents 💌	1
(Applied filter: rows=10	first=1 sort=nan	ne)						1	🚺 🚺 1 - 3 of 1	3
Backend operation: 0.01	5					Greenbone Security	y Assistant (GSA) Copyright 2009 -	2018 by Greenbone Networks Gr	ıbH, www.gree	nbone.net

Załóż nowe celi:

- + Nazwa "sosiad" Port List: "All privileged TCP"
- + Nazwa "sosiad+SSH" Port List: "All privileged TCP" Credentials for authenticated checks: SSH: ubuntu
- + Nazwa "Cisco" Port List: "TCP dla Cisco"

Obejrzyj dostępne konfiguracji testów: "Configurations" \rightarrow "Scan Configs"

Applications - Pla	aces 🔻 🤨 Firefox ESR 🝷	♦ Firefox ESR Thu 11:02 •) ()	•
			Greenbone Security Ass	istant - Mozilla Firefox						0	•	⊗
ightarrow Greenbone Security	y Assis 🗙 🕂											
(←) → 健 @	🛈 윮 https://127.0.0	.1:9392/omp?cmd	=get_configs&token=3e5	3e190-4f9e-4f30-b	♥ ☆	Q Sear	ch			lii\	•	≡
A Most Visited 🚺 Of	ffensive Security 🥆 Kali Linux	🔨 Kali Docs 🌂	Kali Tools 🧆 Exploit-D	B 🐚 Aircrack-ng 🌂 I	Kali Forums 🦄	NetHunt	er ۏ G	etting Start	ed			
Greenbone Security Assi	istant				No auto-r	efresh	Ŧ	Logged in a Thu l	s Admi Mar 28 1	n admin 16:02:37 20	Logou 19 UT	rt î
Dashboard	Scans	Assets	SecInfo	Configuration	Extras		Admir	histration		Help		
2 🗙 🚹			Filter: rows=10 first=1 sort=name				SX	? 🖌 📃		×	- *)
Scan Co	nfigs (8 of 8)											
									0	🕻 🔚 1 - 8 of	8 💽 💽	3
Name						Familio Total	es Trend	NVTs Total	frend	Actions		
Discovery (Network Discovery sca	n configuration.)				6	20		2721		à 🖍 💁	3	
empty (Empty and static confi	iguration template.)				6	o 🗟	-	0	•	à / <mark>-</mark>		
Full and fast (Most NVT's; optimized	by using previously collected info	rmation.)			6	62		49689		à / 💁	3	
Full and fast ultimate (Most NVT's including th	e hose that can stop services/hosts	; optimized by using	previously collected inform	ation.)	G	62	2	49689	2	à / 💁		
Full and very deep (Most NVT's; don't trust	previously collected information;	slow.)			6	62		49689		à / 💁	3	
Full and very deep ul (Most NVT's including th	ltimate hose that can stop services/hosts	; don't trust previou:	sly collected information; slo	ow.)	6	62		49689		à 🖊 💁		
Host Discovery (Network Host Discover	y scan configuration.)				6	2		2		à / 💁	3	
System Discovery (Network System Disco	very scan configuration.)				đ	6	-	29	-	à 🖍 👴		
								√Apply to	page co	ntents 🔻	D	
(Applied filter: rows=10 first=	1 sort=name)								0	🕻 🗲 1 - 8 of	8 💽 🖸	1
Backend operation: 0.01s				Greenbone Securi	ity Assistant (GSA) Co	opyright 200	9 - 2018 by	Greenbone Net	works Gm	ibH, www.gree	nbone.n	et

W ramach ćwiczenia będziemy korzystać ze zmienionej listy "Full and fast ultimate".

Sklonuj listą "Full and fast ultimate" i skonfiguruj ją w następny sposób: *nazwa:* "*lab204*". *safe_checks = yes*

Opcja "safe_checks = yes" blokuje możliwość wykorzystanie niebezpiecznych testów (testów które mogą doprowadzić do awarii na skanowanym przez OpenVas systemu).

Obejrzyj dostępny zadania OpenVas:

"Configurations"	$' \rightarrow$ "Tasks"					
Applications Places	🍪 Firefox ESR 🔻		Thu 12:01 •		, ;;	◄ ٺ ((ا) محم
		Greenbor	ne Security Assistant - Mozilla F	refox		•••
ightarrow Greenbone Security Assis >	< +					
	1 https://127.0.0.1:	9392/omp?cmd=get_tasks	&token=3e53e190-4f9e-4f30-	ost 🚥 🔽 🛧 Searc	h	
A Most Visited Offensive	Security 🛰 Kali Linux	🕻 Kali Docs 🌂 Kali Tools	🔅 Exploit-DB 🐚 Aircrack-n	n 🍾 Kali Forums 🌂 NetHunte	r 👶 Getting Started	
Greenbone Security Assistant	•	•	~	Refresh every 30 Sec	Logged in as Adr Thu Mar 28	min admin Logout [^] 8 17:00:59 2019 UTC
Dashboard	Scans	Assets Se	cInfo Configuration	Extras	Administration	Help
? 📉 🖈		Filter: min_qod=70 a	pply_overrides=1 rows=10 first=1 sort=na	me	SX?~	- -
Tasks (1 of 1)					2
Tasks by Sever	ity Class (Total: 1)	▼ Tasks v	vith most High results per host asks with High severity found		hasks by status (Total: 1)	Done
Name windows10 (Applied filter: min_god=70 apply_overr	Status Done Ides=1 rows=10 first=1 sort=nam	Reports Total 1 (1)	Last Mar 28 2019	Severity 5.0 (Medium)	Trend VApply to page	
Backend operation: 0.01s			Greenbor	e Security Assistant (GSA) Copyright 2009	- 2018 by Greenbone Networks (3mbH, www.greenbone.net

Załóż nowe zadania:

- + Nazwa: "Windows10" Scan Targets: "sosiad" Scan Config: "lab204"
- + Nazwa: "Ubuntu" Scan Targets: "sosiad" Scan Config: "lab204"
- + Nazwa: "Ubuntu+SSH" Scan Targets: "sosiad+SSH" Scan Config: "lab204"
- + Nazwa: "Cisco" Scan Targets: "Cisco" Scan Config: "lab204"

Zarządzanie bezpieczeństwem informacji

Zademonstruj konfigurację prowadzącemu.

Uruchom Windows10 OS na komputerze sosiada. Uruchom zadanie "Windows10".

1) Ile podatności zostało wykryte? 2) ile czasu zajął test?

Uruchom Ubuntu OS na komputerze sosiada. Uruchom zadanie "Ubuntu".

1) Ile podatności zostało wykryte? 2) ile czasu zajął test?

Uruchom zadanie "Ubuntu+SSH".

1) Ile podatności zostało wykryte?
 2) ile czasu zajął test?
 3) jaka jest różnica w porównaniu do testu "Ubuntu"

Uruchom zadanie "Cisco".

1) Ile podatności zostało wykryte?
 2) ile czasu zajął test?

OpenVas analizuje poziom zagrożenia każdej podatności oraz prawdopodobieństwo poprawnego wykrycia (jakość wykrycia) - parametr QoD.

Applications 🗸	Places 🔻	🕑 Firefox ESR 🔻			Thu 12	2:01 •			ž.	1	< •))	Ċ,	-
				Greenbo	ne Security Assi	stant - Mozilla F	irefox				0		8
ight state of the second secon	curity Assis 🗙	: +											
(←) → C ² ⁽¹⁾		1 10 10 https://127.0	.0.1:9392/omp?cmd	=get_repo	ort&report_id=b	e788a5c-fa26-4	d9: 😶 🖸 🏠	Q Search	1		lii\ 🗉		=
A Most Visited	Offensive	Security 🌂 Kali Lin	ux 🌂 Kali Docs 🌂	Kali Tool	s 🔅 Exploit-DI	B 📡 Aircrack-n	g 🌂 Kali Forums	NetHunter	💩 Getting Starte	ed			
Greenberg Security	one Assistant								Logged in a Thu M	s Admin adr Mar 28 17:01::	nin L 13 201	.ogout .9 UTC	^
Dashboard		Scans	Assets	Se	ecinfo	Configuration	Extra		Administration	н	lelp		
Anonymous XN	1L 🔻 IJ 🛀 (9 🔮 🛃 💽 🗖 🗖	one	Filter: autofp=0 app reverse=seve	ly_overrides=1 notes rity levels=hml min_	=1 overrides=1 result god=70	_hosts_only=1 first=1 row	s=100 sort-	SX?/			- *	
Repo	ort: Resi	ults (1 of 12)						ID: be788a5c Modified: Thu Mar 2 Created: Thu Mar 2 Owner: admin	-fa26-4d99-8f03- 28 17:00:51 2019 28 16:58:48 2019	-22d4e9e	ed377d	
										((1	-1 of 1		
Vulnerability				e	Severity	C QoD	Host		Lo	ocation	Actio	ns	
DCE/RPC and MSR	PC Services En	numeration Reporting	cult basts only=1 first=1	rows=100 sort	5.0 (Medium)	80%	10.1.1.14 (komp14	4.lab204.local)	13	35/tcp	1 of 1		
(Applied litter.autorp-	o apply_overnues	s=1 holes=1 overhoes=1 re	surt_nosts_ony=111st=1	1003-100 3010	sevency le	veis-nin nin_qou-7	//			^{. ر} اینا اینا	1011		
Backend operation: 0.14	s					Greenbor	ne Security Assistant (GSA	.) Copyright 2009 -	2018 by Greenbone Net	vorks GmbH, ww	w.greent	oone.net	t
Applications -	Places 🔻	Firefox ESR •			Thu 1	2:01 •)**	1	√ •))	Ċ	~
		_		Greenbo	one Security Ass	istant - Mozilla F	irefox				•	•	8
ightarrow Greenbone Se	curity Assis >	< +											

Steenbolle Security ASSIS	^ _ T						
← → ♂ ŵ	🛈 🐔 https://12	27.0.0.1:9392/omp?cmd=	get_result&result_id=	3021d11f-9f01-	🛛 🏠 🔍	Search	II\ © ≡
A Most Visited Most Visited	e Security 🥆 Kali	Linux 🌂 Kali Docs 🌂	Kali Tools 🤵 Exploit	-DB 📡 Aircrack-ng 🌂 I	Kali Forums 🦄 Net	Hunter 🛛 💩 Getting Start	ed
Greenbone Security Assistant						Logged in a Thu	as Admin admin Logout Mar 28 17:01:19 2019 UTC
Dashboard	Scans	Assets	SecInfo	Configuration	Extras	Administration	Help
? 💵 🐺 🖎							
Result: DCE/	RPC and M	ISRPC Services	s Enumeratio	n Reporting		ID: 3021d11 Created: Thu Mar Modified: Thu Mar Owner: admin	f-9f01-42a5-blac-8be42913e470 28 17:00:18 2019 28 17:00:18 2019
Vulnerability			3	Severity	🙆 QoD H	lost Locat	ion Actions
DCE/RPC and MSRPC Services E	numeration Reporti	ing	S	5.0 (M <mark>edium)</mark>	80% 1	0.1.1.14 135/te	:p 🔀 🛸
Summary Distributed Computing Environ	ment / Remote Proc	edure Calls (DCE/RPC) or N	ISRPC services running o	on the remote host can be e	numerated by connec	ting on port 135 and doing) the appropriate queries.
Vulnerability Detection Res	ult						
Here is the list of DCE/RPC	or MSRPC service	es running on this host	via the TCP protocol				
Port: 49664/tcp							
UUID: d95afe70-a6d5-42 Endpoint: ncacn_ip_tcp	59-822e-2c84da1do :10.1.1.14[49664]	db0d, version l]					
Port: 49665/tcp							
UUID: 3a9ef155-691d-44 Endpoint: ncacn_ip_tcp	49-8d05-09ad5703 :10.1.1.14[49665]	1823, version 1]					
UUID: 86d35949-83c9-40 Endpoint: ncacn_ip_tcp	044-b424-db363231 0:10.1.1.14[49665]	fd0c, version 1]					
Port: 49666/tcp							
UUID: f6beaff7-le19-4f Endpoint: ncacn_ip_tcp Annotation: Event log	bb-9f8f-b89e2018 :10.1.1.14[49666] TCPIP	337c, version 1]					

wartość QoD — zależy od sposobu wykrycia:

```
teoretycznie, jest możliwość podatności - (1%)

została wykryta podatna wersja oprogromowania — średni QoD - (80%)

sukcesem zostało skończone wykorzystanie gotowego eksploitu dla wykrytej podatnosci —
```

```
wysoki QoD (100%)
```

Szczegóły sposobu wykrycia podatności są dostępne w "Vulnerability Detection Method" w opisaniu podatności.



OpenVas jest zdolny dla automatycznego uruchomieniu zaplanowanych testów. Obejrzyj zaplanowane testy:

"Configurations" -> "Schedules"

Załóż nowy dowolny zaplanowany test. Załóż nowe dowolne zaplanowane zadanie.

Zademonstruj konfigurację prowadzącemu.

OpenVas pozwala ocenić tendencję zmiany poziomu bezpieczeństwa. Kolumna "Trend" w: "Configurations" \rightarrow "Tasks".

Uruchom znowu test Windows10.

jak się zmienił Trend?
 dlaczego?

Zahamuj OpenVas: # openvas-stop