MENA SEC

Applied Security Research

Home About us

Wednesday, 6 February 2019

Threat Hunting #5 - Detecting enumeration of users via Net.exe or Net1.exe utility

Detecting an attacker during the reconnaissance phase is very important, because if he\she is at this stage, it means she\he already bypassed all your peripheral and endpoint standard security solutions. If you can detect and stop him at this stage then good for you!

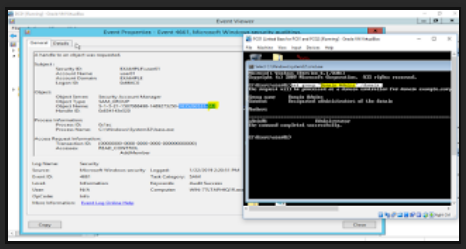
Microsoft Net.exe utility can be used to enumerate local and domain users and groups [a must to do for any attacker trying to get answers for who/where/what/etc. to complete the objectives].

Famous detection techniques for users enumeration with the net.exe utility are limited to processes's command line value and process name verification (i.e. process_name:net.exe and/or commandLine:.*net.*users.*). which is a vulnerable/weak detection and can be bypassed by simply renaming the process name or introducing special obfuscation characters in the command line (i.e. ^, set x, environment variables etc.)

In this post we will be using event ID 4661 to detect enumeration attempts of known privileged AD accounts/groups:

- Enterprise Admins
- Domain Admins
- Administrators group
- Administrator
- etc

Below an example of "Domain Admins" group enumeration:



You will need to enable this event on all your domain controllers (expected target for any domain user enumeration). Note that this method can also detect user enumeration with other utilities/tools.

Detection Logic:

Look for event 4661 with Messgae body containing known AD privileged groups/accounts SID values. Example of IBM Qradar AQL query:

select "SourceUserName", "ObjectType", "ObjectName" from events where "EventID"=4661 and not (SourceUserName IMATCHES '.*\$') and (UTF8(payload) IMATCHES '.*S-1-5-21-.*-(512|502|500|505|519|520|544|551|555).*') last 180 DAYS

References:

Blog Archive

https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4661

Threat Huting #9 - Impacket\Secretdump remote exec...
Threat Hunting #8 - Detecting tracks of... BloodHound\Sharphoun...
Threat Hunting #6 - Hiding in plain sights with re...
Threat Hunting #5 - Detecting enumeration of users...
Threat Hunting #4 - Detecting Excel/Word documents...
Threat Hunting #3 - Detecting PsExec execution usi...
Threat Hunting #2 - Detecting PsLoggedOn exec usin...
Threat Hunting #1 - RDP Hijacking traces - Part 1

No comments:

Post a Comment

To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)