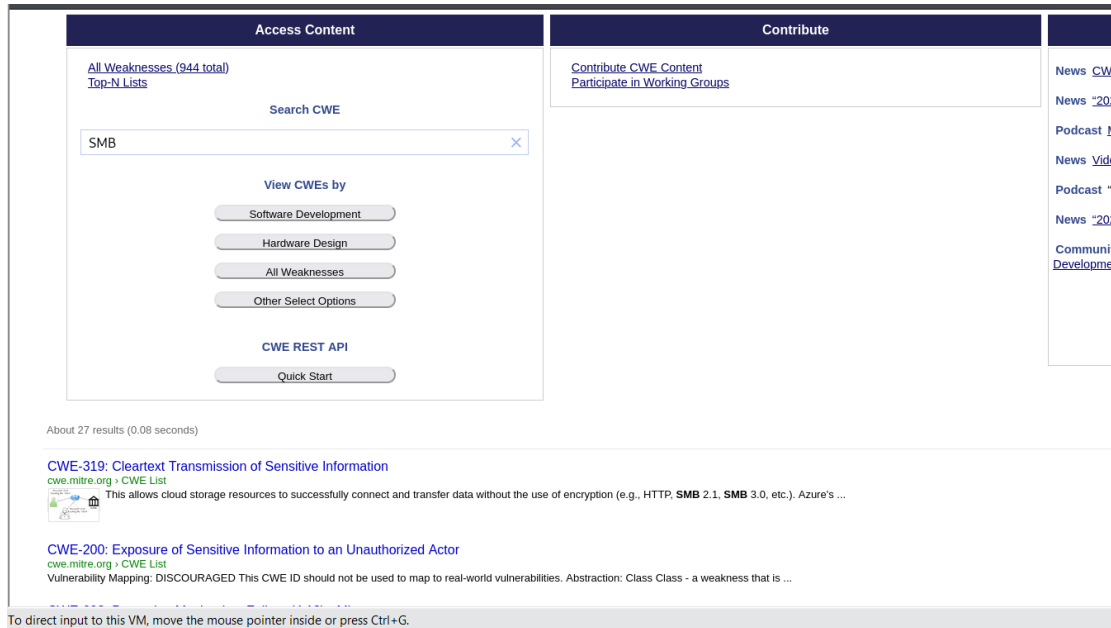


TP : Recherche et analyse de vulnérabilités

Issa MENTA

Partie 1

1.1 Recherche de SMB dans la base CWE – Vulnérabilités SMB



The screenshot shows the CWE Mitre search interface. The search bar contains 'SMB' and the results show 'About 27 results (0.08 seconds)'. The first result is 'CWE-319: Cleartext Transmission of Sensitive Information' with a description: 'This allows cloud storage resources to successfully connect and transfer data without the use of encryption (e.g., HTTP, SMB 2.1, SMB 3.0, etc.). Azure's ...'. The second result is 'CWE-200: Exposure of Sensitive Information to an Unauthorized Actor' with a description: 'Vulnerability Mapping: DISCOURAGED This CWE ID should not be used to map to real-world vulnerabilities. Abstraction: Class Class - a weakness that is ...'. The interface also includes navigation links like 'All Weaknesses (944 total)', 'Top-N Lists', 'Search CWE', 'View CWEs by' (with buttons for Software Development, Hardware Design, All Weaknesses, and Other Select Options), 'CWE REST API', and 'Quick Start'. A sidebar on the right contains links for News, Podcast, and Community Development.

1. Recherche “SMB” dans CWE Mitre

En cherchant “SMB” sur le site CWE Mitre, on trouve plusieurs faiblesses associées au protocole Server Message Block (SMB).

Vulnérabilités courantes liées à SMB

Voici les plus fréquentes que j’ai trouvé :

- CWE-20 – Improper Input Validation (exploitation via paquets SMB malformés)
- CWE-200 – Exposure of Sensitive Information (ex : fuite d’infos via SMBv1)
- CWE-287 – Improper Authentication (authentification faible ou désactivée)

- CWE-522 – Insufficiently Protected Credentials
(mots de passe envoyés en clair)
- CWE-611 – Improper Restriction of XML External Entity (si utilisé)
- CWE-693 – Protection Mechanism Failure
(mécanismes de sécurité insuffisants : SMBv1, NTLMv1)

Les exemple de vulnérabilité sélectionnée : CWE-287 – Improper Authentication

Description courte :

Le service SMB n’applique pas correctement l’authentification, permettant à un attaquant d’accéder à des ressources sans fournir des identifiants valides.

Conséquences :

- Accès non autorisé
- Exfiltration de données
- Mouvement latéral

Exemples d’exploitation :

- SMB avec authentification nulle activée
- Partages accessibles à “Everyone”
- Weak NTLM authentication

1.2 Recherche dans la base CVE – Exemple : CVE-2021-44228

The screenshot shows a web browser window displaying the CVE website search results for CVE-2021-44228. The browser tabs include 'CVE - Common Weakne...', 'CVE - CWE-693: Protecti...', and 'CVE - Common Vulnerabili...'. The address bar shows the URL 'www.cve.org/CVERecord/SearchResults?query=CVE-2021-44228'. The page header features the CVE logo and navigation links: 'About', 'Partner Information', 'Program Organization', 'Downloads', and 'Resources & Support'. A search bar contains the query 'CVE-2021-44228'. Below the header, a notice states: 'Expanded keyword searching of CVE Records (with limitations) is now available in the search box above. Learn more here.' The main content area is titled 'Search Results' and includes a section for 'CVE Record Found'. This section provides details for CVE-2021-44228, including the CNA (Apache Software Foundation) and a description of the vulnerability in Apache Log4j 2.0-beta9 through 2.15.0. The description notes that JNDI features used in configuration, log messages, and parameters do not protect against attacker-controlled LDAP and other JNDI-related endpoints. It also mentions that this behavior has been disabled by default from version 2.16.0 onwards. Below the description is a 'Show less' link. There is also an 'Other Results' section which includes all records that reference this CVE ID. At the bottom, it shows 'Showing 1 - 9 of 9 results for CVE-2021-44228'.

Quelques détails depuis CVE Mitre

- CVE ID : CVE-2021-44228
- Produit affecté : Apache Log4j2 versions 2.0-beta9 à 2.15.0
- Type de vulnérabilité : Remote Code Execution (RCE) via JNDI
- Cause :
Log4j ne protège pas correctement l'utilisation de JNDI dans la configuration, les messages et les paramètres.
- Exploit :
Un attaquant qui contrôle une donnée loguée peut injecter une chaîne du type :
- → Cela charge du code depuis un serveur LDAP malveillant → exécution de code à distance.
- **Corrections :**
 - 2.15.0 : JNDI désactivé par défaut
 - 2.16.0+ : fonctionnalité supprimée
 - Versions maintenues corrigées : 2.12.2, 2.12.3, 2.3.1

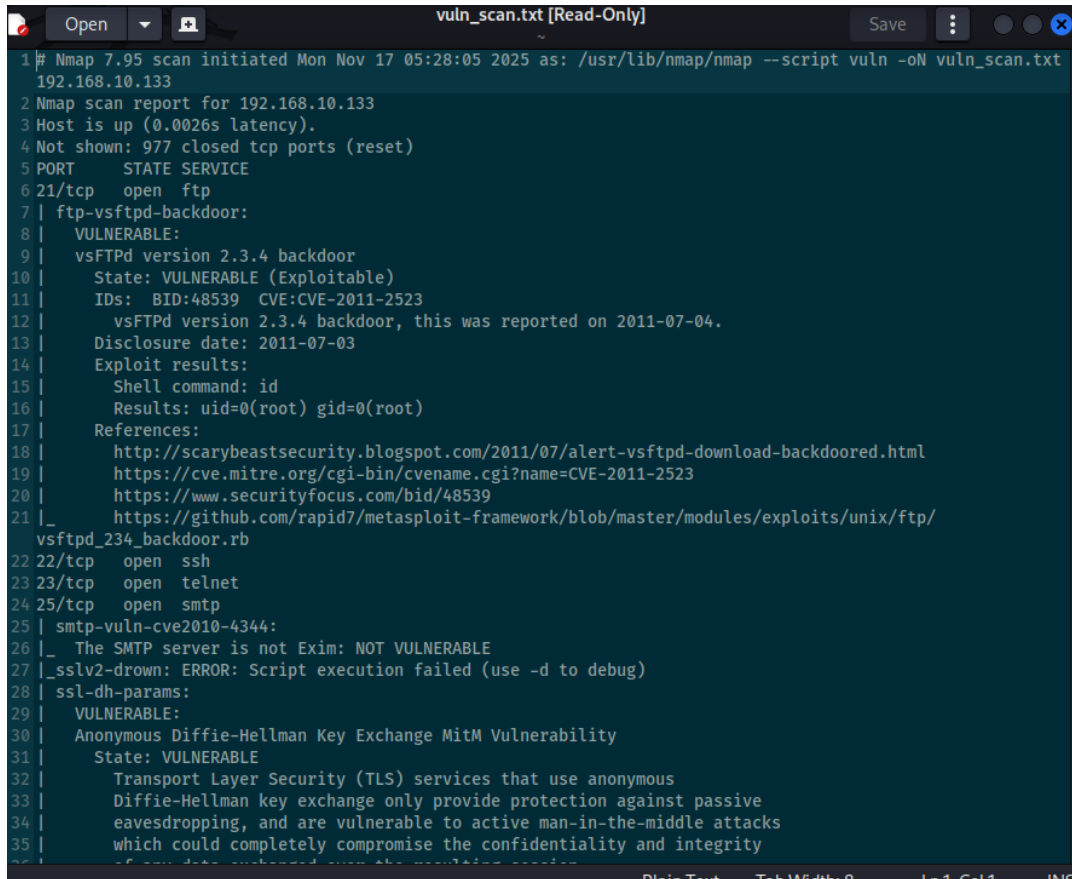
Comparaison avec NVD (NIST)

Sur NVD, les informations sont similaires mais plus détaillées :

- Score CVSS v3.1 : 10.0 (critique)
- Impact :
 - RCE complète
 - Confidentialité/Intégrité/Disponibilité : compromises totalement
- Vecteur d'attaque :
 - Network
 - Complexité faible
 - Pas d'authentification nécessaire

1- Analyse des résultats et des services ouverts

```
Host is up (0.0026s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs:  BID:48539  CVE:CVE-2011-2523
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   https://www.securityfocus.com/bid/48539
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
|_ sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|   State: VULNERABLE
|   Transport Layer Security (TLS) services that use anonymous
|   Diffie-Hellman key exchange only provide protection against passive
```



```
vuln_scan.txt [Read-Only]
Open Save
1 # Nmap 7.95 scan initiated Mon Nov 17 05:28:05 2025 as: /usr/lib/nmap/nmap --script vuln -oN vuln_scan.txt
2 192.168.10.133
3 Nmap scan report for 192.168.10.133
4 Host is up (0.0026s latency).
5 Not shown: 977 closed tcp ports (reset)
6 PORT      STATE SERVICE
7 | ftp-vsftpd-backdoor:
8 |   VULNERABLE:
9 |   vsFTPD version 2.3.4 backdoor
10 |   State: VULNERABLE (Exploitable)
11 |   IDs:  BID:48539  CVE:CVE-2011-2523
12 |   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
13 |   Disclosure date: 2011-07-03
14 |   Exploit results:
15 |   Shell command: id
16 |   Results: uid=0(root) gid=0(root)
17 |   References:
18 |   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
19 |   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
20 |   https://www.securityfocus.com/bid/48539
21 |_   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/
    vsftpd_234_backdoor.rb
22 22/tcp    open  ssh
23 23/tcp    open  telnet
24 25/tcp    open  smtp
25 | smtp-vuln-cve2010-4344:
26 |_ The SMTP server is not Exim: NOT VULNERABLE
27 |_ sslv2-drown: ERROR: Script execution failed (use -d to debug)
28 | ssl-dh-params:
29 |   VULNERABLE:
30 |   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
31 |   State: VULNERABLE
32 |   Transport Layer Security (TLS) services that use anonymous
33 |   Diffie-Hellman key exchange only provide protection against passive
34 |   eavesdropping, and are vulnerable to active man-in-the-middle attacks
35 |   which could completely compromise the confidentiality and integrity
36 |   of any data exchanged over the connection.
37 |_
38 |_
39 |_
40 |_
41 |_
42 |_
43 |_
44 |_
45 |_
46 |_
47 |_
48 |_
49 |_
50 |_
51 |_
52 |_
53 |_
54 |_
55 |_
56 |_
57 |_
58 |_
59 |_
60 |_
61 |_
62 |_
63 |_
64 |_
65 |_
66 |_
67 |_
68 |_
69 |_
70 |_
71 |_
72 |_
73 |_
74 |_
75 |_
76 |_
77 |_
78 |_
79 |_
80 |_
81 |_
82 |_
83 |_
84 |_
85 |_
86 |_
87 |_
88 |_
89 |_
90 |_
91 |_
92 |_
93 |_
94 |_
95 |_
96 |_
97 |_
98 |_
99 |_
100 |_
101 |_
102 |_
103 |_
104 |_
105 |_
106 |_
107 |_
108 |_
109 |_
110 |_
111 |_
112 |_
113 |_
114 |_
115 |_
116 |_
117 |_
118 |_
119 |_
120 |_
121 |_
122 |_
123 |_
124 |_
125 |_
126 |_
127 |_
128 |_
129 |_
130 |_
131 |_
132 |_
133 |_
134 |_
135 |_
136 |_
137 |_
138 |_
139 |_
140 |_
141 |_
142 |_
143 |_
144 |_
145 |_
146 |_
147 |_
148 |_
149 |_
150 |_
151 |_
152 |_
153 |_
154 |_
155 |_
156 |_
157 |_
158 |_
159 |_
160 |_
161 |_
162 |_
163 |_
164 |_
165 |_
166 |_
167 |_
168 |_
169 |_
170 |_
171 |_
172 |_
173 |_
174 |_
175 |_
176 |_
177 |_
178 |_
179 |_
180 |_
181 |_
182 |_
183 |_
184 |_
185 |_
186 |_
187 |_
188 |_
189 |_
190 |_
191 |_
192 |_
193 |_
194 |_
195 |_
196 |_
197 |_
198 |_
199 |_
200 |_
201 |_
202 |_
203 |_
204 |_
205 |_
206 |_
207 |_
208 |_
209 |_
210 |_
211 |_
212 |_
213 |_
214 |_
215 |_
216 |_
217 |_
218 |_
219 |_
220 |_
221 |_
222 |_
223 |_
224 |_
225 |_
226 |_
227 |_
228 |_
229 |_
230 |_
231 |_
232 |_
233 |_
234 |_
235 |_
236 |_
237 |_
238 |_
239 |_
240 |_
241 |_
242 |_
243 |_
244 |_
245 |_
246 |_
247 |_
248 |_
249 |_
250 |_
251 |_
252 |_
253 |_
254 |_
255 |_
256 |_
257 |_
258 |_
259 |_
260 |_
261 |_
262 |_
263 |_
264 |_
265 |_
266 |_
267 |_
268 |_
269 |_
270 |_
271 |_
272 |_
273 |_
274 |_
275 |_
276 |_
277 |_
278 |_
279 |_
280 |_
281 |_
282 |_
283 |_
284 |_
285 |_
286 |_
287 |_
288 |_
289 |_
290 |_
291 |_
292 |_
293 |_
294 |_
295 |_
296 |_
297 |_
298 |_
299 |_
300 |_
301 |_
302 |_
303 |_
304 |_
305 |_
306 |_
307 |_
308 |_
309 |_
310 |_
311 |_
312 |_
313 |_
314 |_
315 |_
316 |_
317 |_
318 |_
319 |_
320 |_
321 |_
322 |_
323 |_
324 |_
325 |_
326 |_
327 |_
328 |_
329 |_
330 |_
331 |_
332 |_
333 |_
334 |_
335 |_
336 |_
337 |_
338 |_
339 |_
340 |_
341 |_
342 |_
343 |_
344 |_
345 |_
346 |_
347 |_
348 |_
349 |_
350 |_
351 |_
352 |_
353 |_
354 |_
355 |_
356 |_
357 |_
358 |_
359 |_
360 |_
361 |_
362 |_
363 |_
364 |_
365 |_
366 |_
367 |_
368 |_
369 |_
370 |_
371 |_
372 |_
373 |_
374 |_
375 |_
376 |_
377 |_
378 |_
379 |_
380 |_
381 |_
382 |_
383 |_
384 |_
385 |_
386 |_
387 |_
388 |_
389 |_
390 |_
391 |_
392 |_
393 |_
394 |_
395 |_
396 |_
397 |_
398 |_
399 |_
400 |_
401 |_
402 |_
403 |_
404 |_
405 |_
406 |_
407 |_
408 |_
409 |_
410 |_
411 |_
412 |_
413 |_
414 |_
415 |_
416 |_
417 |_
418 |_
419 |_
420 |_
421 |_
422 |_
423 |_
424 |_
425 |_
426 |_
427 |_
428 |_
429 |_
430 |_
431 |_
432 |_
433 |_
434 |_
435 |_
436 |_
437 |_
438 |_
439 |_
440 |_
441 |_
442 |_
443 |_
444 |_
445 |_
446 |_
447 |_
448 |_
449 |_
450 |_
451 |_
452 |_
453 |_
454 |_
455 |_
456 |_
457 |_
458 |_
459 |_
460 |_
461 |_
462 |_
463 |_
464 |_
465 |_
466 |_
467 |_
468 |_
469 |_
470 |_
471 |_
472 |_
473 |_
474 |_
475 |_
476 |_
477 |_
478 |_
479 |_
480 |_
481 |_
482 |_
483 |_
484 |_
485 |_
486 |_
487 |_
488 |_
489 |_
490 |_
491 |_
492 |_
493 |_
494 |_
495 |_
496 |_
497 |_
498 |_
499 |_
500 |_
501 |_
502 |_
503 |_
504 |_
505 |_
506 |_
507 |_
508 |_
509 |_
510 |_
511 |_
512 |_
513 |_
514 |_
515 |_
516 |_
517 |_
518 |_
519 |_
520 |_
521 |_
522 |_
523 |_
524 |_
525 |_
526 |_
527 |_
528 |_
529 |_
530 |_
531 |_
532 |_
533 |_
534 |_
535 |_
536 |_
537 |_
538 |_
539 |_
540 |_
541 |_
542 |_
543 |_
544 |_
545 |_
546 |_
547 |_
548 |_
549 |_
550 |_
551 |_
552 |_
553 |_
554 |_
555 |_
556 |_
557 |_
558 |_
559 |_
560 |_
561 |_
562 |_
563 |_
564 |_
565 |_
566 |_
567 |_
568 |_
569 |_
570 |_
571 |_
572 |_
573 |_
574 |_
575 |_
576 |_
577 |_
578 |_
579 |_
580 |_
581 |_
582 |_
583 |_
584 |_
585 |_
586 |_
587 |_
588 |_
589 |_
590 |_
591 |_
592 |_
593 |_
594 |_
595 |_
596 |_
597 |_
598 |_
599 |_
600 |_
601 |_
602 |_
603 |_
604 |_
605 |_
606 |_
607 |_
608 |_
609 |_
610 |_
611 |_
612 |_
613 |_
614 |_
615 |_
616 |_
617 |_
618 |_
619 |_
620 |_
621 |_
622 |_
623 |_
624 |_
625 |_
626 |_
627 |_
628 |_
629 |_
630 |_
631 |_
632 |_
633 |_
634 |_
635 |_
636 |_
637 |_
638 |_
639 |_
640 |_
641 |_
642 |_
643 |_
644 |_
645 |_
646 |_
647 |_
648 |_
649 |_
650 |_
651 |_
652 |_
653 |_
654 |_
655 |_
656 |_
657 |_
658 |_
659 |_
660 |_
661 |_
662 |_
663 |_
664 |_
665 |_
666 |_
667 |_
668 |_
669 |_
670 |_
671 |_
672 |_
673 |_
674 |_
675 |_
676 |_
677 |_
678 |_
679 |_
680 |_
681 |_
682 |_
683 |_
684 |_
685 |_
686 |_
687 |_
688 |_
689 |_
690 |_
691 |_
692 |_
693 |_
694 |_
695 |_
696 |_
697 |_
698 |_
699 |_
700 |_
701 |_
702 |_
703 |_
704 |_
705 |_
706 |_
707 |_
708 |_
709 |_
710 |_
711 |_
712 |_
713 |_
714 |_
715 |_
716 |_
717 |_
718 |_
719 |_
720 |_
721 |_
722 |_
723 |_
724 |_
725 |_
726 |_
727 |_
728 |_
729 |_
730 |_
731 |_
732 |_
733 |_
734 |_
735 |_
736 |_
737 |_
738 |_
739 |_
740 |_
741 |_
742 |_
743 |_
744 |_
745 |_
746 |_
747 |_
748 |_
749 |_
750 |_
751 |_
752 |_
753 |_
754 |_
755 |_
756 |_
757 |_
758 |_
759 |_
760 |_
761 |_
762 |_
763 |_
764 |_
765 |_
766 |_
767 |_
768 |_
769 |_
770 |_
771 |_
772 |_
773 |_
774 |_
775 |_
776 |_
777 |_
778 |_
779 |_
780 |_
781 |_
782 |_
783 |_
784 |_
785 |_
786 |_
787 |_
788 |_
789 |_
790 |_
791 |_
792 |_
793 |_
794 |_
795 |_
796 |_
797 |_
798 |_
799 |_
800 |_
801 |_
802 |_
803 |_
804 |_
805 |_
806 |_
807 |_
808 |_
809 |_
810 |_
811 |_
812 |_
813 |_
814 |_
815 |_
816 |_
817 |_
818 |_
819 |_
820 |_
821 |_
822 |_
823 |_
824 |_
825 |_
826 |_
827 |_
828 |_
829 |_
830 |_
831 |_
832 |_
833 |_
834 |_
835 |_
836 |_
837 |_
838 |_
839 |_
840 |_
841 |_
842 |_
843 |_
844 |_
845 |_
846 |_
847 |_
848 |_
849 |_
850 |_
851 |_
852 |_
853 |_
854 |_
855 |_
856 |_
857 |_
858 |_
859 |_
860 |_
861 |_
862 |_
863 |_
864 |_
865 |_
866 |_
867 |_
868 |_
869 |_
870 |_
871 |_
872 |_
873 |_
874 |_
875 |_
876 |_
877 |_
878 |_
879 |_
880 |_
881 |_
882 |_
883 |_
884 |_
885 |_
886 |_
887 |_
888 |_
889 |_
890 |_
891 |_
892 |_
893 |_
894 |_
895 |_
896 |_
897 |_
898 |_
899 |_
900 |_
901 |_
902 |_
903 |_
904 |_
905 |_
906 |_
907 |_
908 |_
909 |_
910 |_
911 |_
912 |_
913 |_
914 |_
915 |_
916 |_
917 |_
918 |_
919 |_
920 |_
921 |_
922 |_
923 |_
924 |_
925 |_
926 |_
927 |_
928 |_
929 |_
930 |_
931 |_
932 |_
933 |_
934 |_
935 |_
936 |_
937 |_
938 |_
939 |_
940 |_
941 |_
942 |_
943 |_
944 |_
945 |_
946 |_
947 |_
948 |_
949 |_
950 |_
951 |_
952 |_
953 |_
954 |_
955 |_
956 |_
957 |_
958 |_
959 |_
960 |_
961 |_
962 |_
963 |_
964 |_
965 |_
966 |_
967 |_
968 |_
969 |_
970 |_
971 |_
972 |_
973 |_
974 |_
975 |_
976 |_
977 |_
978 |_
979 |_
980 |_
981 |_
982 |_
983 |_
984 |_
985 |_
986 |_
987 |_
988 |_
989 |_
990 |_
991 |_
992 |_
993 |_
994 |_
995 |_
996 |_
997 |_
998 |_
999 |_
1000 |_
1001 |_
1002 |_
1003 |_
1004 |_
1005 |_
1006 |_
1007 |_
1008 |_
1009 |_
1010 |_
1011 |_
1012 |_
1013 |_
1014 |_
1015 |_
1016 |_
1017 |_
1018 |_
1019 |_
1020 |_
1021 |_
1022 |_
1023 |_
1024 |_
1025 |_
1026 |_
1027 |_
1028 |_
1029 |_
1030 |_
1031 |_
1032 |_
1033 |_
1034 |_
1035 |_
1036 |_
1037 |_
1038 |_
1039 |_
1040 |_
1041 |_
1042 |_
1043 |_
1044 |_
1045 |_
1046 |_
1047 |_
1048 |_
1049 |_
1050 |_
1051 |_
1052 |_
1053 |_
1054 |_
1055 |_
1056 |_
1057 |_
1058 |_
1059 |_
1060 |_
1061 |_
1062 |_
1063 |_
1064 |_
1065 |_
1066 |_
1067 |_
1068 |_
1069 |_
1070 |_
1071 |_
1072 |_
1073 |_
1074 |_
1075 |_
1076 |_
1077 |_
1078 |_
1079 |_
1080 |_
1081 |_
1082 |_
1083 |_
1084 |_
1085 |_
1086 |_
1087 |_
1088 |_
1089 |_
1090 |_
1091 |_
1092 |_
1093 |_
1094 |_
1095 |_
1096 |_
1097 |_
1098 |_
1099 |_
1100 |_
1101 |_
1102 |_
1103 |_
1104 |_
1105 |_
1106 |_
1107 |_
1108 |_
1109 |_
1110 |_
1111 |_
1112 |_
1113 |_
1114 |_
1115 |_
1116 |_
1117 |_
1118 |_
1119 |_
1120 |_
1121 |_
1122 |_
1123 |_
1124 |_
1125 |_
1126 |_
1127 |_
1128 |_
1129 |_
1130 |_
1131 |_
1132 |_
1133 |_
1134 |_
1135 |_
1136 |_
1137 |_
1138 |_
1139 |_
1140 |_
1141 |_
1142 |_
1143 |_
1144 |_
1145 |_
1146 |_
1147 |_
1148 |_
1149 |_
1150 |_
1151 |_
1152 |_
1153 |_
1154 |_
1155 |_
1156 |_
1157 |_
1158 |_
1159 |_
1160 |_
1161 |_
1162 |_
1163 |_
1164 |_
1165 |_
1166 |_
1167 |_
1168 |_
1169 |_
1170 |_
1171 |_
1172 |_
1173 |_
1174 |_
1175 |_
1176 |_
1177 |_
1178 |_
1179 |_
1180 |_
1181 |_
1182 |_
1183 |_
1184 |_
1185 |_
1186 |_
1187 |_
1188 |_
1189 |_
1190 |_
1191 |_
1192 |_
1193 |_
1194 |_
1195 |_
1196 |_
1197 |_
1198 |_
1199 |_
1200 |_
1201 |_
1202 |_
1203 |_
1204 |_
1205 |_
1206 |_
1207 |_
1208 |_
1209 |_
1210 |_
1211 |_
1212 |_
1213 |_
1214 |_
1215 |_
1216 |_
1217 |_
1218 |_
1219 |_
1220 |_
1221 |_
1222 |_
1223 |_
1224 |_
1225 |_
1226 |_
1227 |_
1228 |_
1229 |_
1230 |_
1231 |_
1232 |_
1233 |_
1234 |_
1235 |_
1236 |_
1237 |_
1238 |_
1239 |_
1240 |_
1241 |_
1242 |_
1243 |_
1244 |_
1245 |_
1246 |_
1247 |_
1248 |_
1249 |_
1250 |_
1251 |_
1252 |_
1253 |_
1254 |_
1255 |_
1256 |_
1257 |_
1258 |_
1259 |_
1260 |_
1261 |_
1262 |_
1263 |_
1264 |_
1265 |_
1266 |_
1267 |_
1268 |_
1269 |_
1270 |_
1271 |_
1272 |_
1273 |_
1274 |_
1275 |_
1276 |_
1277 |_
1278 |_
1279 |_
1280 |_
1281 |_
1282 |_
1283 |_
1284 |_
1285 |_
1286 |_
1287 |_
1288 |_
1289 |_
1290 |_
1291 |_
1292 |_
1293 |_
1294 |_
1295 |_
1296 |_
1297 |_
1298 |_
1299 |_
1300 |_
1301 |_
1302 |_
1303 |_
1304 |_
1305 |_
1306 |_
1307 |_
1308 |_
1309 |_
1310 |_
1311 |_
1312 |_
1313 |_
1314 |_
1315 |_
1316 |_
1317 |_
1318 |_
1319 |_
1320 |_
1321 |_
1322 |_
1323 |_
1324 |_
1325 |_
1326 |_
1327 |_
1328 |_
1329 |_
1330 |_
1331 |_
1332 |_
1333 |_
1334 |_
1335 |_
1336 |_
1337 |_
1338 |_
1339 |_
1340 |_
1341 |_
1342 |_
1343 |_
1344 |_
1345 |_
1346 |_
1347 |_
1348 |_
1349 |_
1350 |_
1351 |_
1352 |_
1353 |_
1354 |_
1355 |_
1356 |_
1357 |_
1358 |_
1359 |_
1360 |_
1361 |_
1362 |_
1363 |_
1364 |_
1365 |_
1366 |_
1367 |_
1368 |_
1369 |_
1370 |_
1371 |_
1372 |_
1373 |_
1374 |_
1375 |_
1376 |_
1377 |_
1378 |_
1379 |_
1380 |_
1381 |_
1382 |_
1383 |_
1384 |_
1385 |_
1386 |_
1387 |_
1388 |_
1389 |_
1390 |_
1391 |_
1392 |_
1393 |_
1394 |_
1395 |_
1396 |_
1397 |_
1398 |_
1399 |_
1400 |_
1401 |_
1402 |_
1403 |_
1404 |_
1405 |_
1406 |_
1407 |_
1408 |_
1409 |_
1410 |_
1411 |_
1412 |_
1413 |_
1414 |_
1415 |_
1416 |_
1417 |_
1418 |_
1419 |_
1420 |_
1421 |_
1422 |_
1423 |_
1424 |_
1425 |_
1426 |_
1427 |_
1428 |_
1429 |_
1430 |_
1431 |_
1432 |_
1433 |_
1434 |_
1435 |_
1436 |_
1437 |_
1438 |_
1439 |_
1440 |_
1441 |_
1442 |_
1443 |_
1444 |_
1445 |_
1446 |_
1447 |_
1448 |_
1449 |_
1450 |_
1451 |_
1452 |_
1453 |_
1454 |_
1455 |_
1456 |_
1457 |_
1458 |_
1459 |_
1460 |_
1461 |_
1462 |_
1463 |_
1464 |_
1465 |_
1466 |_
1467 |_
1468 |_
1469 |_
1470 |_
1471 |_
1472 |_
1473 |_
1474 |_
1475 |_
1476 |_
1477 |_
1478 |_
1479 |_
1480 |_
1481 |_
1482 |_
1483 |_
1484 |_
1485 |_
1486 |_
1487 |_
1488 |_
1489 |_
1490 |_
1491 |_
1492 |_
1493 |_
1494 |_
1495 |_
1496 |_
1497 |_
1498 |_
1499 |_
1500 |_
1501 |_
1502 |_
1503 |_
1504 |_
1505 |_
1506 |_
1507 |_
1508 |_
1509 |_
1510 |_
1511 |_
1512 |_
1513 |_
1514 |_
1515 |_
1516 |_
1517 |_
1518 |_
1519 |_
1520 |_
1521 |_
1522 |_
1523 |_
1524 |_
1525 |_
1526 |_
1527 |_
1528 |_
1529 |_
1530 |_
1531 |_
1532 |_
1533 |_
1534 |_
1535 |_
1536 |_
1537 |_
1538 |_
1539 |_
1540 |_
1541 |_
1542 |_
1543 |_
1544 |_
1545 |_
1546 |_
1547 |_
1548 |_
1549 |_
1550 |_
1551 |_
1552 |_
1553 |_
1554 |_
1555 |_
1556 |_
1557 |_
1558 |_
1559 |_
1560 |_
1561 |_
1562 |_
1563 |_
1564 |_
1565 |_
1566 |_
1567 |_
1568 |_
1569 |_
1570 |_
1571 |_
1572 |_
1573 |_
1574 |_
1575 |_
1576 |_
1577 |_
1578 |_
1579 |_
1580 |_
1581 |_
1582 |_
1583 |_
1584 |_
1585 |_
1586 |_
1587 |_
1588 |_
1589 |_
1590 |_
1591 |_
1592 |_
1593 |_
1594 |_
1595 |_
1596 |_
1597 |_
1598 |_
1599 |_
1600 |_
1601 |_
1602 |_
1603 |_
1604 |_
1605 |_
1606 |_
1607 |_
1608 |_
1609 |_
1610 |_
1611 |_
1612 |_
1613 |_
1614 |_
1615 |_
1616 |_
1617 |_
1618 |_
1619 |_
1620 |_
1621 |_
1622 |_
1623 |_
1624 |_
1625 |_
1626 |_
1627 |_
1628 |_
1629 |_
1630 |_
1631 |_
1632 |_
1633 |_
1634 |_
1635 |_
1636 |_
1637 |_
1638 |_
1639 |_
1640 |_
1641 |_
1642 |_
1643 |_
1644 |_
1645 |_
1646 |_
1647 |_
1648 |_
1649 |_
1650 |_
1651 |_
1652 |_
1653 |_
1654 |_
1655 |_
1656 |_
1657 |_
1658 |_
1659 |_
1660 |_
1661 |_
1662 |_
1663 |_
1664 |_
1665 |_
1666 |_
1667 |_
1668 |_
1669 |_
1670 |_
1671 |_
1672 |_
1673 |_
1674 |_
1675 |_
1676 |_
1677 |_
1678 |_
1679 |_
1680 |_
1681 |_
1682 |_
1683 |_
1684 |_
1685 |_
1686 |_
1687 |_
1688 |_
1689 |_
1690 |_
1691 |_
1692 |_
1693 |_
1694 |_
1695 |_
1696 |_
1697 |_
1698 |_
1699 |_
1700 |_
1701 |_
1702 |_
1703 |_
1704 |_
1705 |_
1706 |_
1707 |_
1708 |_
1709 |_
1710 |_
1711 |_
1712 |_
1713 |_
1714 |_
1715 |_
1716 |_
1717 |_
1718 |_
1719 |_
1720 |_
1721 |_
1722 |_
1723 |_
1724 |_
1725 |_
1726 |_
1727 |_
1728 |_
1729 |_
1730 |_
1731 |_
1732 |_
1733 |_
1734 |_
1735 |_
1736 |_
1737 |_
1738 |_
1739 |_
1740 |_
1741 |_
1742 |_
1743 |_
1744 |_
1745 |_
1746 |_
1747 |_
1748 |_
1749 |_
1750 |_
1751 |_
1752 |_
1753 |_
1754 |_
1755 |_
1756 |_
1757 |_
1758 |_
17
```

Étape 2 : Détection automatique de vulnérabilités Nmap

```
(root@kali) ~/home/kali
# nikto -h http://192.168.10.133
Nikto v2.5.0

-----
Target IP:      192.168.10.133
Target Hostname: 192.168.10.133
Target Port:    80
Start Time:    2025-11-17 05:43:44 (GMT-5)
-----

Server: Apache/2.2.8 (Ubuntu) DAV/2
/: Retrieved X-powered-by header: PHP/5.2.4-2ubuntu5.10.
/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
/index: Uncommon header 'tcn' found, with contents: list.
/index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
/: Web Server returns a valid response with junk HTTP methods which may cause false positives.
/: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
/phpinfo.php: Output from the phpinfo() function was found.
/doc/: Directory indexing found.
/doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-2184
/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-2184
/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-2184
/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-2184
```

2- Voici les vulnérabilités Nikto + leurs CVE typiques :

| Vulnérabilité Nikto | Description | CVE associé |
|------------------------------------|---|---|
| Apache 2.2.8 obsolète | Version non maintenue pouvant contenir de multiples failles | CVE-2011-3192, CVE-2010-1452, etc. |
| PHP 5.2.4 exposé | Version vulnérable à RCE et LFI | CVE-2007-4887, CVE-2007-3996 |
| phpinfo() accessible | Fuite d'infos sensibles | CVE-2007-0405 |
| Directory listing activé | Exposition de fichiers | Non spécifique (faiblesse configuration) |
| TRACE method activé | Vulnérable à XST | CVE-2004-2763 |
| PHP Easter Eggs (PHPE9568F36...) | Fuite d'infos PHP | OSVDB-12184 |
| phpMyAdmin accessible publiquement | Fuite d'infos, brute force | CVE-2009-1151, CVE-2012-5159 |

Exemples d'exploits trouvés :

| CVE | Exploit disponible | Type |
|---------------|--------------------|------------------------|
| CVE-2011-3192 | Oui | DoS Apache |
| CVE-2007-4887 | Oui | RCE PHP |
| CVE-2009-1151 | Oui | Auth bypass phpMyAdmin |

3. Niveau de criticité (CVSS)

| CVE | Score CVSS | Criticité |
|---------------|------------|-----------|
| CVE-2011-3192 | 7.8 | High |
| CVE-2007-4887 | 10.0 | Critical |
| CVE-2009-1151 | 7.5 | High |
| CVE-2004-2763 | 4.3 | Medium |

4. Mesures correctives

- Mettre à jour **Apache** (≥ 2.4).
- Mettre à jour **PHP** ($\geq 8.x$).
- Désactiver la méthode **TRACE** :
- Supprimer **phpinfo.php**.
- Restreindre l'accès à **phpMyAdmin** (pare-feu + authentification).
- Désactiver **directory listing** (Options -Indexes).
- Désactiver **MultiViews** pour éviter les bruteforce de fichiers.
- Ajouter des en-têtes de sécurité (X-Frame-Options, X-Content-Type-Options).

PARTIE 3 – NESSUS

1- Téléchargement de Nessus pour Kali

2- Installation de Nessus

```
(root@kali)-[~/Downloads]
└─# ls
Nessus-10.11.0-debian10_amd64.deb  Nessus-10.11.0-ubuntu1604_amd64.deb
Nessus-10.11.0-ubuntu1604_amd64

(root@kali)-[~/Downloads]
└─# sudo dpkg -i Nessus-10.11.0-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 417367 files and directories currently installed.)
Preparing to unpack Nessus-10.11.0-debian10_amd64.deb ...
Unpacking nessus (10.11.0) ...
Setting up nessus (10.11.0) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
```

Une fois installer on va démarrer Nessus.

3- Démarrage de Nessus

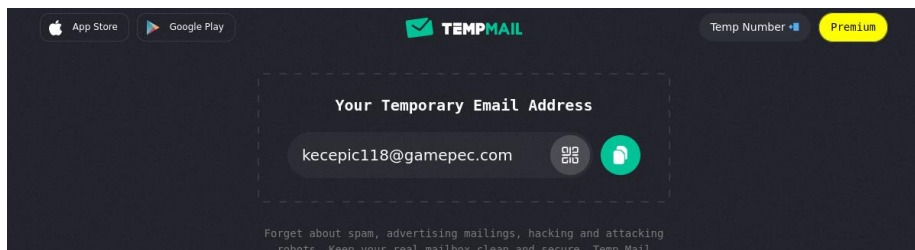
```
(root@kali)-[~/home/kali/Downloads]
└─# sudo systemctl start nessusd

(root@kali)-[~/home/kali/Downloads]
└─# sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disab
   Active: active (running) since Sat 2025-11-22 12:40:06 EST; 25s ago
   Invocation: ed6bb740fa804606ba527340d269254f
   Main PID: 32940 (nessus-service)
     Tasks: 16 (limit: 2197)
    Memory: 171.2M (peak: 200.2M)
       CPU: 25.147s
    CGroup: /system.slice/nessusd.service
           └─32940 /opt/nessus/sbin/nessus-service -q
             └─32949 nessusd -q
```

2.2 Création d'un Scan avec Nessus

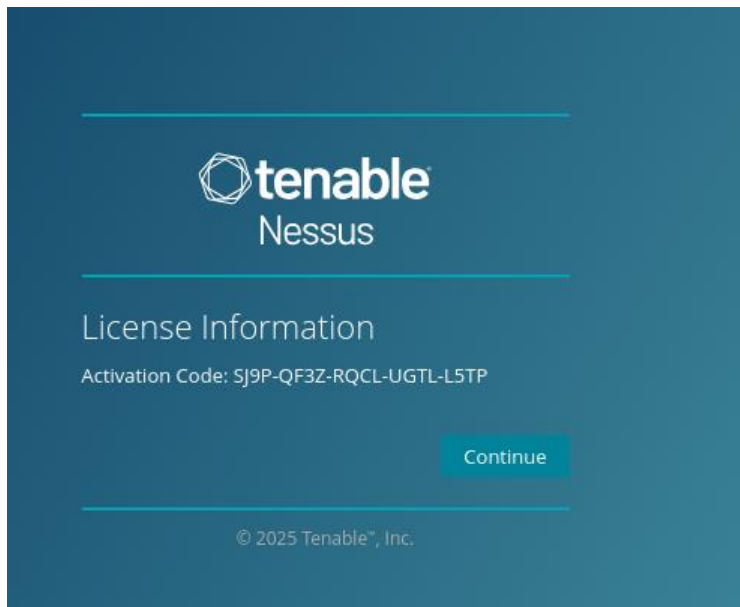
2.1. Se connecter à Nessus.

⇒ Ici, on va récupérer une adresse email professionnel sur le site temp email :

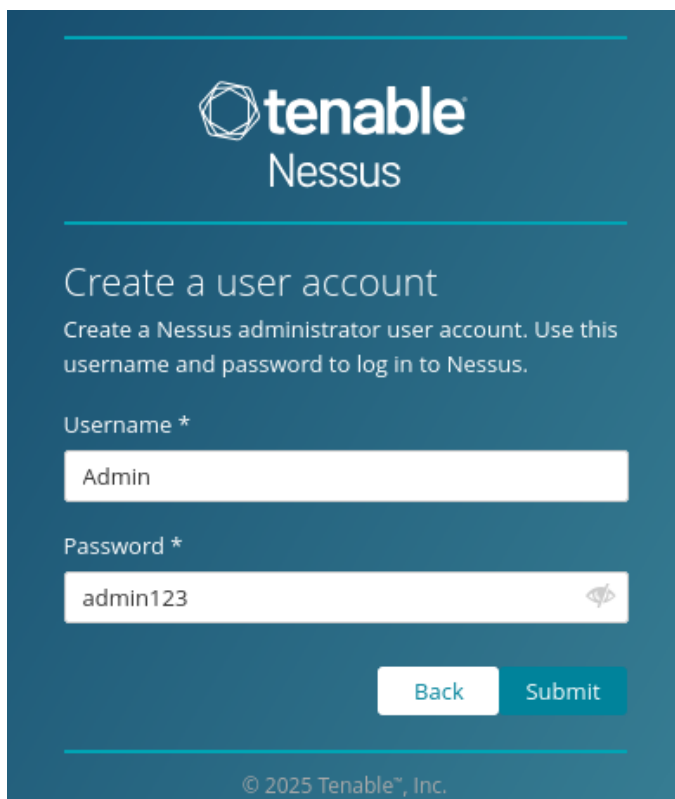


Tel est l'adresse email qu'on va utiliser pour se connecter.

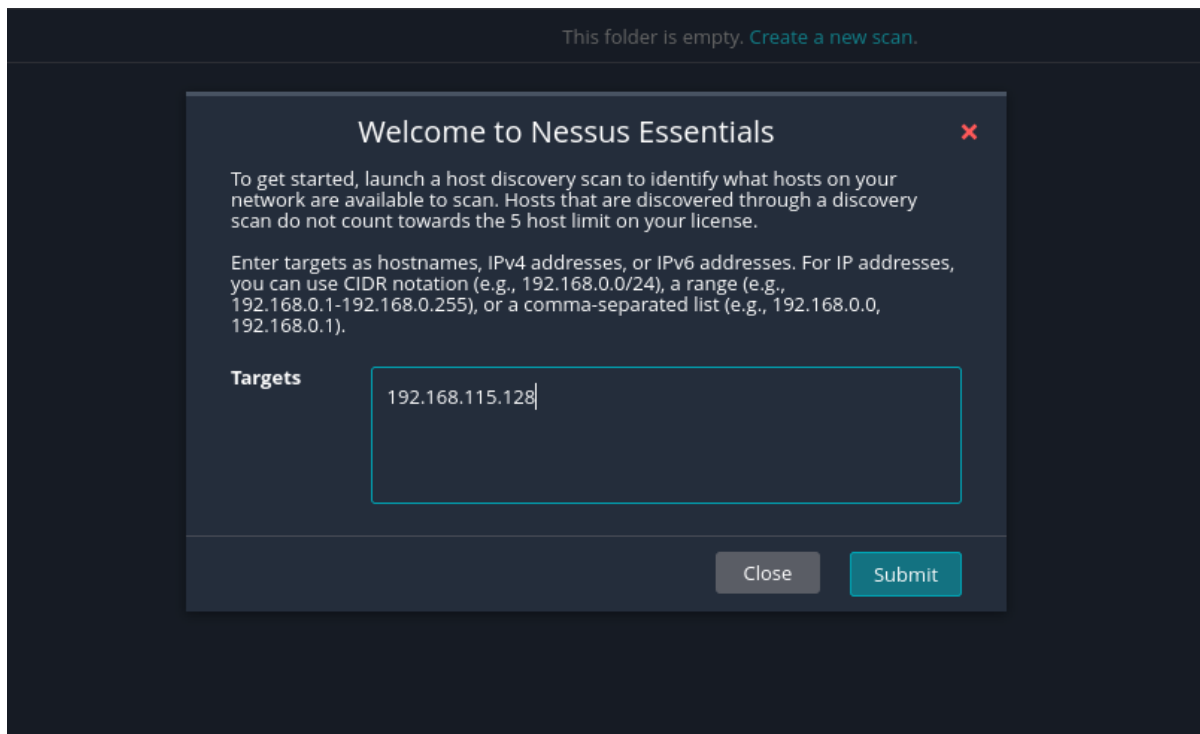
Ici, on voit notre code d'activation



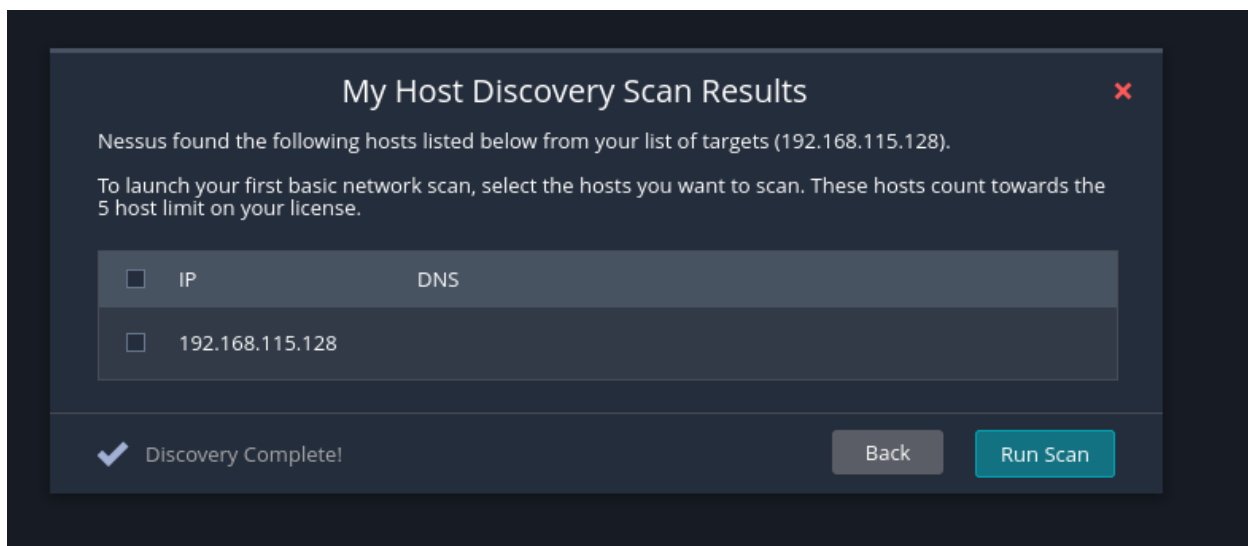
⇒ Ensuite, on donne les identifiants pour se connecter Nessus :



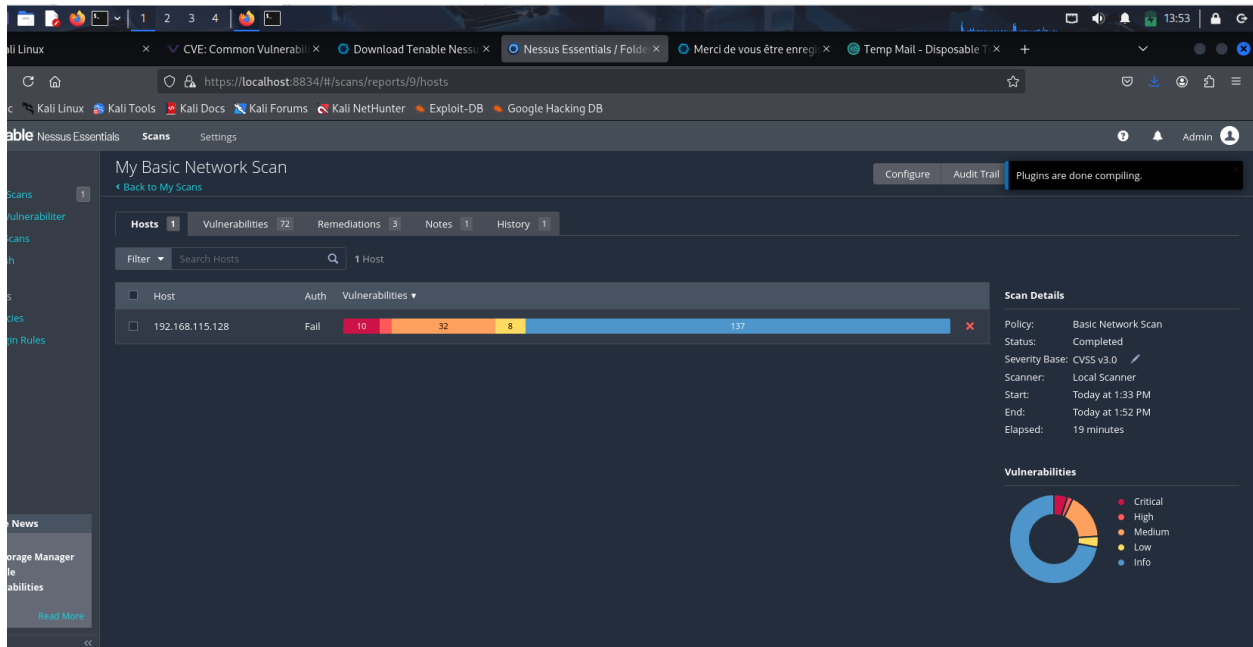
2.2. Créer un nouveau scan :



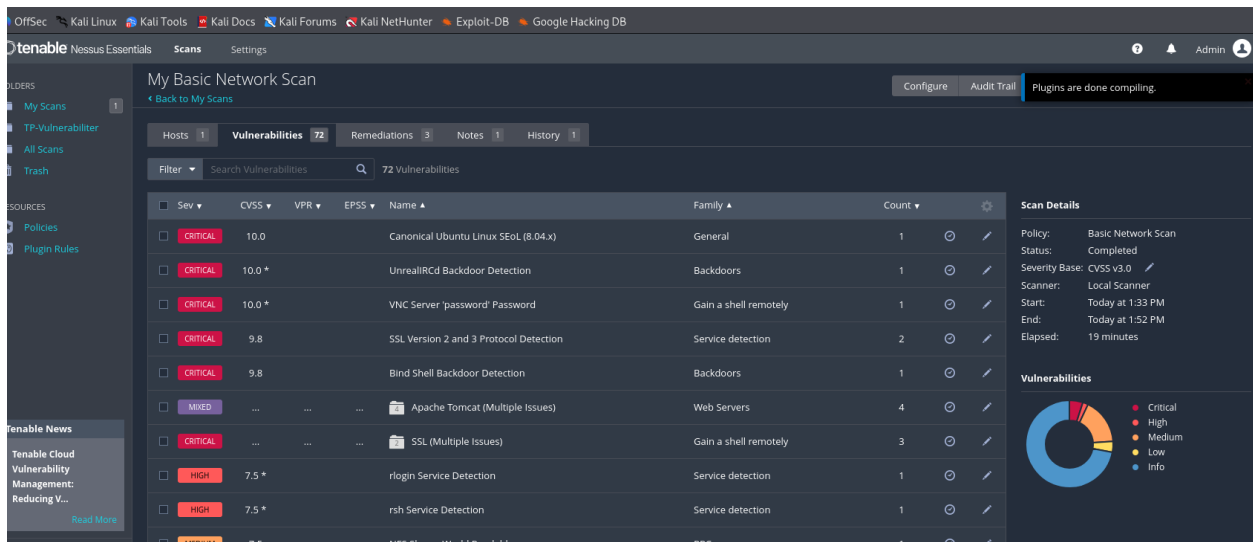
On sélection l'IP qu'on doit scanner et puis on run scan :



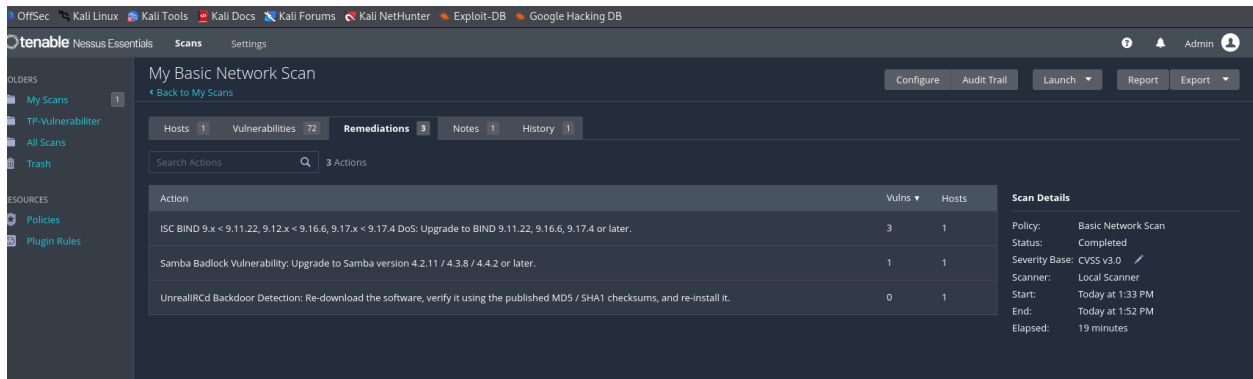
2.3 Analyse des Résultats



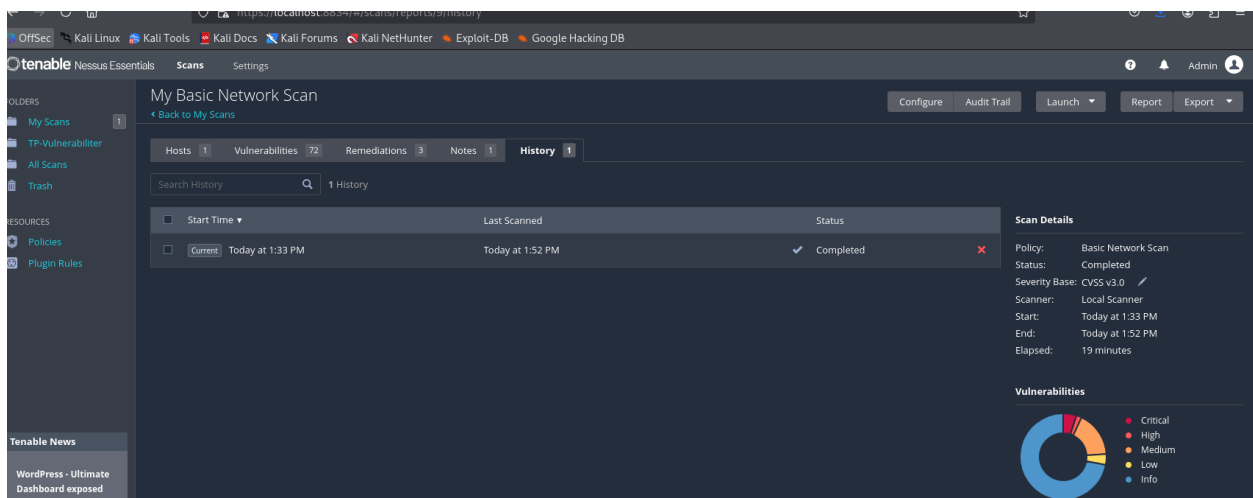
La page qui nous montre les vulnérabilités :



⇒ Remédiations :



⇒ History :



1. Une fois le scan terminé, ouvrez Scans, Complétez et commentez les résultats.

La machine analysée présente un grand nombre de vulnérabilités, dont plusieurs critiques, indiquant qu'il s'agit probablement d'un système volontairement vulnérable (comme Metasploitable). De nombreux services sont exposés et reposent sur des versions anciennes présentant des failles connues.

2. Analyse des résultats :

a. Vulnérabilités détectées

Le scan révèle dix vulnérabilités critiques susceptibles de permettre une exécution de code à distance (RCE) ou une compromission complète du système.

Trente-deux vulnérabilités de niveau élevé concernent principalement des services obsolètes comportant des failles connues.

Huit vulnérabilités de niveau moyen relèvent surtout de problèmes de configuration et de protocoles insuffisamment sécurisés.

b. Recommandations proposées

Nessus recommande avant tout la mise à jour des logiciels obsolètes, la désactivation des services non indispensables, l'application des correctifs de sécurité et le renforcement des protocoles de chiffrement.

Pour les vulnérabilités critiques, une mise à jour immédiate des composants concernés (Samba, FTP, Apache, SSH, etc.) est préconisée.

Conclusion :

Ce travail pratique a permis d'apprendre à identifier des vulnérabilités connues et à analyser une machine à l'aide d'outils tels que Nmap, Nikto et Nessus. Les résultats ont mis en évidence de nombreuses failles, dont certaines particulièrement graves. Cette analyse souligne l'importance de maintenir les systèmes à jour, d'appliquer les correctifs nécessaires et de sécuriser les ports ouverts.

En définitive, ce TP démontre que l'analyse de vulnérabilités constitue une étape essentielle pour prévenir les attaques et garantir la sécurité d'un système.