Istituto Nazionale di Fisica Nucleare

NUcleo CyberSecurity

Test di Greenbone Enterprise TERA

Cristian Greco, *L. G. Carbone, V. Ciaschini, L. Lanzi, S. Stalio, G. Tagliente, A. Tirel*

Workshop sul Calcolo nell'INFN

Loano, 22 - 26 maggio 2023

Partecipanti

- Cristian Greco
- Luca Giovanni Carbone
- Vincenzo Ciaschini
- Leandro Lanzi
- Stefano Stalio
- Gabriele Tagliente
- Alessandro Tirel

Introduzione

Nell'ambito dell'attività del gruppo Scansioni del NUCS (NUcleo CyberSecurity INFN) è stato scelto di mettere a confronto le scansioni di vulnerabilità effettuate con Greenbone Source Edition (opensource) e con Greenbone Enterprise TERA (Proof of Concept)

Configurazioni Greenbone Enterprise

Greenbone Enterprise è disponibile in appliance fisiche, virtuali o servizi cloud:

- Appliances Fisiche, viene fornito hardware e software
- Appliances Virtuali, file OVA da installare in ambiente Microsoft Hyper-V o in VMware vSphere Hypervisor (ESXi)
- Cloud Services, l'infrastruttura e i dati risiedono presso il fornitore del servizio

Configurazioni Greenbone Enterprise

APPLIANCES FISICHE

Greenbone Enterprise è disponibile come **dispositivo fisico** in tre diverse classi, oltre che come sensore.

Soluzioni per PMI
Enterprise 150 | 50 – 500 IP/24h

Soluzioni di fascia media
Enterprise 400 | 300 – 2.200 IP/24h
Enterprise 450 | 500 – 4.000 IP/24h
Enterprise 600 | 500 – 6.000 IP/24h
Enterprise 650 | 1.000 – 10.000 IP/24h

Soluzioni per grandi imprese
Enterprise 5400 | 4.000 – 40.000 IP/24h
Enterprise 6500 | 9.000 – 80.000 IP/24h

Sensore
Enterprise 35 | 20 – 300 IP/24h

APPLIANCES VIRTUALI

Greenbone Enterprise è disponibile come **dispositivo virtuale** in tre diverse classi, oltre che come sensore.

Soluzioni per PMI
Enterprise CENO | 50 – 500 IP/24h

Soluzioni di fascia media
Enterprise DECA | 50 – 1.500 IP/24h
Enterprise TERA | 300 – 3.000 IP/24h
Enterprise PETA | 1.000 – 9.000 IP/24h
Enterprise EXA | 2.000 – 18.000 IP/24h

Sensore
Enterprise 25V | 20 – 300 IP/24h

Cyber Resilience as a Service

La combinazione dell'esclusiva **tecnologia di scansione Greenbone Networks e dei servizi vMSP (Virtual Managed Service Provider).**

GCS è il servizio perfetto per effettuare azioni di Vulnerability Assessment sia per le reti gestite a livello centrale che per gli ambienti distribuiti che richiedono **elevata scalabilità.**

La piattaforma **funziona mediante un semplice gateway virtuale** e può essere configurata in pochi minuti, utilizzando poi i risultati per migliorare la propria **resilienza digitale.**

- ✔ Non necessita di Hardware aggiuntivo
- ✔ Bassi costi operativi
- ✔ Massima flessibilità
- ✔ Continuità del servizio

Configurazioni Greenbone Enterprise

Dell'Appliances Virtuale (versione utilizzata per la POC) esistono diverse tipologie con licenze, caratteristiche e costi diverse ma tutte hanno in comune:

- Nessun limite al numero di sistemi target
- L'abbonamento include Greenbone Enterprise Support, Greenbone Enterprise Feed e aggiornamenti delle funzionalità e GOS
- Sistema operativo Greenbone OS con SSH, GMP, HTTPS
- Web Interface (HTTPS)
- Sistema di backup, restore e snapshot integrato

Versioni di Greenbone Enterprise – Virtual Appliance

Quello che varie nelle diverse tipologie è il numero di "sonde" (slave) utilizzabili, le risorse hardware (virtuale) richieste e la copertura stimata di indirizzi IP in 24 ore.

Le versioni disponibili sono: CENO, DECA, TERA, PETA, EXA

La versione CENO è un'unica macchina virtuale (solo master che non prevede l'utilizzo delle sonde).

Tutte le altre versioni hanno:

- Il nodo Master dove risiede il database, l'interfaccia web e ha la possibilità di eseguire scansioni.
- Il nodo Slave (Sonda) da cui vengono effettuate le scansioni.

Versioni di Greenbone Enterprise – Virtual Appliance

- **Greenbone Enterprise CENO**

  https://www.greenbone.net/en/gsm-ceno

  Coverage of up to 500 IP addresses within 24 hours (actual achievable number depends on scan pattern and scan targets)

  System Requirements for the Virtual Machine:

  64-Bit version Linux OS, 2 vCPU cores, 8 GB RAM, 135 GB HDD, 4 virtual Ethernet ports

- **Greenbone Enterprise DECA**

  https://www.greenbone.net/en/gsm-deca/

  Control of up to 2 sensors

  Coverage of up to 1,500 IP addresses within 24 hours (actual achievable number depends on scan pattern and scan targets)

  System Requirements for the Virtual Machine:

  64-Bit version Linux OS, 4 vCPU cores, 8 GB RAM, 220 GB HDD, 4 virtual Ethernet ports

Versioni di Greenbone Enterprise – Virtual Appliance

- **Greenbone Enterprise TERA**

  https://www.greenbone.net/en/gsm-tera

  Control of up to 6 sensors

  Coverage of up to 3,000 IP addresses within 24 hours (actual achievable number depends on scan pattern and scan targets)

  System Requirements for the Virtual Machine:

  64-Bit version Linux OS, 6 vCPU cores, 8 GB RAM, 220 GB HDD, 8 virtual Ethernet ports

- **Greenbone Enterprise PETA**

  https://www.greenbone.net/en/gsm-peta/

  Control of up to 12 sensors

  Coverage of up to 9,000 IP addresses within 24 hours (actual achievable number depends on scan pattern and scan targets)

  System Requirements for the Virtual Machine:

  64-Bit version Linux OS, 8 vCPU cores, 16 GB RAM, 220 GB HDD, 8 virtual Ethernet ports

Versioni di Greenbone Enterprise – Virtual Appliance

- **Greenbone Enterprise EXA**

  https://www.greenbone.net/en/gsm-exa/

  Control of up to 24 sensors

  Coverage of up to 18,000 IP addresses within 24 hours (actual achievable number depends on scan pattern and scan targets)

  System Requirements for the Virtual Machine:

  64-Bit version Linux OS, 12 vCPU cores, 24 GB RAM, 225 GB HDD, 8 virtual Ethernet ports

- **Greenbone Enterprise 25V (Sonda)**

  https://www.greenbone.net/en/gsm-25v/

  Coverage of up to 300 IP addresses within 24 hours (actual achievable number depends on scan pattern and scan targets)

  System Requirements for the Virtual Machine:

  64-Bit version Linux OS, 2 vCPU cores, 6 GB RAM, 70 GB HDD, 4 virtual Ethernet ports

POC – Greenbone Enterprise TERA

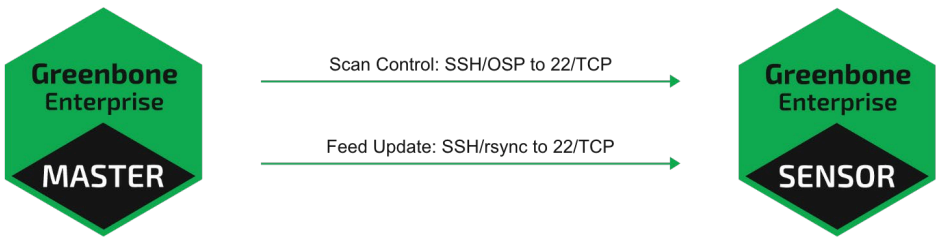
Siamo riusciti ad ottenere una versione di prova per un mese di Greenbone Enterprise TERA

La POC è iniziata 11 Aprile e terminata 11 Maggio

Ci sono state fornite due immagini OVA (una master e una slave).

Il nodo Master è stato installato a Trieste

Il nodo Slave (Sonda) è stato installato a Roma2



POC – Che prove sono state fatte?

- Tutte scansioni a tappeto senza pre-selezione di IP con nmap/zmap.
- Per ogni scansione fatta con Greenbone Enterprise è stata effettuata la stessa scansione con gli stessi parametri con Greenbone Source Edition
- Tipi di scansioni previste:

Scansioni dall'esterno della rete

Rete Target	Sede 1	Sede 2	Sede 3	Sede 4	Sede 5	Sede 6	Sede 7
IP Disponibili	508	762	3830	764	254	254	1782

Scansioni dall'interno della rete (aprendo le ACL dei router delle varie sedi)

Rete Target	Sede 2	Sede 4	Sede 6
IP Disponibili	762	764	254

Scansioni autenticate (su un numero limitato di Host)

Rete Target	Sede 1	Sede 2	Sede 4
IP Disponibili	32	35	9

POC – Configurazione delle scansioni

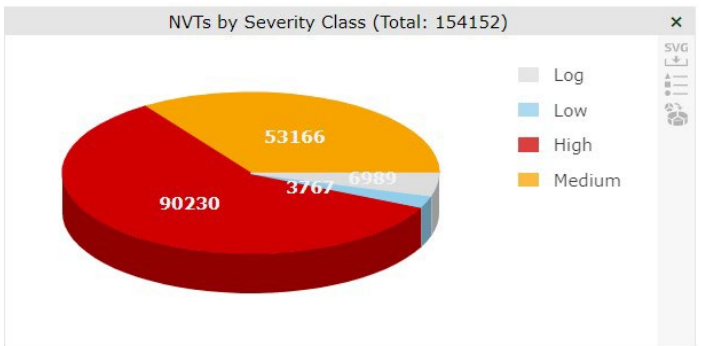
Greenbone Enterprise Tera

Port List:

All TCP and Nmap top 100 UDP
(Version 20200827.)

Comment	Version 20200827.
Port Count	65635
TCP Port Count	65535
UDP Port Count	100

NVT:



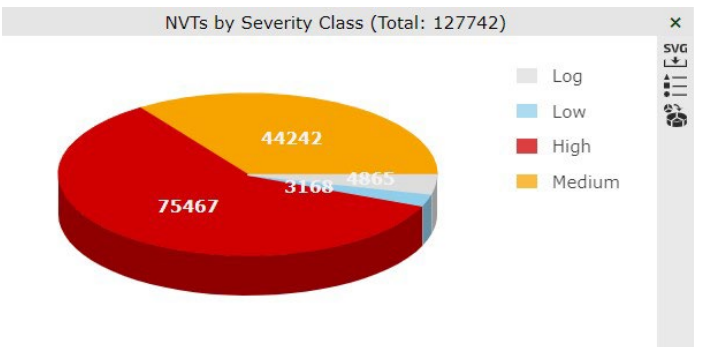
Greenbone Security Assistant

Port List:

All TCP and Nmap top 100 UDP
(Version 20200827.)

Comment	Version 20200827.
Port Count	65635
TCP Port Count	65535
UDP Port Count	100

NVT:



POC – NVT Enterprise vs Community

Nella versione Enterprise sono presenti NVTs Family di specifici Sistemi Operativi che nella versione Community sono completamente assenti

NVTs Family	NVTsEnterprise	NVTsCommunity	Differenza	Differenzapercentuale
AlmaLinux Local Security Checks	828	0	828	100%
PCI-DSS	32	0	32	100%
PCI-DSS 2.0	32	0	32	100%
Rocky Linux Local Security Checks	916	0	916	100%
Solaris Local Security Checks	899	1	898	100%

La differenza fra il numero totale degli NVT è di circa il 17%

NVTs Family	NVTsEnterprise	NVTsCommunity	Differenza	Differenzapercentuale
TOTALE	153.648	127.400	26.248	17%

POC – I Risultati

Scansioni dall'esterno della rete:

IP Disponibili	Rete target		Risultati scansioni con server community	Risultati scansioni con server enterprise	Differenza	Differenza percentuale
508	Sede 1	Numero di host trovati accesi	146	143	3	2%
		Numero di vulnerabilita' GRAVI	3	3	0	0%
		Numero di vulnerabilita' MEDIE	33	34	-1	-3%
		Numero porte+protocollo trovate aperte	12	11	1	8%
		Durata della scansione	8:31:00	13:14:00	-4:43:00	-55%
762	Sede 2	Numero di host trovati accesi	21	22	-1	-5%
		Numero di vulnerabilita' GRAVI	2	5	-3	-150%
		Numero di vulnerabilita' MEDIE	8	46	-38	-475%
		Numero porte+protocollo trovate aperte	2	14	-12	-600%
		Durata della scansione	4:10:00	5:48:00	-1:38:00	-39%
3830	Sede 3	Numero di host trovati accesi	167	165	2	1%
		Numero di vulnerabilita' GRAVI	2	2	0	0%
		Numero di vulnerabilita' MEDIE	131	124	7	5%
		Numero porte+protocollo trovate aperte	9	9	0	0%
		Durata della scansione	28:13:00	9:12:00	19:01:00	67%
764	Sede 4	Numero di host trovati accesi	142	144	-2	-1%
		Numero di vulnerabilita' GRAVI	10	10	0	0%
		Numero di vulnerabilita' MEDIE	81	82	-1	-1%
		Numero porte+protocollo trovate aperte	14	12	2	14%
		Durata della scansione	10:01:00	10:41:00	-0:40:00	-7%

POC – I Risultati

Scansioni dall'esterno della rete:

IP Disponibili	Rete target		Risultati scansioni con server community	Risultati scansioni con server enterprise	Differenza	Differenza percentuale
254	Sede 5	Numero di host trovati accesi	4	4	0	0%
		Numero di vulnerabilita' GRAVI	0	0	0	#DIV/0!
		Numero di vulnerabilita' MEDIE	0	0	0	#DIV/0!
		Numero porte+protocollo trovate aperte	0	0	0	#DIV/0!
		Durata della scansione	1:58:00	0:47:00	1:11:00	60%
254	Sede 6	Numero di host trovati accesi	45	46	-1	-2%
		Numero di vulnerabilita' GRAVI	2	2	0	0%
		Numero di vulnerabilita' MEDIE	69	73	-4	-6%
		Numero porte+protocollo trovate aperte	10	11	-1	-10%
		Durata della scansione	3:43:00	3:11:00	0:32:00	14%
1782	Sede 7	Numero di host trovati accesi	169	60	109	64%
		Numero di vulnerabilita' GRAVI	3	0	3	100%
		Numero di vulnerabilita' MEDIE	49	14	35	71%
		Numero porte+protocollo trovate aperte	13	7	6	46%
		Durata della scansione	11:49:00	10:04:00	1:45:00	15%

POC – I Risultati

Scansioni dall'interno della rete:

IP Disponibili	Rete target		Risultati scansioni con server community	Risultati scansioni con server enterprise	Differenza	Differenza percentuale
762	Sede 2	Numero di host trovati accesi	122	123	-1	-1%
		Numero di vulnerabilita' GRAVI	129	132	-3	-2%
		Numero di vulnerabilita' MEDIE	552	393	159	29%
		Numero porte+protocollo trovate aperte	48	49	-1	-2%
		Durata della scansione	11:42:00	11:33:00	0:09:00	1%
764	Sede 4	Numero di host trovati accesi	158	156	2	1%
		Numero di vulnerabilita' GRAVI	238	166	72	30%
		Numero di vulnerabilita' MEDIE	452	397	55	12%
		Numero porte+protocollo trovate aperte	41	42	-1	-2%
		Durata della scansione	14:40:00	40:53:00	-26:13:00	-179%
254	Sede 6	Numero di host trovati accesi	39	38	1	3%
		Numero di vulnerabilita' GRAVI	11	9	2	18%
		Numero di vulnerabilita' MEDIE	93	79	14	15%
		Numero porte+protocollo trovate aperte	18	15	3	17%
		Durata della scansione	4:04:00	4:36:00	-0:32:00	-13%

POC – I Risultati

Scansioni autenticate:

Host	Rete target		Risultati scansioni con server community	Risultati scansioni con server enterprise	Differenza	Differenza percentuale
32	Sede 1	Numero di host trovati accesi	26	18	8	31%
		Numero di vulnerabilita' GRAVI	180	198	-18	-10%
		Numero di vulnerabilita' MEDIE	83	97	-14	-17%
		Numero porte+protocollo trovate aperte	5	4	1	20%
		Durata della scansione	4:50:00	1:58:00	2:52:00	59%
35	Sede 2	Numero di host trovati accesi	35	34	1	3%
		Numero di vulnerabilita' GRAVI	1830	1881	-51	-3%
		Numero di vulnerabilita' MEDIE	1020	972	48	5%
		Numero porte+protocollo trovate aperte	10	9	1	10%
		Durata della scansione	7:33:00	4:23:00	3:10:00	42%
9	Sede 4	Numero di host trovati accesi	9	8	1	11%
		Numero di vulnerabilita' GRAVI	2	39	-37	-1850%
		Numero di vulnerabilita' MEDIE	19	26	-7	-37%
		Numero porte+protocollo trovate aperte	4	4	0	0%
		Durata della scansione	1:29:00	1:24:00	0:05:00	6%

POC – I Risultati – Scansione autentica (Sede 4)

Greenbone Source Edition - Host con Sistema Operativo Rocky Linux 8.7

IP Address	Hostname	OS ▾	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity
2[redacted]	p[redacted]	?	1	16			Fri, May 12, 2023 1:40 PM CEST	Fri, May 12, 2023 2:56 PM CEST	0	3	2	0	0	5	5.5 (Medium)
1[redacted]	m[redacted]	?	0	20			Fri, May 12, 2023 1:40 PM CEST	Fri, May 12, 2023 2:40 PM CEST	0	1	2	0	0	3	5.5 (Medium)
1[redacted]	s[redacted]	?	1	23			Fri, May 12, 2023 1:40 PM CEST	Fri, May 12, 2023 2:41 PM CEST	0	2	2	0	0	4	5.3 (Medium)

Greenbone Enterprise TERA – Host con Sistema Operativo Rocky Linux 8.7 – Before Upgrades

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity ▾
2[redacted]	p[redacted]	?	1	16			Fri, May 12, 2023 9:08 AM CEST	Fri, May 12, 2023 10:29 AM CEST	11	4	0	0	0	15	9.8 (High)
1[redacted]	s[redacted]	?	1	24			Fri, May 12, 2023 9:08 AM CEST	Fri, May 12, 2023 10:28 AM CEST	11	0	0	0	0	11	8.8 (High)
1[redacted]	m[redacted]	?	1	23			Fri, May 12, 2023 9:08 AM CEST	Fri, May 12, 2023 10:08 AM CEST	15	5	0	0	0	20	8.8 (High)

Greenbone Enterprise TERA – Host con Sistema Operativo Rocky Linux 8.7 – After Upgrades

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity ▾
1[redacted]	s[redacted]	?	2	24			Fri, May 12, 2023 4:14 PM CEST	Fri, May 12, 2023 5:32 PM CEST	11	2	0	0	0	13	8.8 (High)

Come si può notare, usando i pacchetti interni alla distribuzione, non si è riusciti a risanare tutte le vulnerabilità segnalate.

Le ricette proposte da Greenbone per sanare le vulnerabilità che rimangono prevedono di installare pacchetti esterni a quelli della distribuzione, con tutti i problemi di consistenza futura che queste azioni di contaminazione comportano.

POC – I Risultati

Scansioni Totali:

Tipo scansione		Risultati scansioni con server community	Risultati scansioni con server enterprise	Differenza	Differenza percentuale
Scansioni dall'esterno della rete	Numero di host trovati accesi	694	584	110	16%
	Numero di vulnerabilita' GRAVI	22	22	0	0%
	Numero di vulnerabilita' MEDIE	371	373	-2	-1%
	Numero porte+protocollo trovate aperte	60	64	-4	-7%
	Durata della scansione	68:25:00	52:57:00	15:28:00	23%
Scansioni dall'interno della rete	Numero di host trovati accesi	319	317	2	1%
	Numero di vulnerabilita' GRAVI	378	307	71	19%
	Numero di vulnerabilita' MEDIE	1097	869	228	21%
	Numero porte+protocollo trovate aperte	107	106	1	1%
	Durata della scansione	30:26:00	57:02:00	-26:36:00	-87%
Scansioni autenticate	Numero di host trovati accesi	70	60	10	14%
	Numero di vulnerabilita' GRAVI	2012	2118	-106	-5%
	Numero di vulnerabilita' MEDIE	1122	1095	27	2%
	Numero porte+protocollo trovate aperte	19	17	2	11%
	Durata della scansione	13:52:00	7:45:00	6:07:00	44%
Totali Scansioni	Numero di host trovati accesi	1083	961	122	11%
	Numero di vulnerabilita' GRAVI	2412	2447	-35	-1%
	Numero di vulnerabilita' MEDIE	2590	2337	253	10%
	Numero porte+protocollo trovate aperte	186	187	-1	-1%
	Durata della scansione	112:43:00	117:44:00	-5:01:00	-4%

POC – …e la Sonda?

La Sonda permette di effettuare scansioni solo all'interno della rete in cui è installata.

Nella POC la Sonda era installata a Roma2, quindi potevamo effettuare scansioni sulla rete di Roma2 ma non su un'altra rete, come ad esempio Firenze.

In sostanza la sonda non ci serve a meno di non metterne una in ogni sede o di eleggere sedi particolari dove serve.

POC – Conclusioni

- Si tratta solo di una prima analisi preliminare dei risultati (la POC è finita il giorno 11/05/23).
- Tutto il lavoro già fatto con la versione Community, sia per INFN-Cloud che in generale, si potrebbero riutilizzare per la versione Enterprise (le API sono le stesse).
- Dai risultati preliminari del confronto fra versione Community ed Enterprise non risulta una differenza eclatante fra i risultati che si ottengono fra le due versioni e, tutto sommato, già con la versione Community si ottengono risultati validi.
- Ci sono state proposte varie configurazioni per la versione Enterprise con vari livelli di efficienza ma le varie opzioni dell'offerta commerciale proposte hanno costi sufficientemente lontani da quelli che possiamo permetterci, soprattutto in relazione al limitato miglioramento che si otterrebbe passando alla versione Enterprise.
- Stiamo valutando altri software simili (Nessus, Nexpose ed altri) anche se non sono opensource e quindi oltre a testarli sarebbe necessario richiedere delle offerte economiche.