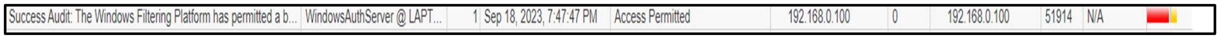
AI FOR CYBER SECURITY WITH IBM QRADAR

Name: J. Manasa

Task-14: Collect logs and analyse any 4 log events of IBM QRadar

The logs of IBM QRadar are collected through wincollect and wincollect standalone applications. By logging into the ip address on which QRadar is run, we can view the events.

1.

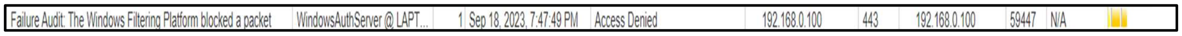


Success Audit: The Windows Filtering Platform has permitted a b...	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:47 PM	Access Permitted	192.168.0.100	0	192.168.0.100	51914	N/A	🟥

In the above log, the event name is the windows filtering platform has permitted a bind to a local port which is a success audit. The log source is Windows Authenticated server which is the laptop where QRadar is installed. Event count is 1. Access for this event is permitted and hence it is a success audit. The source audit is the ip address 192.168.0.100 and port is 0. Destination ip is same as source ip and the port number is 51914. Username of the event where it took place is not mentioned here. The relevance of this log is 9, severity is 0, credibility is 5 and magnitude is 5.

The business impact of this log is as the access is permitted, it is not a risky event. Severity is 0 which indicates that the event is not harmful. Relevance is high which means that it is related to SIEM context and it is important.

2.

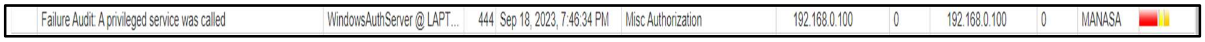


Failure Audit: The Windows Filtering Platform blocked a packet	WindowsAuthServer @ LAPT...	1	Sep 18, 2023, 7:47:49 PM	Access Denied	192.168.0.100	443	192.168.0.100	59447	N/A	🟨

In the above log, the event name is the windows filtering platform blocked a packet which is a failure audit. The log source is Windows Authenticated server which is the laptop where QRadar is installed. Event count is 1. Access for this event is denied and hence it is a failure audit. The source audit is the ip address 192.168.0.100 and port is 443. Destination ip address is same as source ip and the port number is 59447. Username of the event where it took place is not mentioned here. The relevance of this log is 3, severity is 1, credibility is 5 and magnitude is 3.

The business impact of the above event is the fact that the access is denied which means the security controls are active and protecting the system. Though the severity was low, it was denied. Relevance is low which means the log event is slightly related to SIEM.

3.

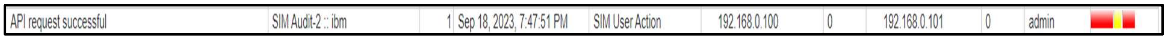


Failure Audit: A privileged service was called	WindowsAuthServer @ LAPT...	444	Sep 18, 2023, 7:46:34 PM	Misc Authorization	192.168.0.100	0	192.168.0.100	0	MANASA	🟥

In the above log, the event name is a privileged service was called which is a failure audit. The log source is Windows Authenticated server which is the laptop where QRadar is installed. Event count is 444. This event is misc authorization which means the miscellaneous context is being authorized and according to the event, it is failed which means the authorization is denied. The source audit is the ip address 192.168.0.100 and port is 0. Destination ip and the port number are same as the source ip and port . Username of the event where it took place is MANASA, which is the name of the system. The relevance of this log is 9, severity is 4, credibility is 2 and magnitude is 4.

The business impact of the above event is the authorization is denied which means it might be potentially risky. Severity is 4 which means it is lightly risky. Relevance is 9 which means it is highly related to SIEM system.

4.



API request successful	SIM Audit-2 :: ibm	1	Sep 18, 2023, 7:47:51 PM	SIM User Action	192.168.0.100	0	192.168.0.101	0	admin	🟥🟨🟥

In the above log, the event name is the API request successful. The log source is SIM Audit-2::ibm. Event count is 1. This is a SIM user action. The source audit is the ip address 192.168.0.100 and port is 0. Destination ip is 192.168.0.101 and the port number is 0. Username of the event where it took place is admin, which is the name given to the virtual machine. The relevance of this log is 7, severity is 3, credibility is 5 and magnitude is 5.

The business impact of the above event is the event is successful. Severity is 3 which means it is not risky. Relevance is 7 which means it is moderately related to the SIEM system.