



VAN ZWAM ARJEN

VULNERABILITY ASSESSMENT

REPORT

TRACCIA

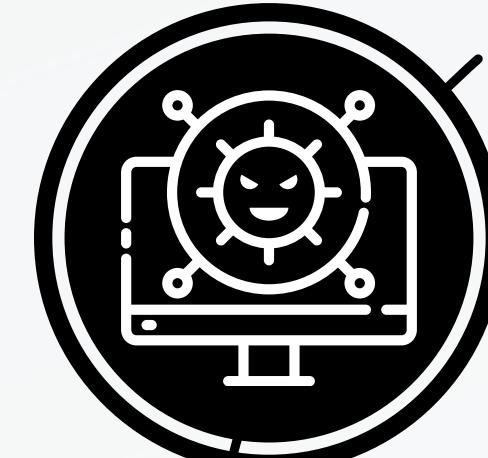
EFFETTUARE UN VULNERABILITY ASSESSMENT CON NESSUS SULLA MACCHINA METASPLOITABLE INDICANDO COME TARGET SOLO LE PORTE COMUNI (POTETE SCEGLIERE COME SCANSIONE IL «BASIC NETWORK SCAN», O L'ADVANCED E POI CONFIGURARLO). A VALLE DEL COMPLETAMENTO DELLA SCANSIONE, ANALIZZATE ATTENTAMENTE IL REPORT PER OGUNA DELLE VULNERABILITÀ RIPORTATE, APPROFONDENDO QUALORA NECESSARIO CON I LINK ALL'INTERNO DEI REPORT E/O CON CONTENUTO DA WEB.

OBIETTIVI DELLO SCAN

Minacce note

La valutazione delle vulnerabilità coinvolge l'utilizzo del software per eseguire una **scansione** del sistema target al fine di identificare le vulnerabilità e le configurazioni insicure presenti.

Il processo di scansione coinvolge l'invio di pacchetti di rete al sistema target e la ricezione delle risposte per determinare la presenza di **vulnerabilità note**.



Potenziali risoluzioni

Nessus utilizza una vasta gamma di plugin di scansione che includono **controlli** per vulnerabilità note, misconfigurazioni, esposizione a minacce note e altri problemi di sicurezza. Dopo la ricerca espone anche piccole pillole per la risoluzione di quella determina vulnerabilità oppure fa redirect di link con la **risoluzione**.



Report dettagliato

Dopo aver completato la scansione, Nessus fornisce un **report dettagliato** che elenca le vulnerabilità rilevate, fornendo informazioni sulle possibili soluzioni e raccomandazioni per mitigare le vulnerabilità. Questo aiuta gli amministratori di sistema e gli specialisti della sicurezza a comprendere meglio le **vulnerabilità** presenti nel sistema e a prendere le misure necessarie per risolverle.



CONFIGURAZIONE

Settings

The screenshot shows the Otenable Nessus Essentials web interface. At the top, there's a navigation bar with the Otenable logo, 'Nessus Essentials', 'Scans', and 'Settings'. On the left, a sidebar lists 'FOLDERS' (My Scans, Test, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main area is titled 'New Scan / Advanced Scan' and has a sub-section 'Back to Scan Templates'. It features three tabs: 'Settings' (selected), 'Credentials', and 'Plugins'. Under 'Settings', there's a 'BASIC' section with a dropdown menu showing 'General' (selected), 'Schedule', and 'Notifications'. Below this are fields for 'Name' (Metasploitable2), 'Description' (empty), 'Folder' (Test), and 'Targets' (192.168.1.222). At the bottom are buttons for 'Upload Targets' and 'Add File'.

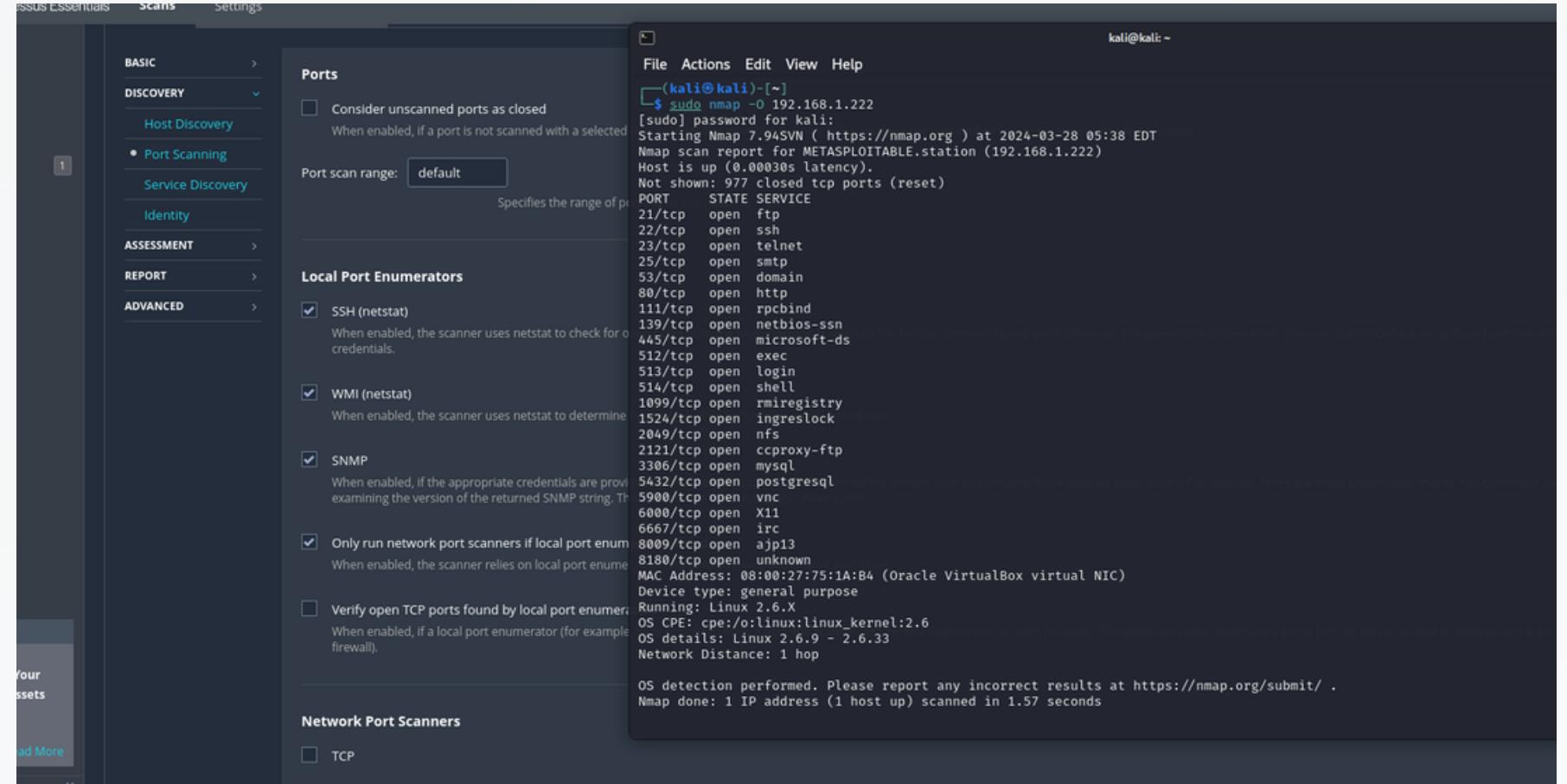
Dopo aver selezionato la tipologia di scan tra “**Basic Network Scan**” o “**Advanced Scan**” si può passare alla configurazione basilare tramite le impostazioni.

Inserendo il nome a scelta (ho ipotizzato la macchina Metasploitable) e inserendo i/il target, in questo caso per ottimizzare le tempistiche ho scelto SOLO la macchina Meta2 che ha come IP 192.168.1.222/24

CONFIGURAZIONE

Port Scanning

Si ha la possibilità di effettuare lo scan per determinate porte aperte a conoscenza oppure effettuare scansioni SYN o TCP in automatico, ho preferito la “**default**” con SYN per tempistiche



The screenshot shows the Nessus configuration interface with the "Scans" tab selected. In the left sidebar, "Port Scanning" is chosen under the "DISCOVERY" section. The main panel displays various configuration options:

- Ports**:
 - Consider unscanned ports as closed (unchecked)
 - Port scan range: default (selected)
- Local Port Enumerators**:
 - SSH (netstat) (checked)
 - WMI (netstat) (checked)
 - SNMP (checked)
 - Only run network port scanners if local port enum (checked)
 - Verify open TCP ports found by local port enum (unchecked)
- Network Port Scanners**:
 - TCP (unchecked)

On the right side of the interface, the terminal window shows the command and output of the Nmap scan:

```
(kali㉿kali)-[~]
$ sudo nmap -O 192.168.1.222
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-03-28 05:38 EDT
Nmap scan report for METASPOITABLE.station (192.168.1.222)
Host is up (0.00030s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:75:1A:B4 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
```

CONFIGURAZIONE

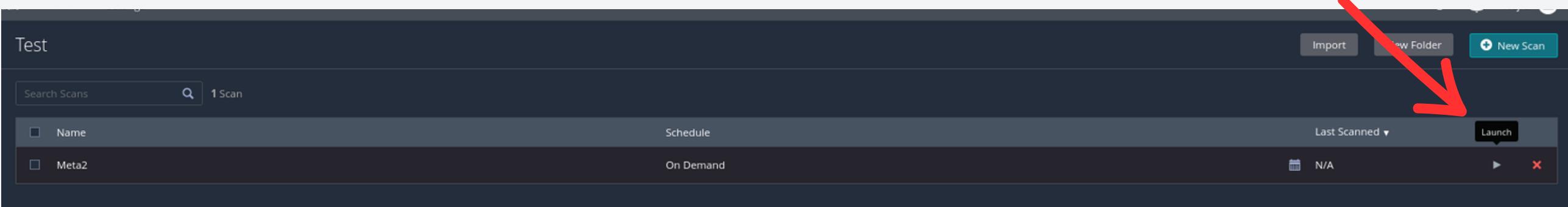
Web Application

The screenshot shows the Nessus configuration interface. At the top, there are tabs for 'Scans' and 'Settings'. Below that, a sub-menu for 'New Scan / Advanced Scan' is visible, with a link to 'Back to Scan Templates'. The main area is titled 'Web Application Settings' under the 'Web Crawler' section. It includes fields for 'Start crawling from' (set to '/'), 'Excluded pages (regex)' (set to '/server_privileges.php|logout'), 'Maximum pages to crawl' (set to '1000'), and 'Maximum depth to crawl' (set to '6'). There is also a checkbox for 'Follow dynamically generated pages' with a note below it stating: 'If selected, Nessus follows dynamic links and may exceed the parameters set above.' On the left side, a sidebar lists various scan types: BASIC, DISCOVERY, ASSESSMENT (with 'General', 'Brute Force', and 'Web Applications' listed), REPORT, and ADVANCED.

Ho preferito abilitare anche lo scan per le Web Application per prendere confidenza.
E' una funzionalità che consente di identificare le vulnerabilità specifiche delle applicazioni web. Questo tipo di scansione è progettato per individuare potenziali falle di sicurezza e debolezze nelle applicazioni web, come errori di configurazione, vulnerabilità del codice, esposizione di dati sensibili e altre minacce..

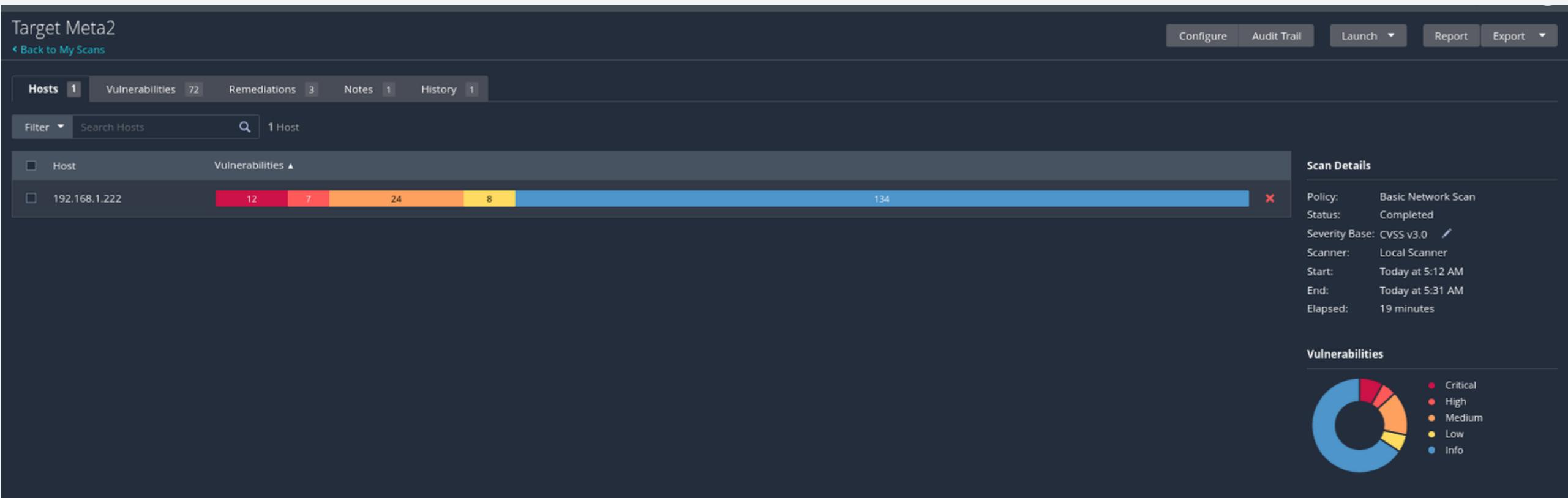
START

Dopo aver salvato la configurazione delle impostazioni per lo **scan** ho premuto il pulsante **LAUNCH**

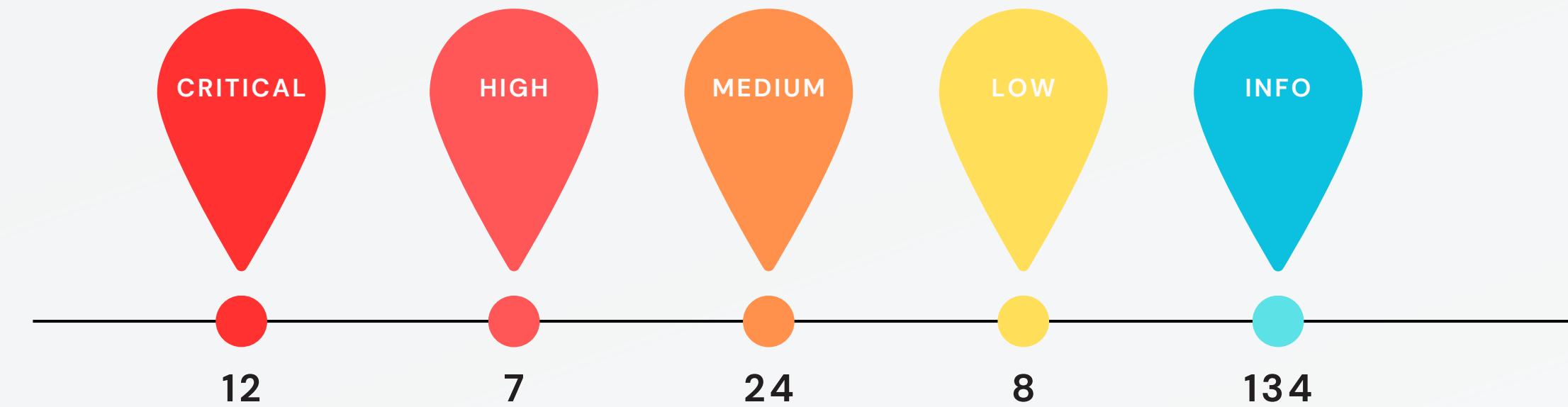


END

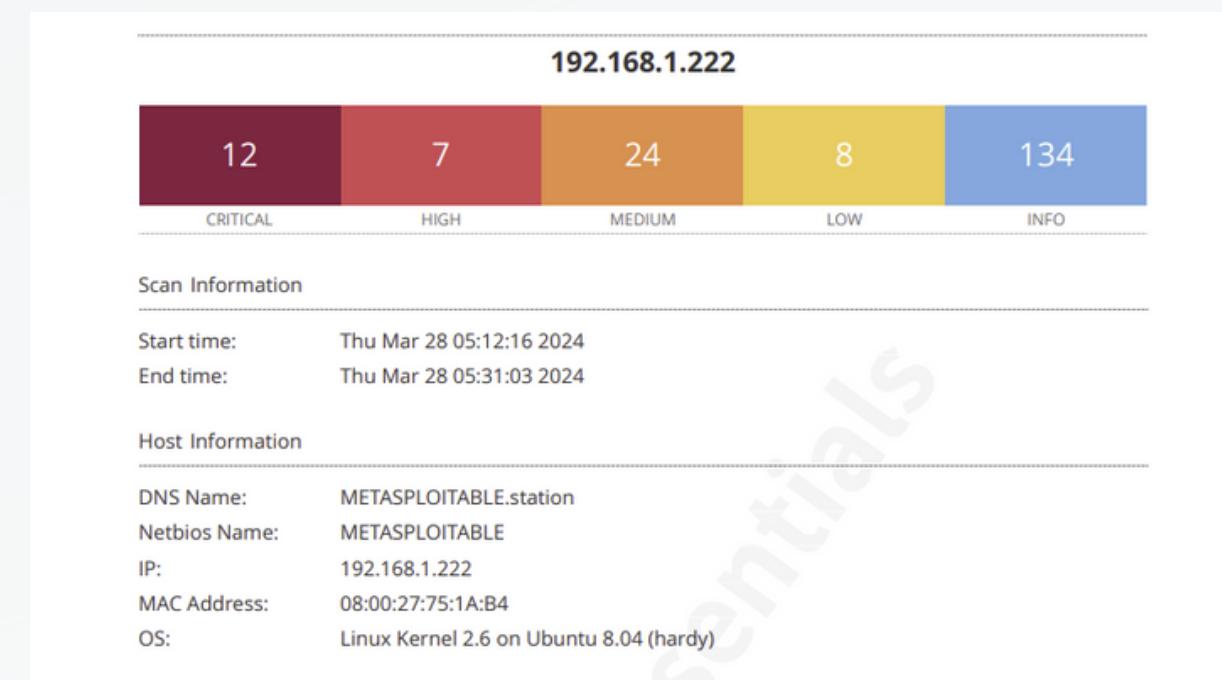
Al termine della lunga attesa dell'effettivo scan terminato con **successo** si potranno vedere i **dettagli** delle vulnerabilità riscontrate



VULNERABILITA'



Ovviamente l'Host Meta2 è stato creato volutamente **iper-vulnerabile**, nonostante ciò ho riscontrato "solamente" 12 critical e 7 high dovuto dal fatto che la mia scansione è stata creata con configurazioni "Lazy"

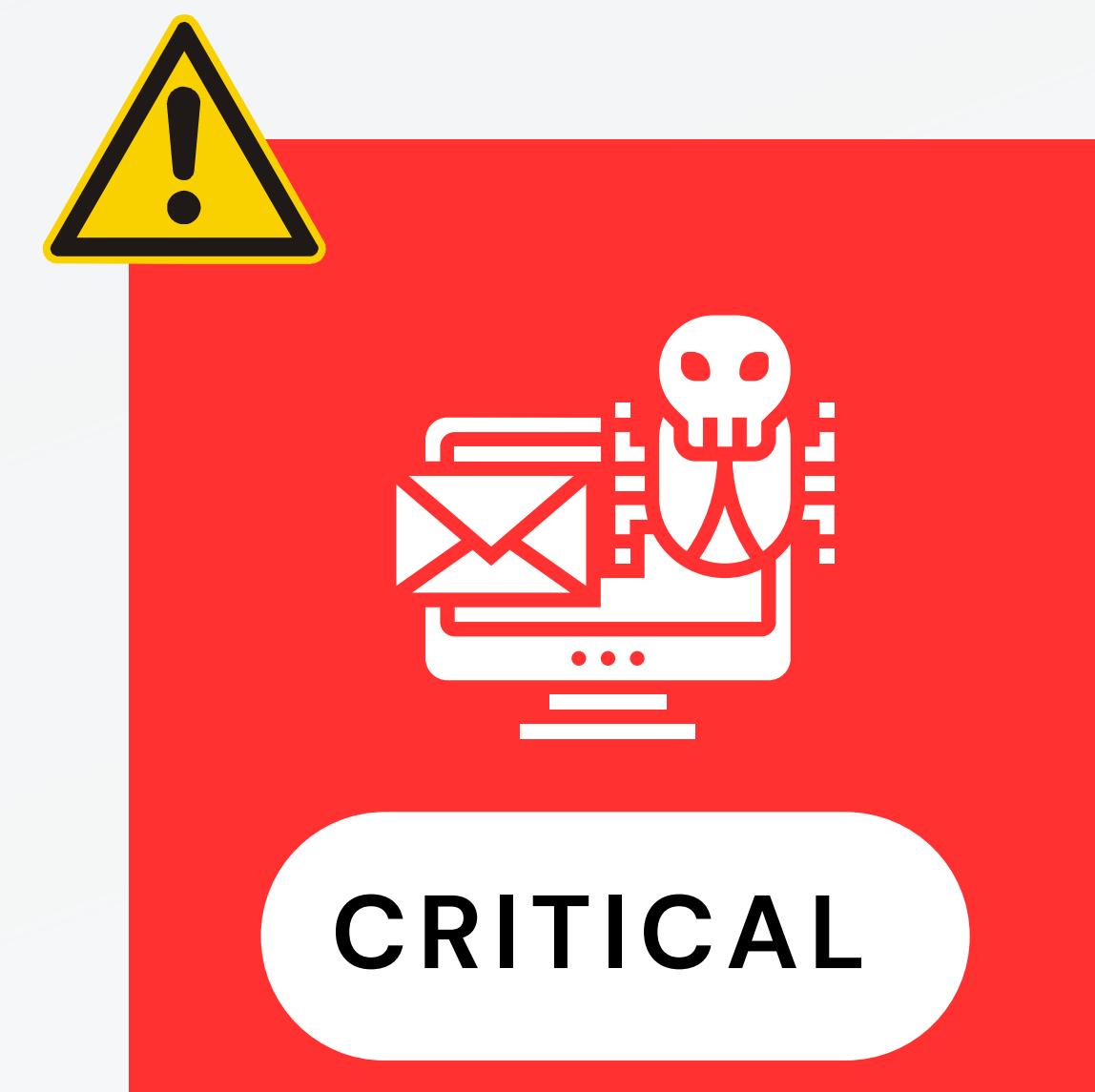
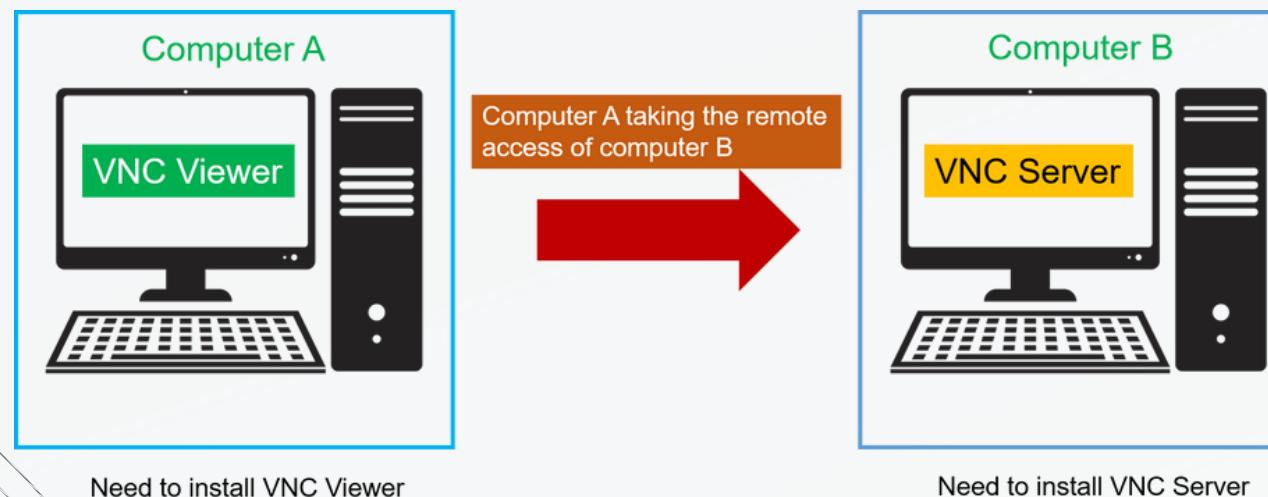


Il report indica anche in dettaglio il MAC Address, l'OS, il nome e tutte le info relative

VNC SERVER 'PASSWORD' PASSWORD

Una delle vulnerabilità riscontrate è quella del **VNC Server** che come default ha come password "password"

Il super tool **Nessus** ci aiuta anche dicendo come poter rimediare.



COSA DICE NESSUS

- The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

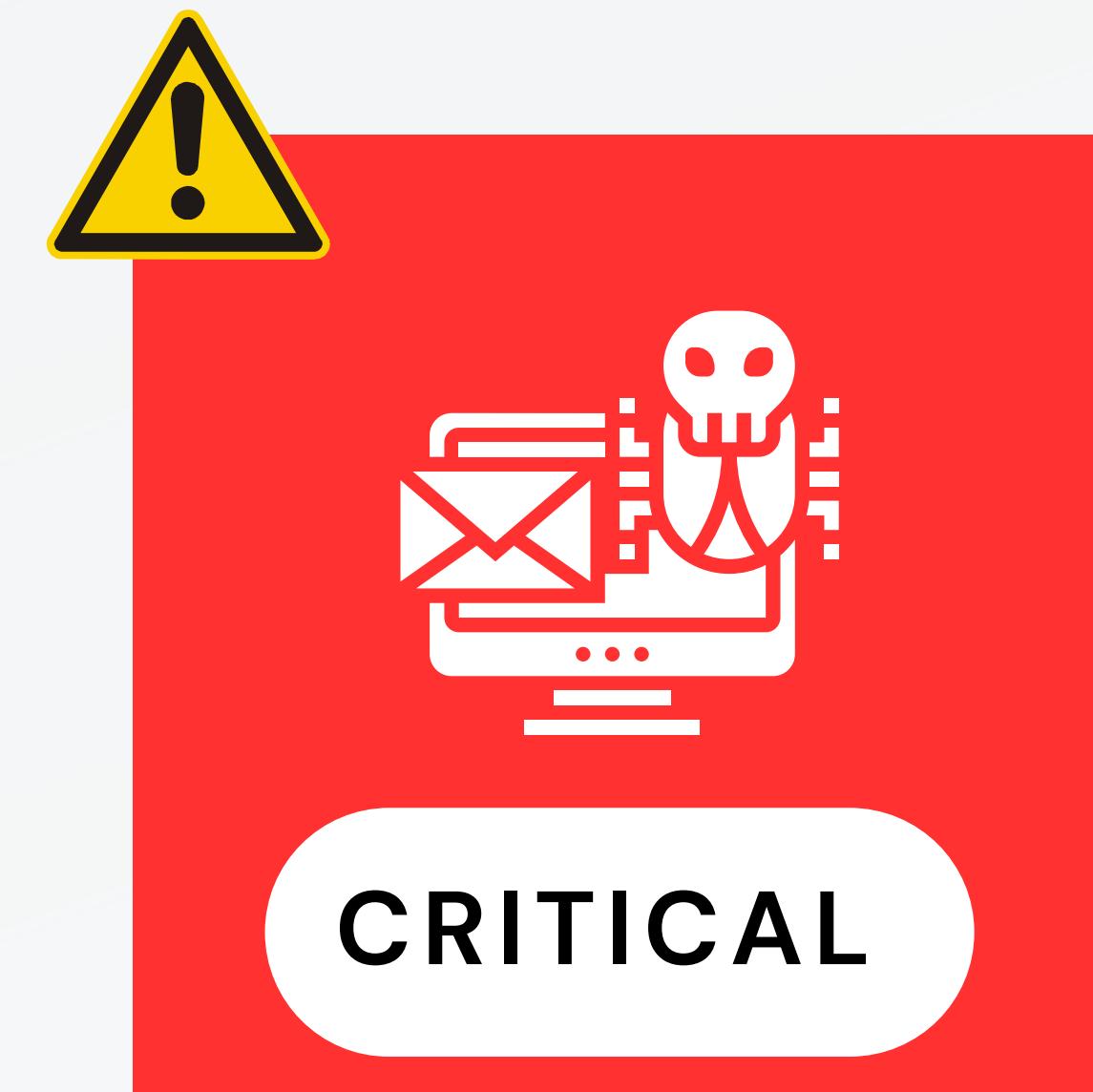
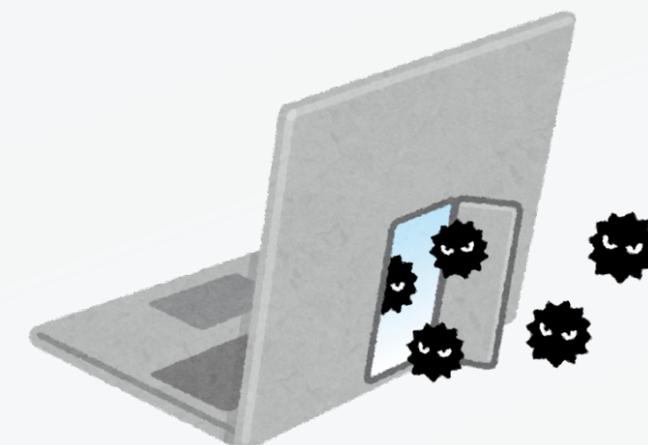
SOLUZIONE

- Secure the VNC service with a strong password.

UNREALIRCd BACKDOOR DETECTION

Un'altra tipologia di vulnerabilità critica trovata è la possibilità della **Backdoor**.

Una delle vulnerabilità più importanti da risolvere immediatamente, Nessus suggerisce anche le credenziali d'accesso, in questo caso "root" e "root".



COSA DICE NESSUS

- The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

SOLUZIONE

- Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

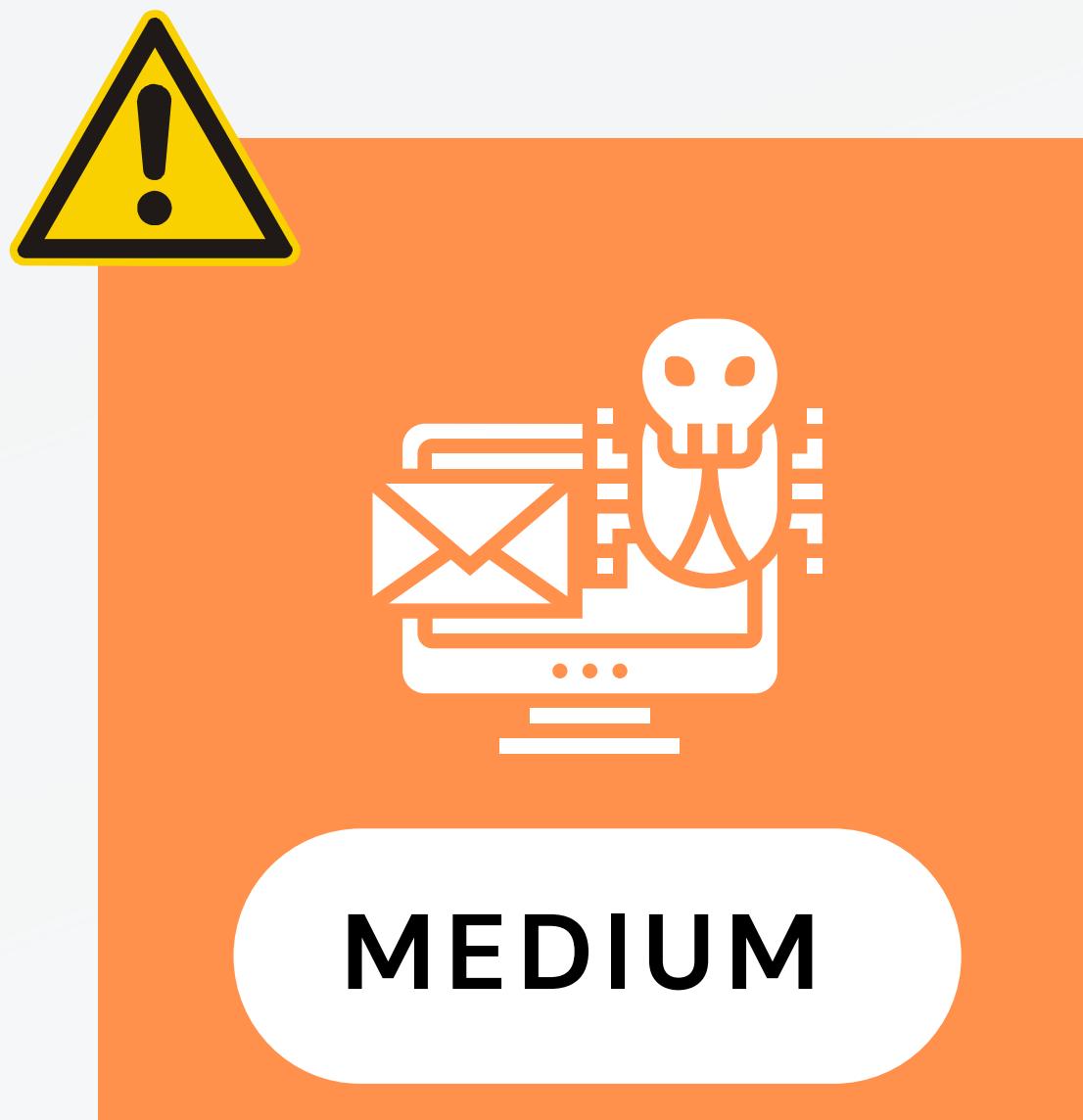
PHPMYADMIN ERROR.PHP BBCODE TAG XSS (PMASA-2010-9)

Tra le vulnerabilità medie abbiamo anche il nostro **phpMyAdmin**.

In questa specifica vulnerabilità, il problema risiede nel modo in cui phpMyAdmin gestisce determinati **tag BBcode** (Basic Bulletin Board Code) all'interno del file error.php. Un attaccante potrebbe sfruttare questa vulnerabilità inserendo del codice malevolo all'interno di un tag BBcode, che verrebbe poi eseguito nel browser dell'utente che visualizza l'errore generato da phpMyAdmin.

L'esecuzione di codice malevolo all'interno del browser dell'utente può consentire all'attaccante di **rubare informazioni sensibili**, come le credenziali di accesso, o di eseguire azioni dannose a nome dell'utente legittimo, come l'inserimento o la modifica di dati nel database.

phpMyAdmin



COSA DICE NESSUS

- The version of phpMyAdmin fails to validate BBcode tags in user input to the 'error' parameter of the 'error.php' script before using it to generate dynamic HTML.
- An attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user's browser to be executed within the security context of the affected site. For example, this could be used to cause a page with arbitrary text and a link to an external site to be displayed.

SOLUZIONE

- Upgrade to phpMyAdmin 3.4.0-beta1 or later.

ALTRO...

Si potrebbero controllare una ad una tutte le vulnerabilità trovate, per ora ho controllato personalmente quelle critical, high e medium.



VAN ZWAM ARJEN