



HideZeroOne
INE – Cyber Sec
www.hide01.ir





Incident Handling & Response Professional

Logging

Section 04 | Module 02

v1

© Caendra Inc. 2019
All Rights Reserved

OUTLINE

Section 4 | Module 2: Logging

Table of Contents

► Learning Objectives

► 2.1 Windows Logging

▼ References

References

References

Table of Contents

Module 02 | Logging

2.1 Windows Logging

OUTLINE

Section 4 | Module 2: Logging

Table of Contents

► Learning Objectives

► 2.1 Windows Logging

▼ References

References

References

Learning Objectives

By the end of this module, you should have a better understanding of:

- ✓ Important Windows events
- ✓ Windows actionable logging strategies

OUTLINE

Section 4 | Module 2: Logging

Table of Contents

▼ Learning Objectives

Logging

► 2.1 Windows Logging

▼ References

References

References

Logging

As you can imagine, there will be no endpoint analytics without logs to query.

We will dedicate this module to talk about Windows logs as well as logging strategies.

```
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
```

OUTLINE

Section 4 | Module 2: Logging

Table of Contents

▼ Learning Objectives

Logging

► 2.1 Windows Logging

▼ References

References

References

IHRP

2.1

Windows Logging



OUTLINE

Section 4 | Module 2: Logging

Table of Contents

▼ Learning Objectives

Logging

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

► 2.1 Windows Logging

▼ References

References

2.1 Windows Logging

Modern Windows systems have great logging capabilities with minimum system impact.

Configuring actionable logging on Windows systems and aggregating these logs into a Security Information Event Management solution is of key importance, if an organization wants to perform effective endpoint analytics.

OUTLINE

Section 4 | Module 2: Logging

Table of Contents

▼ Learning Objectives

Logging

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▶ 2.1 Windows Logging

▼ References

References

2.1 Windows Logging

Windows endpoints store their logs in the `%SystemRoot%\System32\winevt\logs` directory in the binary XML Windows Event Logging format (.evtx files).

It should be noted that through log subscriptions logs can also be forwarded and stored to remote locations.

OUTLINE

Section 4 | Module 2: Logging

Table of Contents

▼ Learning Objectives

Logging

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▶ 2.1 Windows Logging

▼ References

References

2.1 Windows Logging

An analyst can find events being logged in the *Security*, *System* and *Application* event logs.

Additional logs can be found under *Applications and Services* logs inside Windows Event Viewer. The logs contained there may seem complicated, but take our word that they contain a treasure trove of information, since they are a lot more targeted.

OUTLINE

Section 4 | Module 2: Logging

Table of Contents

▼ Learning Objectives

Logging

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▶ 2.1 Windows Logging

▼ References

References

2.1 Windows Logging

We have already seen our fair share of Windows events. Let's now consolidate some important Windows events, that can result in some quick wins.

This way, you can use this module as a point of reference during your investigations.

OUTLINE

Section 4 | Module 2: Logging

Table of Contents

▼ Learning Objectives

Logging

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▼ 2.1 Windows Logging

▶ 2.1.1 Account Management Events

▶ 2.1.2 Account Logon and Logon Events

2.1.1 Account Management Events

Attackers are known for introducing or deleting users, as well as tampering with existing ones. The most important Account Management Events* are:

* If the endpoint is part of the domain the following events will be recorded on the Domain Controller

OUTLINE

Section 4 | Module 2: Logging

Table of Contents

▼ Learning Objectives

Logging

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▼ 2.1 Windows Logging

▼ 2.1.1 Account Management Events

2.1.1 Account Management Events

2.1.1 Account Management Events

Event ID	Description
4720	A user account was created
4722	A user account was enabled
4723	A user attempted to change an account's password
4724	An attempt was made to reset an account's password
4725	A user account was disabled
4726	A user account was deleted
4727	A security-enabled global group was created
4728	A member was added to a security-enabled global group
4729	A member was removed from a security-enabled global group
4730	A security-enabled global group was deleted
4731	A security-enabled local group was created
4732	A member was added to a security-enabled local group
4733	A member was removed from a security-enabled local group
4734	A security-enabled local group was deleted

Event ID	Description
4735	A security-enabled local group was changed
4737	A security-enabled global group was changed
4738	A user account was changed
4741	A computer account was created
4742	A computer account was changed
4743	A computer account was deleted
4754	A security-enabled universal group was created
4755	A security-enabled universal group was changed
4756	A member was added to a security-enabled universal group
4757	A member was removed from a security-enabled universal group
4758	A security-enabled universal group was deleted

OUTLINE

Section 4 | Module 2: Logging

Table of Contents

▼ Learning Objectives

Logging

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▼ 2.1 Windows Logging

▼ 2.1.1 Account Management Events

2.1.1 Account Management Events

2.1.2 Account Logon and Logon Events

When a user authenticates on a Windows endpoint an *Account Logon* event is recorded. Note that account logon events will be recorded in the Security event log of the system responsible for authentication the user.

When an account is accessing a resource a *Logon* event is recorded. Note that logon events will be recorded in the Security event log of the system being accessed.

OUTLINE

Table of Contents

▼ Learning Objectives

Logging

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▼ 2.1 Windows Logging

2.1.1 Account Management
Events

2.1.1 Account
Management Events

▼ 2.1.2 Account Logon and
Logon Events

2.1.2 Account Logon and Logon Events

As you can imagine, if you spot account logon events on a machine other than the Domain Controller, this is a sign of local user account usage.

Local user account usage is abnormal on domain environments and can indicate a compromise.

OUTLINE

▼ Learning Objectives

Logging

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▼ 2.1 Windows Logging

▼ 2.1.1 Account Management Events

2.1.1 Account Management Events

▼ 2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

While analyzing the Account Logon and Logon events on a Domain Controller keep an eye for the following Event IDs.

OUTLINE

Logging

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▼ 2.1 Windows Logging

▼ 2.1.1 Account Management Events

2.1.1 Account Management Events

▼ 2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

OUTLINE

▼ 2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▼ 2.1 Windows Logging

▼ 2.1.1 Account Management Events

2.1.1 Account Management Events

▼ 2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

In the case of remote logon the *Network Information* section will include additional data. Keep an eye on the *Keywords* field for failed attempts (or successful attempts during unusual hours). [Result Code](#) will contain additional data regarding the authentication failure.

OUTLINE

2.1 Windows Logging

2.1 Windows Logging

2.1 Windows Logging

▼ 2.1 Windows Logging

▼ 2.1.1 Account Management Events

2.1.1 Account Management Events

▼ 2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

Keep an eye on the *Keywords* field for failed attempts. *Result Code* will contain additional data regarding the authentication failure. You can use this to track a user's behavior.

OUTLINE

2.1 Windows Logging

2.1 Windows Logging

▼ 2.1 Windows Logging

▼ 2.1.1 Account Management Events

2.1.1 Account Management Events

▼ 2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

Result Code will contain additional data regarding the authentication failure.

OUTLINE

2.1 Windows Logging

▼ 2.1 Windows Logging

▼ 2.1.1 Account Management Events

2.1.1 Account Management Events

▼ 2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

It can uncover penetration testing tools that prefer authenticating using NTLM. Keep an eye on the *Keywords* field for failed attempts. In the case of remote logon the *Network Information* section will include additional data. *Error Code* will contain additional data regarding the authentication failure. High volumes of such events within a small time window with Error Code C000006A and a subsequent Error Code C0000234 may indicate password brute-forcing.

OUTLINE

- ▼ 2.1 Windows Logging
 - ▼ 2.1.1 Account Management Events
 - 2.1.1 Account Management Events
 - ▼ 2.1.2 Account Logon and Logon Events
 - 2.1.2 Account Logon and Logon Events
 - 2.1.2 Account Logon and Logon Events
 - 2.1.2 Account Logon and Logon Events
 - 2.1.2 Account Logon and Logon Events
 - 2.1.2 Account Logon and Logon Events
 - 2.1.2 Account Logon and Logon Events
 - 2.1.2 Account Logon and Logon Events
 - 2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

SMB relay attacks can be uncovered by correlating this event with associated EventIDs 4768, 4769 and 4776.

Keep an eye on the *Caller Process Name* and *Caller Process ID* fields to learn more about the process initiating the logon.

Also keep an eye on the included [Logon Type](#).

OUTLINE

▼ 2.1.1 Account Management Events

2.1.1 Account Management Events

▼ 2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

High volumes of such events may indicate password brute-forcing or password spraying. Refer to the Network Information section to map the remote host. Keep an eye for *Type 3* that may indicate RDP-based failed logons.

OUTLINE

EVENTS

2.1.1 Account Management Events

▼ 2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

You can correlate those with Event ID 4624 to detect abnormalities. More specifically, sessions that do not have an associated log off event.

OUTLINE

INTRODUCTION

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

This indicates a user attempting to use credentials that are different than the current logon session's ones.

From Twitter: If you see TERMSVR SPN in 4648 then it's an evidence of RDP activity from the source machine (operator must supply machine name while using *mstsc* or other RDP client, red team members always use IPv4 as Dst).

To get a list of IPs connected via RDP so far:
`Get-WinEvent -Log 'Microsoft-Windows-TerminalServices-LocalSessionManager/Operational' | select -exp Properties | where {$_.Value -like '*.*.*.*'} | sort Value -u`

OUTLINE

Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

This can indicate elevated access.

OUTLINE

LOGON EVENTS

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

Event ID	Description
4748	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4771	Kerberos pre-authentication failed
4776	The computer attempted to validate the credentials for an account
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4672	Special privileges assigned to new logon
4776	The computer attempted to validate the credentials for an account
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station

Can be an indicator of compromise since it is can be associated with the usage of NTLM and local user accounts.

OUTLINE

LOGON EVENTS

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

By configuring additional logging defenders can identify network share objects being accessed (Event ID **5140**), added (Event ID **5142**), modified (Event ID **5143**) and deleted (Event ID **5144**).

It should be noted that Event ID **5140** will contain source address and accessing account information. Unfortunately, information about specific files being accessed is not provided.

OUTLINE

- Logon Events
- 2.1.2 Account Logon and Logon Events
- 2.1.2 Account Logon and Logon Events
- 2.1.2 Account Logon and Logon Events
- 2.1.2 Account Logon and Logon Events
- 2.1.2 Account Logon and Logon Events
- 2.1.2 Account Logon and Logon Events
- 2.1.2 Account Logon and Logon Events
- 2.1.2 Account Logon and Logon Events
- 2.1.2 Account Logon and Logon Events

2.1.4 Scheduled Task Logging

If scheduled task logging is configured, defenders can identify scheduled tasks being created (Event ID **106**), updated (Event ID **140**), deleted (Event ID **141**), executed (Event ID **200**) and completed (Event ID **201**).

Information about the account that scheduled the task is included in Event ID **106**. Information about the user that updated a scheduled task is included in Event ID **140** so on and so forth...

OUTLINE

Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

2.1.4 Scheduled Task Logging

2.1.5 Object Access Auditing

As we have already covered Object Access Auditing is disabled by default. On critical systems having such visibility is of key importance though.

We have covered cases of Object Access Auditing while covering deception-like approaches in the “Preparing & Defending Against Post-exploitation” module.

OUTLINE

LOGON EVENTS

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

2.1.4 Scheduled Task Logging

2.1.5 Object Access Auditing

2.1.6 Audit Policy Changes

An attacker tampering with System audit policy can result in significant evidence loss. For this reason keep an eye for Event IDs **4719** and **1102** that are related to System audit policy changes and the Security event log being erased.

Event ID **4719** may contain the account that caused the audit policy change. Event ID **1102** usually contains the name of the user account performing the erase.

OUTLINE

Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

2.1.4 Scheduled Task Logging

2.1.5 Object Access Auditing

2.1.6 Audit Policy Changes

2.1.7 Process Tracking

With attackers abusing legitimate Windows binaries to execute malicious, command line process auditing has gained a lot of traction.

Keep an eye for Event ID 4688 which is related to a new process being created. This event is similar in nature to Sysmon Event ID 1 and can provide you with critical process information.

OUTLINE

LOGON EVENTS

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

2.1.4 Scheduled Task Logging

2.1.5 Object Access Auditing

2.1.6 Audit Policy Changes

▼ 2.1.7 Process Tracking

2.1.7 Process Tracking

If your organization has command line process auditing enabled, there are great chances that you will also be able to see some additional entries under the Security log. These entries will originate from the [Windows Filtering Platform](#) and can enhance your network connection and port visibility.

Keep an eye for [Event IDs 5031, 5152, 5154, 5156, 5157, 5158 and 5159](#).

<https://docs.microsoft.com/bg-bg/windows/desktop/FWP/about-windows-filtering-platform>

<https://docs.microsoft.com/en-us/windows/desktop/fwp/auditing-and-logging>

IHRPv1 - Caendra Inc. © 2019 | p.31

OUTLINE

Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

2.1.4 Scheduled Task Logging

2.1.5 Object Access Auditing

2.1.6 Audit Policy Changes

▼ 2.1.7 Process Tracking

2.1.7 Process Tracking

2.1.8 Auditing PowerShell

Finally, let's talk about the most important PowerShell-related Event IDs (these appear inside `%SystemRoot%/System32/winevt/Logs/Microsoft-Windows-PowerShell%40Operational.evtx`).

- Event ID **4103** is filled with data from the module logging facility.
- Event ID **4104** is filled with data from the Script Block logging functionality. It contains actual command captures and logs everything inside a block.
- Event ID **400** is related to a command execution or session starting. The hostname field reveals if we are dealing with a local or remote session.
- Event ID **800** contains pipeline execution details, again the hostname field reveals if we are dealing with a local or remote session and the *HostApplication* field can indicate malicious PowerShell usage (for example PowerShell being executed with the `-enc` option)

OUTLINE

LOGON EVENTS

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

2.1.4 Scheduled Task Logging

2.1.5 Object Access Auditing

2.1.6 Audit Policy Changes

▼ 2.1.7 Process Tracking

2.1.7 Process Tracking

2.1.8 Auditing PowerShell

IHRP

References

OUTLINE

Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

2.1.4 Scheduled Task Logging

2.1.5 Object Access Auditing

2.1.6 Audit Policy Changes

▼ 2.1.7 Process Tracking

2.1.7 Process Tracking

2.1.8 Auditing PowerShell

▼ References

References

Windows Security Log Event ID 4768

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4768>

Logon Type: Windows Security Log Event ID 4624

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624>

Twitter - deckkh

<https://twitter.com/deckkh>

How can I enable the Windows Server Task Scheduler History recording?

<https://stackoverflow.com/questions/11013132/how-can-i-enable-the-windows-server-task-scheduler-history-recording/14651161>

OUTLINE

Logon Events

2.1.2 Account Logon and Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

2.1.4 Scheduled Task Logging

2.1.5 Object Access Auditing

2.1.6 Audit Policy Changes

▼ 2.1.7 Process Tracking

2.1.7 Process Tracking

2.1.8 Auditing PowerShell

▼ References

References

References

command line process auditing

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing>

Windows Security Log Event ID 4688

<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4688>

Windows Filtering Platform

<https://docs.microsoft.com/bg-bg/windows/desktop/FWP/about-windows-filtering-platform>

Event IDs **5031, 5152, 5154, 5156, 5157, 5158** and **5159**

<https://docs.microsoft.com/en-us/windows/desktop/fwp/auditing-and-logging>

OUTLINE

Logon Events

2.1.2 Account Logon and Logon Events

2.1.3 Access to Shared Objects

2.1.4 Scheduled Task Logging

2.1.5 Object Access Auditing

2.1.6 Audit Policy Changes

▼ 2.1.7 Process Tracking

2.1.7 Process Tracking

2.1.8 Auditing PowerShell

▼ References

References

References