Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

Scansioni di vulnerabilità in ambito CCR

Leandro Lanzi

Miniworkshop sulla Sicurezza Informatica
(Padova, 13-15 febbraio 2023)

Storia degli strumenti per scansioni di vulnerabilità del gruppo auditing/security di CCR

2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022

Scansioni del gruppo auditing/security dall'esterno delle sedi con Nessus + nmap, audiweb (2010-2019). *Aurora Mazzone*, *Leandro Lanzi* e *Franco Brasolin*

KALINFN, distribuzione live con OpenVAS per scansioni interne locali (2017-2019). *Leandro Lanzi*

Greenbone Community Edition per scansioni interne locali (2018-2020)

SCANBOT + Greenbone Community Edition per scansioni dall'esterno delle sedi (2021-2022) *Leandro Lanzi*

Scansioni standard

- Scansioni con **`nmpa`** su tutte le reti del dominio `infn.it`. al fine di identificare un ristretto numero di IP attivi.
  - Porte investigate
    - UDP: 7, 19, 21, 53, 69, 123, 141, 161, 162
    - TCP: 21, 22, 23, 25, 53, 80, 109, 110, 123, 135, 139, 143, 161, 162, 443, 445, 465, 587, 993, 995, 1080, 1433, 1434, 1443, 2301, 2381, 3306, 3389, 5432, 5900, 8000, 8443, 8080, 8081, 8888
  - Il livello di dettaglio dei risultati è:

    IP - Protocollo (TCP/UDP) - Porta + informazioni su sistema operativo, servizio, ...
- Recentemente scansioni con **`zmpa`** su tutte le porte TCP.
  - Il livello di dettaglio dei risultati è:

    IP - Porta TCP aperta/chiusa
- Scansioni con **Greenbone Community Edition (GCE)**, spesso chiamato anche OpenVAS, solo sugli IP risultati attivi nelle scansioni `nmap` e `zmap` precedenti.
  - Il livello di dettaglio dei risultati è:

    IP - Protocollo (TCP/UDP) - Porta - Vulnerabilità

Altri tipi di scansioni

- 2014
  - Porta UDP 123 - Attacchi DDoS causati da NTP reflection tramite il comando monlist
  - Poodle - Attacchi MITM su connessioni SSL/TLS che utilizzano SSL 3.0
  - Heartbleed - openssl
- 2021
  - Log4j
- 2022
  - Siti web e protocolli SSL/TLS obsoleti (Piano Triennale per l'Informatica nella Pubblica Amministrazione)

Pubblicazione dei risultati

- I risultati delle scansioni sono pubblicati su

  https://scan.fi.infn.it

- I permessi di accesso ai risultati delle scansioni delle singole strutture vengono gestiti in INFN-AAI in base a ruoli e in qualche caso eccezionale in base all'identità.
- Per ogni struttura hanno accesso ai dati solo
  - gli afferenti al Servizio Calcolo e Reti (o simile) della struttura;
  - il rappresentante della struttura in CCR;
  - il Direttore della struttura.
- Una funzionalità che non è stata pubblicizzata: il Responsabile del Servizio Calcolo e Reti tramite GODIVA-GUI può modificare lo schema di accesso di default per la propria struttura aprendo o chiudendo l'accesso ad altri utenti o ad utenti con ruoli diversi.

Gestione e correzione delle vulnerabilità

- Nessuna attività consolidata:
  - salvo periodi eccezionali o rari casi estremamente pericolosi, la consultazione delle vulnerabilità rilevate e la loro gestione e correzione sono sempre state lasciate ai diretti interessati senza obblighi o verifiche.

Un esempio: scansione su server web e protocolli SSL/TLS [1/6]

- **Entro giugno 2022** - Piano Triennale per l'Informatica nella Pubblica Amministrazione per gli anni 2021-2023: usare per HTTPS solo protocolli TLS 1.2 e 1.3 ed implementare un qualche meccanismo di ridirezione da HTTP ad HTTPS.
- **Marzo 2022** - Scansione sui siti web INFN: solo porta 80 e 443; sono esclusi dalla scansione tutti i server web attivi su porte diverse e tutti i "virtual host".
- **Maggio 2022** - Workshop del Calcolo INFN: presentazione dei risultati, invito a risolvere i problemi rilevati, indicazioni per risolvere i problemi e segnalazione di tool di verifica.
- **17 giugno 2022** - Mail alle Sedi: link per accedere ai dati, invito a risolvere i problemi rilevati, indicazioni per risolvere i problemi e segnalazione di tool di verifica.
- **Settembre 2022** - Nuova scansione sui siti web INFN con le stesse modalità della precedente.
- **Settembre 2022** - Riunione di bilancio del Calcolo INFN: presentazione dei risultati e confronto con i dati precedenti.

  Non si registrano particolari miglioramenti rispetto alla scansione precedente.
- **2 novembre 2022** - Fonoconferenza CCR: decisione di segnalare i problemi tramite mail e monitorare le operazioni di correzione tramite un sistema di ticket.
  - 10/11/2022: invio di 453 segnalazioni via mail con relativa apertura di 453 ticket.
  - 2022-11-15: invio del primo promemoria per i ticket non chiusi.
  - 2022-11-28 invio del secondo promemoria per i ticket non chiusi.

Un esempio: scansione su server web e protocolli SSL/TLS [2/6]

Risultati dell'analisi dei server web dell'Ente nelle due scansioni di marzo e giugno: porte aperte, server web e reindirizzamento automatico

Lanzi, Carbone
Riunione di bilancio
per il Calcolo nell'INFN
Castel Gandolfo
28-30/09/2022

Numero totale di	Vecchia scansione marzo 2022	Nuova scansione settembre 2022
IP che rispondono sulla porta 80 (compresi falsi positivi)	741	663 (-10,53%)
IP che rispondono sulla porta 443 (compresi falsi positivi)	759	753 (-0,79%)
Server web che rispondono sulla porta 80	535	559 (4,49%)
Server web che rispondono sulla porta 443	637	686 (7,69%)
Server web che rispondono solo sulla porta 80 ma non sulla porta 443	128	124 (-3,13%)
Server web che rispondono solo sulla porta 443 ma non sulla porta 80	230	251 (9,13%)
Server web che rispondono sia sulla porta 80 che sulla porta 443	407	435 (6,88%)
Server web che rispondono sulla porta 80 con redirect alla porta 443 (sullo stesso IP o su un IP diverso)	206	227 (10,19%)
Server web che rispondono sulla porta 80 e senza redirect alla porta 443 (sullo stesso IP o su un IP diverso)	329	332 (0,91%)

Un esempio: scansione su server web e protocolli SSL/TLS [3/6]

Risultati dell'analisi dei server web dell'Ente nelle due scansioni di marzo e giugno: protocolli SSL e TLS

Lanzi, Carbone
Riunione di bilancio
per il Calcolo nell'INFN
Castel Gandolfo
28-30/09/2022

	Vecchia scansione marzo 2022		Nuova scansione settembre 2022	
Numero totale dei server web con solo HTTP (NO HTTPS)	128		124 (-3,13%)	
Numero totale dei server web con HTTPS (ed eventualmente HTTP)	637		686	
Protocollo	Offerto	**Non** offerto	Offerto (variazione %)	**Non** offerto (variazione %)
SSLv2	2	635	4 (100,00%)	682 (7,40%)
SSLv3	49	588	29 (-40,82%)	657 (11,73%)
TLS1	416	221	326 (-21,63%)	360 (62,90%)
TLS1.1	394	243	309 (-21,57%)	377 (55,14%)
TLS1.2	609	28	653 (7,22%)	33 (17,86%)
TLS1.3	114	523	152 (33,33%)	534 (2,10%)

Un esempio: scansione su server web e protocolli SSL/TLS [4/6]

Risultati dell'analisi dei server web dell'Ente nelle due scansioni di marzo e giugno: classificazione delle configurazioni secondo AgID

		Vecchia scansione marzo 2022			Nuova scansione settembre 2022		
Configurazioni	**Descrizione**	**Numero**	**Totale**		**Numero**	**Totale**	
Sicure	**TLS1.2**, **TLS1.3**	65	**211**		101	**354 (68%)**	
	TLS1.3	0			10		
	TLS1.2	146			243		
Mal configurate	TLS1.1, **TLS1.2**, **TLS1.3**	2	**358**	637	0	**292 (-18%)**	686 (7,7%)
	TLS1.1, **TLS1.2**	7			5		
	TLS1, TLS1.1, **TLS1.2**, **TLS1.3**	47			41		
	TLS1, TLS1.1, **TLS1.2**	298			246		
	TLS1, **TLS1.2**	4			0		
Gravi	SSLv2 o SSLv3 oppure TLS1 + nessuno tra TLS 1.1, TLS 1.2 e TLS 1.3 oppure TLS1.1 + nessuno tra TLS 1.2 e TLS 1.3	**68**			**40**	**(-41%)**	
No HTTPS	Comunicazione esclusivamente in chiaro sulla porta 80	**128**			**124**		**(-3,1%)**
TOTALE		**765**			**810**		(5,9%)

Lanzi, Carbone
Riunione di bilancio per il Calcolo nell'INFN
Castel Gandolfo
28-30/09/2022

Un esempio: scansione su server web e protocolli SSL/TLS [5/6]

Un primo esperimento di monitoraggio delle correzioni di vulnerabilità.

- **2 novembre 2022 -** videoconferenza CCR: decisione di segnalare i problemi tramite mail e monitorare le operazioni di correzione tramite un sistema di ticket.
  - 10/11/22: invio di 453 segnalazioni via mail con relativa apertura di 453 ticket.
  - 15/11/22: invio del primo promemoria per i ticket non chiusi.
  - 28/11/22: invio del secondo promemoria per i ticket non chiusi.

Un esempio: scansione su server web e protocolli SSL/TLS [6/6]

- Andamento temporale dei ticket (1 ticket = 1 mail = 1 IP)

Data	Numero totale di Ticket	Ticket IN STALLO in attesa di risposta	Ticket IN STALLO in attesa di risposta su cui stanno lavorando	Ticket CHIUSI	Ticket CHIUSI con PROBLEMA RISOLTO	Ticket CHIUSI con PROBLEMA NON RISOLTO
23/11/2022	453	117 (26%)	22 (5%)	336 (74%)	294 (65%)	42 (9%)
30/11/2022	453	80 (18%)	17 (4%)	373 (82%)	325 (72%)	48 (11%)
06/12/2022	453	64 (14%)	15 (3%)	389 (86%)	341 (75%)	48 (11%)

- La situazione nelle varie Sedi (sezioni, laboratori, gruppi collegati, SI, ...)

Sedi	Numero di Ticket	Ticket IN STALLO in attesa di risposta	Ticket IN STALLO in attesa di risposta su cui stanno lavorando	Ticket CHIUSI	Ticket CHIUSI con PROBLEMA RISOLTO	Ticket CHIUSI con PROBLEMA NON RISOLTO
Le **15 sedi** più efficienti	149	0 (%0)	0 0%0)	149 (100%)	149 (100%)	0 (0%)
Le **14 sedi** che si danno da fare	277	37 (13%)	14 (5%)	240 (87%)	192 (69%)	48 (17%)
Le **4 sedi** con maggiori difficoltà	27	27 (100%)	1 (4%)	0 (0%)	0 (0%)	0 (0%)

Conclusione

- In ambito CCR è stata maturata un'esperienza più che decennale nell'ambito delle scansioni di vulnerabilità che può essere utile anche in futuro.
- Buona parte delle operazioni vengono compiute in modo quasi automatico.
- È già disponibile un sistema di autenticazione e autorizzazione basato su INFN-AAI.
- Come evidenziato nell'esempio di scansione riportato (scansione su server web e protocolli SSL/TLS), la parte maggiormente critica riguarda il monitoraggio delle correzioni delle vulnerabilità.
  - Pubblicare semplicemente i dati non è efficace.
  - Seguire tramite e-mail + sistema di ticket porta ad un notevole miglioramento.
    - Implica però un pesante lavoro di interazione con le struttura.
    - Anche per le strutture dover gestire tutto tramite e-mail è risultato molto dispersivo. Inoltre non hanno una visione generale della situazione per la loro struttura (tipo una pagina web di riepilogo) ma si devono organizzare in proprio.
    - Spesso la mail di riferimento di una struttura è una mailing list, non una singola persona, e questo ha portato a maggiore confusione.
  - L'esperimento e-mail + sistema di ticket, anche se faticoso, è stato comunque utile a definire il nuovo modello di gestione delle vulnerabilità che si vuole realizzare.