Lateral movement analyzer tool

Download Latma

Lateral movement analyzer (LATMA) collects authentication logs from the domain and searches for potential lateral movement attacks and suspicious activity. The tool visualizes the findings with diagrams depicting the lateral movement patterns. This tool contains two modules, one that collects the logs and one that analyzes them. You can execute each of the modules separately, the event log collector should be executed in a Windows machine in an active directory domain environment with python 3.8 or above. The analyzer can be executed in a linux machine and a Windows machine.

The Collector

The Event Log Collector module scans domain controllers for successful NTLM authentication logs and endpoints for successful Kerberos authentication logs. It requires LDAP/S port 389 and 636 and RPC port 135 access to the domain controller and clients. In addition it requires domain admin privileges or a user in the Event log Reader group or one with equivalent permissions. This is required to pull event logs from all endpoints and domain controllers.

The collector gathers NTLM logs from event 8004 on the domain controllers and Kerberos logs from event 4648 on the clients. It generates as an output a csv comma delimited format file with all the available authentication traffic. The output contains the fields source host, destination, username, auth type, SPN and timestamps in the format %Y/%m/%d %H:%M. The collector requires credential of a valid user with event viewer privileges across the environment and queries the specific logs for each protocol.

Verify Kerberos and NTLM protocols are audited across the environment using group policy:

1. Kerberos – Computer configuration -> policies -> Windows Settings -> Security settings -> Local policies -> Audit Policies -> audit account logon events
2. NTLM – Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> Network Security: Restrict NTLM: audit NTLM authentication in this domain

The Analyzer

The Analyzer receives as input a spreadsheet with authentication data formatted as specified in Collector's output structure. It searches for suspicious activity with the lateral movement analyzer algorithm and also detects additional IoCs of lateral movement. The authentication source and destination should be formalized with netbios name and not ip addresses.

Preliminaries and key concepts of the LATMA algorithm

LATMA gets a batch of authentication requests and sends an alert when it finds suspicious lateral movement attacks. We define the following:

- Authentication Graph: A directed graph that contains information about authentication traffic in the environment. The nodes of the graphs are computers, and the edges are authentications between the computers. The graph edges have the attributes: protocol type, date of authentication and the account that sent the request. The graph nodes contain information about the computer

it represents, detailed below.

- Lateral movement graph: A sub-graph of the authentication graph that represents the attacker's movement. The lateral movement graph is not always a path in the sub-graph, in some attacks the attacker goes in many different directions.
- Alert: A sub-graph the algorithm suspects are part of the lateral movement graph.

LATMA performs several actions during its execution:

- Information gathering: LATMA monitors normal behavior of the users and machines and characterizes them. The learning is used later to decide which authentication requests deviate from a normal behavior and might be involved in a lateral movement attack. For a learning period of three weeks LATMA does not throw any alerts and only learns the environment. The learning continues after those three weeks.
- Authentication graph building: After the learning period every relevant authentication is added to the authentication graph. It is critical to filter only for relevant authentication, otherwise the number of edges the graph holds might be too big. We filter on the following protocol types: NTLM and Kerberos with the services "rpc", "rpcss" and "termsrv."

Alert handling:

Adding an authentication to the graph might trigger a process of alerting. In general, a new edge can create a new alert, join an existing alert or merge two alerts.

Information gathering

Every authentication request monitored by LATMA is used for learning and stored in a dedicated data structure. First, we

identify sinks and hubs. We define sinks as machines accessed by many (at least 50) different accounts, such as a company portal or exchange server. We define hubs as machines many different accounts (at least 20) authenticate from, such as proxies and VPNs. Authentications to sinks or from hubs are considered benign and are therefore removed from the authentication graph.

In addition to basic classification, LATMA matches between accounts and machines they frequently authenticate from. If an account authenticates from a machine at least three different days in a three weeks' period, it means that this account matches the machine and any authentication of this account from the machine is considered benign and removed from the authentication graph.

The lateral movement IoCs are:

White cane - User accounts authenticating from a single machine to multiple ones in a relatively short time.

Bridge – User account X authenticating from machine A to machine B and following that, from machine B to machine C. This IoC potentially indicates an attacker performing actual advance from its initial foothold (A) to destination machine that better serves the attack's objectives.

Switched Bridge – User account X authenticating from machine A to machine B, followed by user account Y authenticating from machine B to machine C. This IoC potentially indicates an attacker that discovers and compromises an additional account along its path and uses the new account to advance forward (a common example is account X being a standard domain user and account Y being a admin user)

Weight Shift – White cane (see above) from machine A to machines {B1,…, Bn}, followed by another White cane from machine Bx to machines {C1,…,Cn}. This IoC potentially indicates an attacker that has determined that machine B would

better serve the attack’s purposes from now on uses machine B as the source for additional searches.

Blast – User account X authenticating from machine A to multiple machines in a very short timeframe. A common example is an attacker that plants \ executes ransomware on a mass number of machines simultaneously

Output:

The analyzer outputs several different files

1. A spreadsheet with all the suspected authentications (all_authentications.csv) and their role classification and a different spreadsheet for the authentications that are suspected to be part of lateral movement (propagation.csv)
2. A GIF file represents the progression, wherby each frame of the GIF specifies exactly what was the suspicious action
3. An interactive timeline with all the suspicious events. Events that are related to each other have the same color

Dependencies:

1. Python 3.8
2. libraries as follows in requirements.txt
3. Run pip install . for running setup automatically
4. Audit Kerberos and NTLM across the environment
5. LDAP queries to the domain controllers
6. Domain admin credentials or any credentials with MS-EVEN6 remote event viewer permissions.

usage

The Collector

Required arguments:

1. credentials [domain.com/]username[:password] credentials format alternatively [domain.com/]username and then password will be prompted securely. For domain please insert the FQDN (Fully Quallified Domain Name). Optional arguments:
2. -ntlm Retrieve ntlm authentication logs from DC
3. -kerberos Retrieve kerberos authentication logs from all computers in the domain
4. -debug Turn DEBUG output ON
5. -help show this help message and exit
6. -filter Query specific ou or container in the domain, will result all workstations in the sub-OU as well. Each OU will be in format of DN (Distinguished Name). Supports multiple OUs with a semicolon delimiter. Example: OU=subunit,OU=unit;OU=anotherUnit,DC=domain,DC=com Example: CN=container,OU=unit;OU=anotherUnit,DC=domain,DC=com
7. -date Starting date to collect event logs from. month-day-year format, if not specified take all available data
8. -threads amount of working threads to use
9. -ldap Use Unsecure LDAP instead of LDAP/S
10. -ldap_domain Custom domain on ldap login credentials. If empty, will use current user’s session domain

Binary Usage Open command prompt and navigate to the binary folder. Run executables with the specified above arguments.

Examples

In the example files you have several samples of real

environments (some contain lateral movement attacks and some don’t) which you can give as input for the analyzer.

Usage example

1. python eventlogcollector.py domain.com/username:password -ntlm -kerberos