A

PROJECT REPORT

ON

“ACTIVE HUNTING USING ELK”

SUBMITTED

BY:

ASHUTOSH BHAVE

UNDER THE GUIDANCE OF

PROF. SMITA PATIL

SAVITRIBAI PHULE PUNE UNIVERSITY

IN PARTIAL FULFILLMENT OF

MASTER IN COMPUTER SCIENCE

SARHAD COLLEGE OF SCIENCE, PUNE -41

ACKNOWLEDGEMENT

At the completion of my industrial training, I feel obliged to express my gratitude to all who contributed to the success of this endeavor.

I would like to express my thankfulness to the people who mentored and guided me during this period of my internship. Words can hardly express my deep sense of gratitude for my project guide, Prof Smita Patil, for her intellectual, moral and technical expertise and ceaseless co-operation.

I am also grateful to my entire team at Smokescreen Technologies Pvt. Ltd for sharing their vast expanse of knowledge and experience in the field of cybersecurity. The learning experience and exposure provided by you will assist me greatly and serve as a foundation for my career in the future.

Thank you

Yours sincerely,
Ashutosh Bhave

INDEX

SMOKESCREEN TECHNOLOGIES PVT. LTD

Smokescreen's DECEPTION TECHNOLOGY is a revolution in enterprise security. It relies on three major methodologies:

DETECT

Discover advanced attackers and internal threats on your network. Get real-time alerts that are false positive free.

DEFLECT

Silently divert attackers from your real system into a virtual world. Keep them busy while watching their every move.

DEFEAT

After gathering intel on their tactics, you have the necessary information to effectively contain and clean them out.

Website: www.smokescreen.io

Introduction

1. INTRODUCTION & OBJECTIVE

Active hunting is a methodology used by an organization’s information security team to Detect and track down any malicious activity occurring within their internal network by monitoring the network logs for anomalous behavior. Its aim is to parse all critical system logs and detect patterns and signatures for unusual activities that might compromise critical information. This process has helped safeguard the internal infrastructure of a large enterprise networks. Here, active hunting is carried out by using Elasticsearch, Kibana and Logstash(ELK) as the data logging and analysis tool.

2. PURPOSE OF THE PROJECT

This active hunting simulation is set up and carried out in a lab environment to test data logging and its analysis. Its model will later be deployed in corporate networks for the same purpose. The lab environment is scaled down replica of a corporate network upon which hacking and breach simulations have been carried out to identify the patterns of such attacks in the generated logs.

3. EXISTING SYSTEM DISADVANTAGES

Methods of data parsing and its analysis prior to ELK were complicated and only few experts in the field could accomplish such tasks to a mediocre level of efficiency. Grep is not scalable and RegEx scripts are too complicated to be written for every custom need. Sophisticated and efficient tools (like Splunk) cost a fortune and generates bills in millions of dollars. ELK is an open-source tool and has proven to be very efficient to an extent where corporations are rapidly switching to it for their data processing needs.

1. System Analysis

2.1 STUDY OF THE SYSTEM

There are various features of the Windows and Linux operating system incorporated in this simulation to replicate an enterprise network. They are as follows:

2.1.1 ELASTICSEARCH

ElasticSearch is a search server based on Lucene. It provides a distributed, multitenant-Capable, full-text search engine with an HTTP web interface and schema-free JSON documents. Elasticsearch is developed in Java and is released as open source under the terms of the Apache License.

Logs fed to the ELK server are of various types. By applying the right filters to elasticsearch using configuration files, we can retrieve logs customized according our needs.

2.1.2 LOGSTASH

Logstash is an open source tool for collecting, parsing, and storing logs for future use. It was developed by Jordan Sissel.

Logstash is configured to listen on a certain tcp port and stores all forwarded logs which are later used for analysis.

2.1.3 KIBANA

Kibana 3 (or later versions) is a web interface that can be used to search and view the logs that Logstash has indexed.

It has a text based (not script-based) search module which does not require any programming proficiency. Various visualization mechanisms like bar graphs, pie charts, etc can formed containing the fields of your choice.

2.1.4 Windows Domain

A Windows domain is a form of a computer network in which all user accounts, computers, printers and other security principals, are registered with a central database located on one or more clusters of central computers known as domain controllers. Authentication takes place on domain controllers. Each person who uses computers within a domain receives a unique user account that can then be assigned access to resources within the domain. Starting with Windows 2000, Active Directory is the Windows component in charge of maintaining that central database. The concept of Windows domain is in contrast with that of a workgroup in which each computer maintains its own database of security principals.

Computers can connect to a domain via LAN, WAN or using a VPN connection. Users of a domain are able to use enhanced security for their VPN connection due to the support for a certification authority which is gained when a domain is added to a network, and as a result smart cards and digital certificates can be used to confirm identities and protect stored information.

In a Windows domain, the directory resides on computers that are configured as "domain controllers." A domain controller is a Windows or Samba server that manages all security-related aspects between user and domain interactions, centralizing security and administration. A domain controller is generally suited for businesses and/or organizations when more than 10 PCs are in use. A domain does not refer to a single location or specific type of network configuration. The computers in a domain can share physical proximity on a small LAN or they can be located in different parts of the world. As long as they can communicate, their physical position is irrelevant.

2.1.5 Group Policy Management Console

The Group Policy Management Console (GPMC) is a new and comprehensive administrative tool for Group Policy management.

Prior to GPMC, administrators used property pages in various Active Directory administrative tools to manage Group Policy. For example, an administrator who wanted to implement policy for users might open the Active Directory Users and Computers snap-in, find an appropriate Organizational Unit (OU) and open its property page to access the Group Policy tab. On the Group Policy tab, the administrator might do any of a dozen or so administrative tasks, like creating Group Policy object links or manipulating their order to achieve the desired results. Whatever the tasks, when the administrator leaves the Group Policy tab, access to a visual representation of Group Policy ends and a view that focuses on Active Directory’s user and computer objects appears.

GPMC integrates the existing Group Policy functionality of the property pages on the Active Directory administrative tools into a single, unified console dedicated to Group Policy management tasks; GPMC also expands management capabilities with new features.

Administrators still use Active Directory administrative tools to manage Active Directory, but GPMC replaces the Group Policy management functionality of those tools with its own.

2.1.6 Windows Event Forwarding/Collection

Event collection allows administrators to get events from remote computers and store them in a local event log on the collector computer. The destination log path for the events is a property of the subscription. All data in the forwarded event is saved in the collector computer event log (none of the information is lost). Additional information related to the event forwarding is also added to the event.

Subscriptions

There are two types of event subscriptions

- **Source-initiated subscriptions**: allows you to define an event subscription on an event collector computer without defining the event source computers. Multiple remote event source computers can then be set up (using a group policy setting) to forward events to the event collector computer.
- **Collector-initiated subscriptions**: allows you to create an event subscription if you know all the event source computers that will forward events. You specify all the event sources at the time the subscription is created.

This lab simulation using Source-initiated subscription using Windows Remote Management.

2.1.7 Logstash Configuration Files

To configure Logstash, you create a config file that specifies which plugins you want to use and settings for each plugin. You can reference event fields in a configuration and use conditionals to process events when they meet certain criteria. When you run logstash, you use the -f to specify your config file.

There are 3 main sections:

- Inputs
- Filters
- Outputs.

Each section has configurations for each plugin available in that section.

2. System Design

HARDWARE/ SOFTWARE REQUIREMENTS

Hardware Requirements

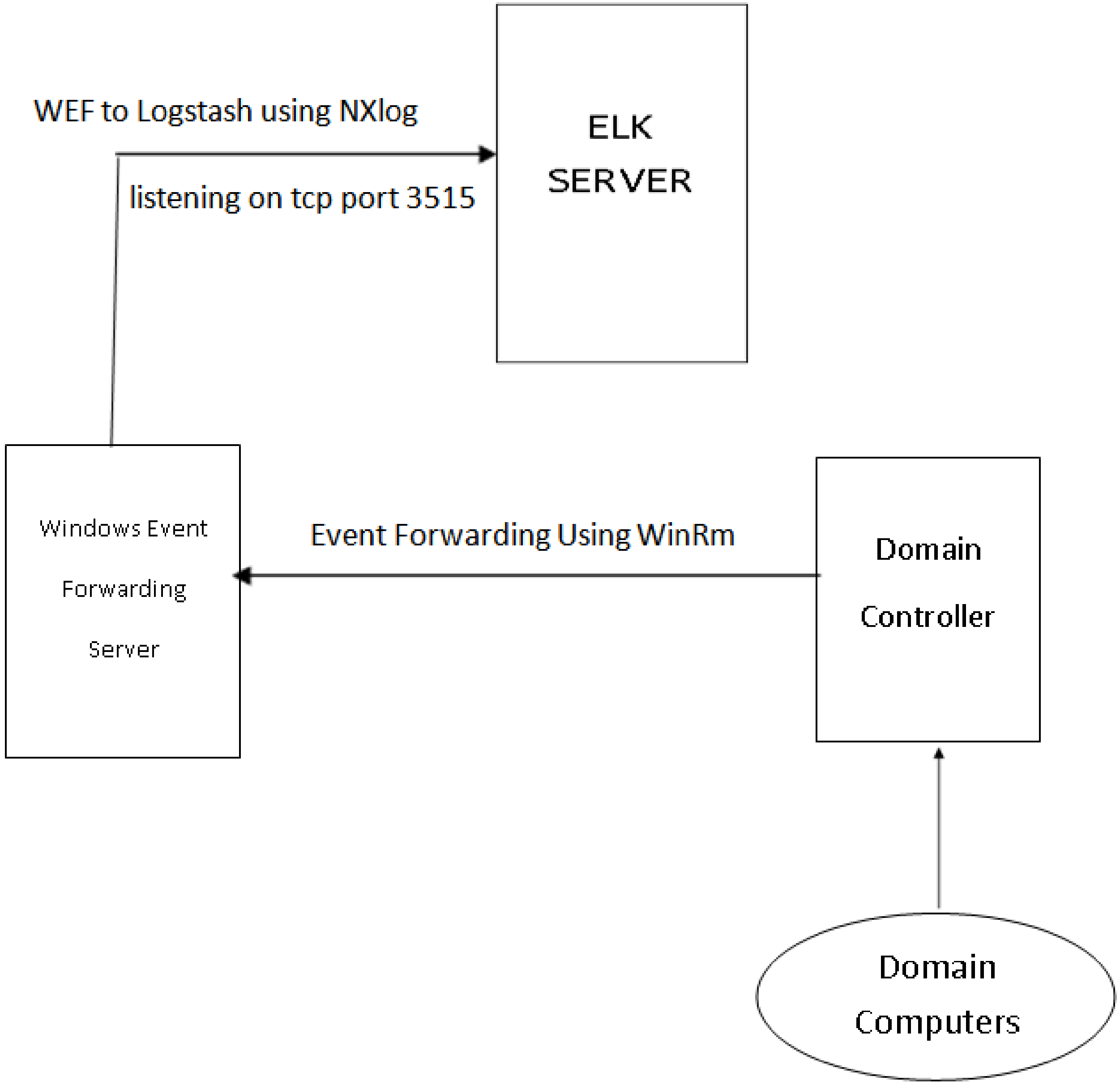
- 16 GB RAM
- 500 GB HDD
- 8 core processor

Software Requirements

- VMWare ESXi Console
- VMRC
- ISO images for :
    1. Windows Server 2008 R2 Enterprise
    2. Windows 8.1
    3. Ubuntu 14.04 Server

4.

Topology Diagram


WEF to Logstash using NXlog
listening on tcp port 3515
ELK SERVER
Windows Event Forwarding Server
Event Forwarding Using WinRm
Domain Controller
Domain Computers

3.1 Windows Domain

Windows domain in this simulation is used to replicate the numerous user terminals which will be added to the enterprise network. Every user in the organization is added to this domain with various levels of authoritative privileges. They have the same network policy and services provided to them when they're added to the domain.

A domain (hallows.local) has been created on the domain controller and a few users are added to it.

3.2 Domain Controller

A domain controller is used to configure the domain computers with similar configuration. It offers features like

- Group Policy Management
- DHCP
- DNS Services

Windows 2008 R2 server has been deployed to for this purpose in the simulation. Windows 2008 R2 server has backward compatibility for every service provided by all earlier Windows Server versions.

The domain controller allows us to use Active Directory Services which provides the creation of users domain user accounts with which terminals users can authenticate themselves on the network.

Group Policy Management Console allows you to create a Group Policy which enables event forwarding using Windows Remote management (WinRm), set firewalls rules for inbound http logs on tcp port 5985 and subscription manager server for your domain.

3.3 Windows Event Forwarding Server

A dedicated Windows Server 2008 R2 is set up as event collector. WinRm quickconfig is enabled to user to view event collection using event viewer interface. (wecutil qc can be used to for command line retrievals). This event collector is configured for source initiated forwarding (wherein the domain computers forward logs to event collector via the domain controller using WinRm).

A subscription is configured for this purpose. The types of logs, domain computers and encryption can be assigned here.

Benefits of Windows Event Forwarding

- The WEF architecture forwards events in the native event log format. This is helpful because the event log format uses XML to cleanly structure data into different fields that will be helpful when querying in ElasticSearch.
- WEF utilizes group policy, so all clients that join a network or change OUs will automatically begin to participate in the log forwarding architecture. This is helpful to ensure completeness of coverage from a logging perspective.
- WEF does not require an agent to be installed. The lack of an agent requirement is helpful as some organizations will be hesitant to install another agent on each box (e.g. event-to-sys) and ensuring completeness of agent deployment can be challenging as clients are constantly changing
- WEF encrypts all data between the log collector and the clients by default
    - If using HTTP: WEF will use the Microsoft Negotiate security support provider (SSP) in workgroup environments or the Microsoft Kerberos SSP in domain environments.

Nxlog is a tool installed to aid logstash to pull logs from the event forwarding server. It is configured as wherein the destination is the ELK server and the port is a TCP port (3515) which the ELK is configured for listening.

3.4 ELK SERVER

An ubuntu 14.04 server is dedicated as the ELK server. Logstash is provided with a configuration file to receive logs from the Windows Forwarding Server and direct them to ElasticSearch so that it can be indexed and queried for patterns. Logstash configuration has 3 modules.

- Input: configured to receive incoming logs on tcp port 3515
- Filter: configured to parse logs in a format customized to user’s needs
- Output: Submodule defining the parameters for elasticsearch. Incorporates plugins for debugging.

Benefits of Elasticsearch

- Scalable horizontal compute and storage.

- ElasticSearch can accommodate node failure and automatically re-distribute shards without data loss
- ElasticSearch leverages parallel processing to execute queries on massive data sets very quickly
- Open source (free)
- Great for long tail analysis and querying

Once the logs are indexed and parsed into elasticsearch, Kibana interface can be used to query and perform long tail analysis on the collected logs.

Benefits of Kibana

- Kibana provides a beautiful interface that allows you to easily query ElasticSearch.
- Using Kibana, you can quickly filter to perform long tail analysis and anomaly detection.

3. Workflow

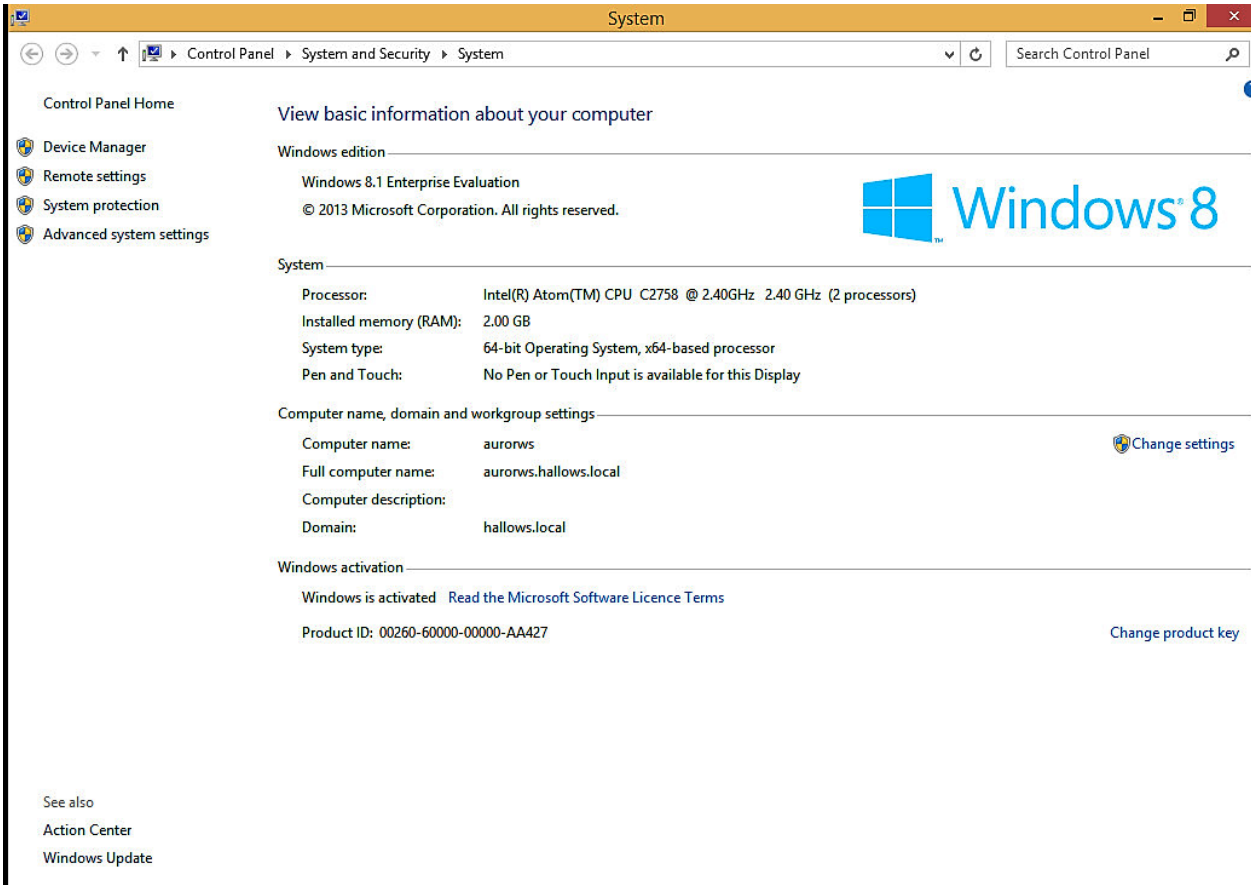
4.1 Stepwise Methodology

1. Configuring a group Policy on the Domain Controller to enable WinRm, firewall rules to listen to inbound logs and Event Forwarding. Also, configure the event collectors IP domain name and destination port.
2. Push the group policy onto the domain computers.
3. Create a subscription for source initiated event collection on the event forwarding server for the domain and add the list of domain computers allowed for event forwarding.
4. Start NXlog as a service on Event forwarder to send logs to ELK server on tcp port 3515.
5. Configure logstash to gather incoming on tcp port 3515, parse them according to set filters and forward them into elasticsearch using the provided configuration file.

   Every component and its configuration is explained below:

4.2 Domain Computers

Windows Active Directory Services allows us to create domain user profiles. We can add the required number of users by creating their respective profiles which also includes their access credentials on the domain controller.



View basic information about your computer

Windows edition

Windows 8.1 Enterprise Evaluation

© 2013 Microsoft Corporation. All rights reserved.

System

Processor: Intel(R) Atom(TM) CPU C2758 @ 2.40GHz 2.40 GHz (2 processors)

Installed memory (RAM): 2.00 GB

System type: 64-bit Operating System, x64-based processor

Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain and workgroup settings

Computer name: aurorws

Full computer name: aurorws.hallows.local

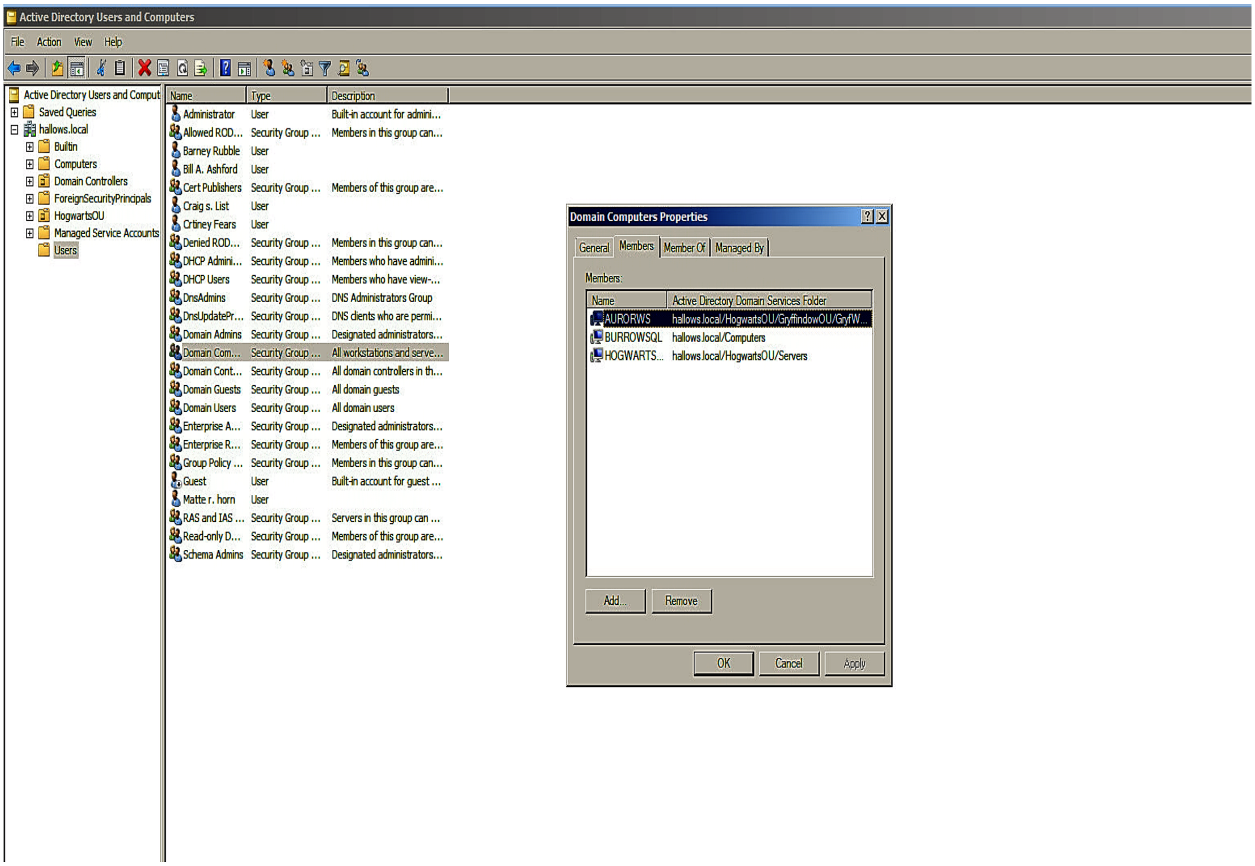
Computer description:

Domain: hallows.local

Windows activation

Windows is activated Read the Microsoft Software Licence Terms

Product ID: 00260-60000-00000-AA427



Name	Type	Description
Administrator	User	Built-in account for admini...
Allowed ROD...	Security Group ...	Members in this group can...
Barney Rubble	User	
Bill A. Ashford	User	
Cert Publishers	Security Group ...	Members of this group are...
Craig s. List	User	
Crtiney Fears	User	
Denied ROD...	Security Group ...	Members in this group can...
DHCP Admini...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Com...	Security Group ...	All workstations and serve...
Domain Cont...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise A...	Security Group ...	Designated administrators...
Enterprise R...	Security Group ...	Members of this group are...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
Matte r. horn	User	
RAS and IAS ...	Security Group ...	Servers in this group can ...
Read-only D...	Security Group ...	Members of this group are...
Schema Admins	Security Group ...	Designated administrators...

Members:

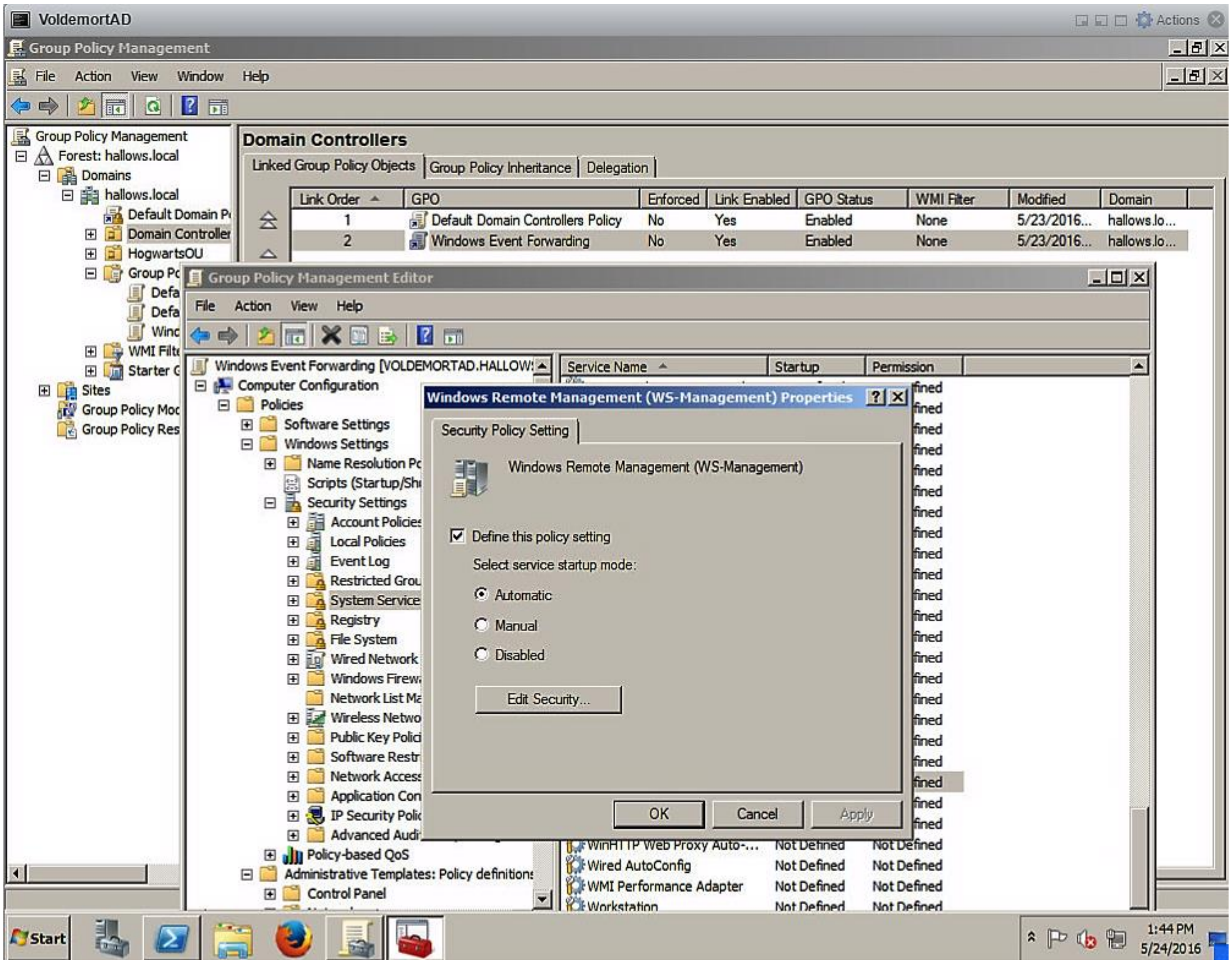
Name	Active Directory Domain Services Folder
AURORWS	hallows.local/HogwartsOU/GryffindowOU/GryfW...
BURROWSQL	hallows.local/Computers
HOGWARTS...	hallows.local/HogwartsOU/Servers

4.3 Domain Controller

A dedicated Windows Server 2008 R2 has been set up as the Domain Controller. It facilitates the user of Active Directory Services to create users under the same domain (hallows.local).DHCP addresses are assigned to all users in the domain from the private IP range of 10.10.6.0/24. It also DNS services for domain name resolution.

A Group policy is configured using the GPMC with the following rules

1. Enable Windows Remote Management (WinRm)
2. Configuring listeners on for incoming http traffic on port 5985.
3. Create inbound firewall rules to allow Windows event forwarding from domain computers.
4. Configure event collector server name and destination port in Event Forwarding Policy.
5. Link Windows Event Forwarding Policy to OUs.



Domain Controllers

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	Default Domain Controllers Policy	No	Yes	Enabled	None	5/23/2016...	hallows.lo...
2	Windows Event Forwarding	No	Yes	Enabled	None	5/23/2016...	hallows.lo...

Windows Remote Management (WS-Management) Properties

Security Policy Setting

Windows Remote Management (WS-Management)

☑ Define this policy setting

Select service startup mode:

● Automatic

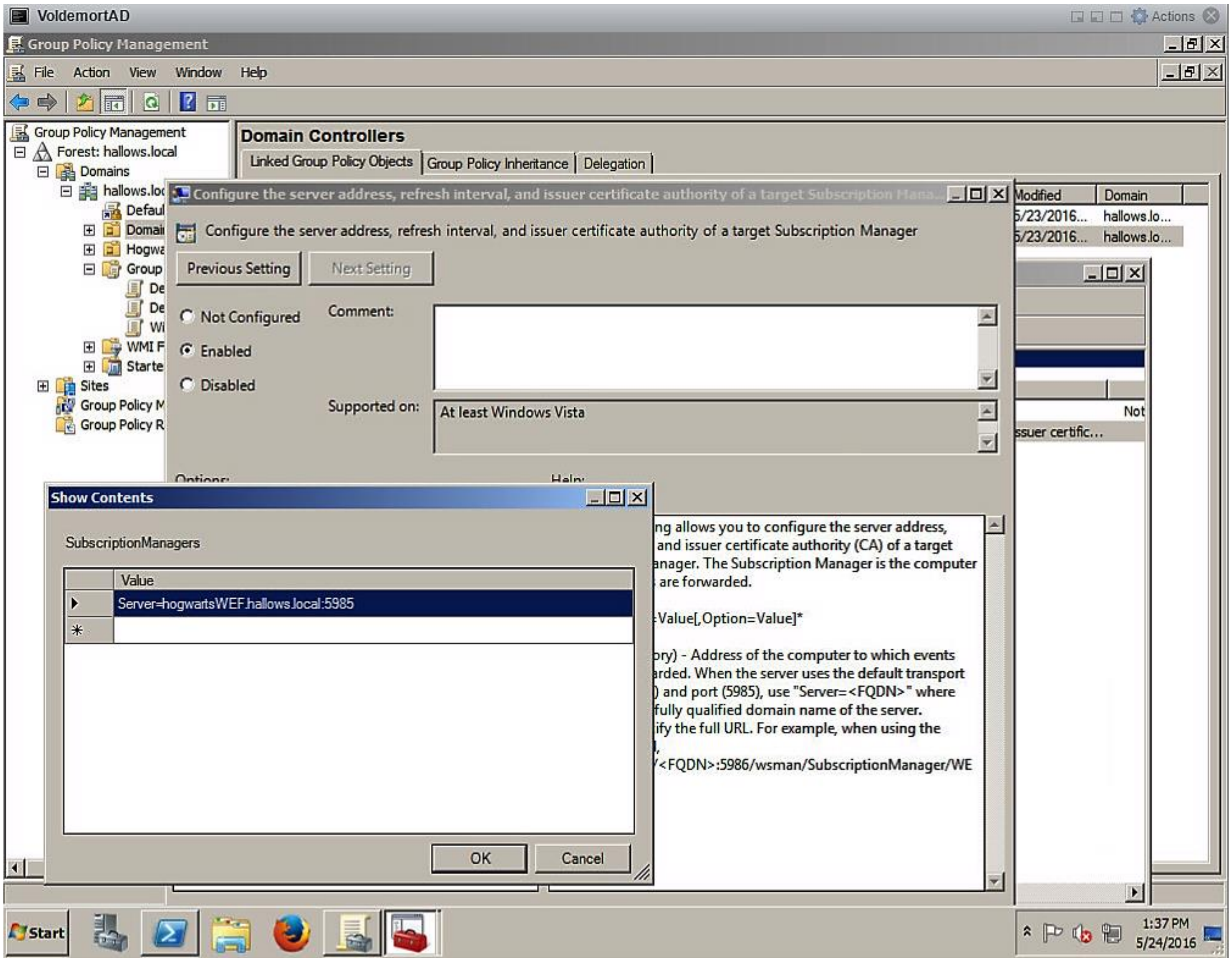
○ Manual

○ Disabled

Edit Security...

OK Cancel Apply

Service Name	Startup	Permission
WinHTTP Web Proxy Auto-...	Not Defined	Not Defined
Wired AutoConfig	Not Defined	Not Defined
WMI Performance Adapter	Not Defined	Not Defined
Workstation	Not Defined	Not Defined



Configure the server address, refresh interval, and issuer certificate authority of a target Subscription Mana...

Configure the server address, refresh interval, and issuer certificate authority of a target Subscription Manager

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Show Contents

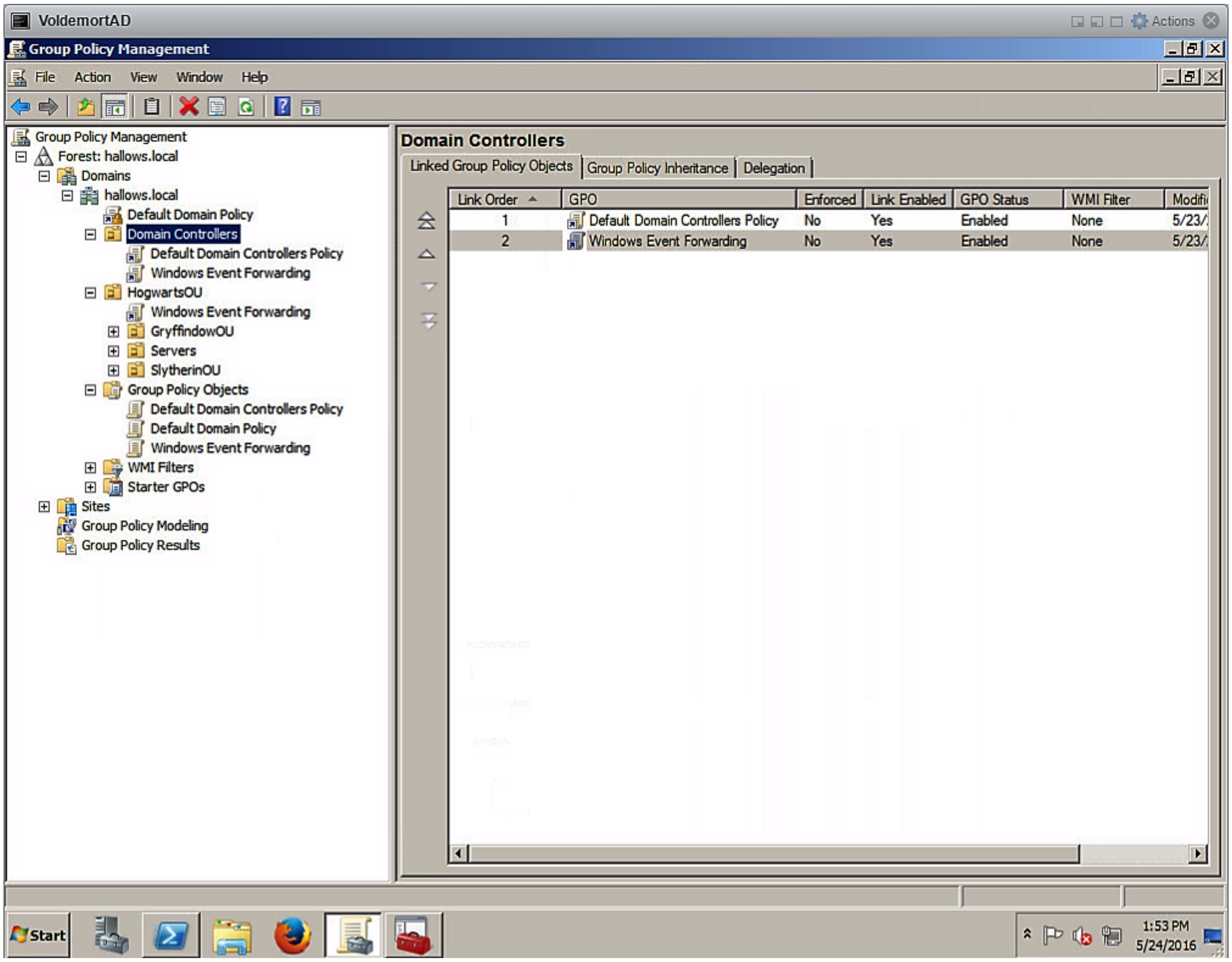
SubscriptionManagers

	Value
▶	Server=hogwartsWEF.hallows.local:5985
*	

ng allows you to configure the server address,
and issuer certificate authority (CA) of a target
anager. The Subscription Manager is the computer
are forwarded.

:Value[,Option=Value]*

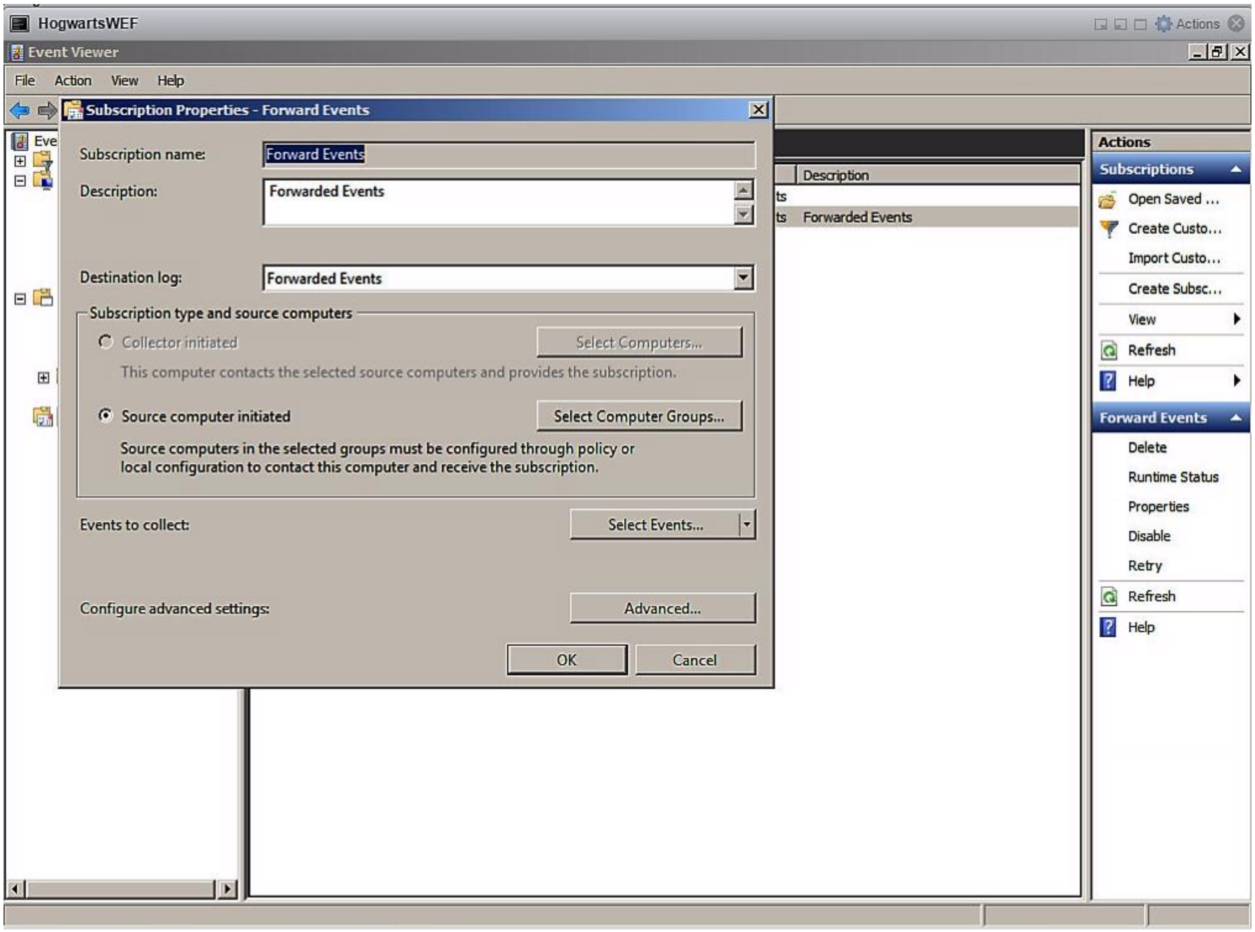
ory) - Address of the computer to which events
arded. When the server uses the default transport
) and port (5985), use "Server=<FQDN>" where
fully qualified domain name of the server.
ify the full URL. For example, when using the
,
/<FQDN>:5986/wsman/SubscriptionManager/WE



Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modifi
1	Default Domain Controllers Policy	No	Yes	Enabled	None	5/23/
2	Windows Event Forwarding	No	Yes	Enabled	None	5/23/

4.4 Windows Event Forwarding Server

A dedicated Windows Server 2008 R2 is configured with a source-initiated subscription to receive all system logs from the entire (hallows.local) domain. The list of computers in the domain is added for it collector to know events sourced from which terminals are to logged. A "Forwarded Events" destination folder is created to storing the forwarded Events. Event logs sourced from every level are collected and stored accordingly. Incoming HTTP request are allowed without any delay in authentication.



Subscription Properties - Forward Events

Subscription name: Forward Events

Description: Forwarded Events

Destination log: Forwarded Events

Subscription type and source computers

○ Collector initiated — Select Computers...

This computer contacts the selected source computers and provides the subscription.

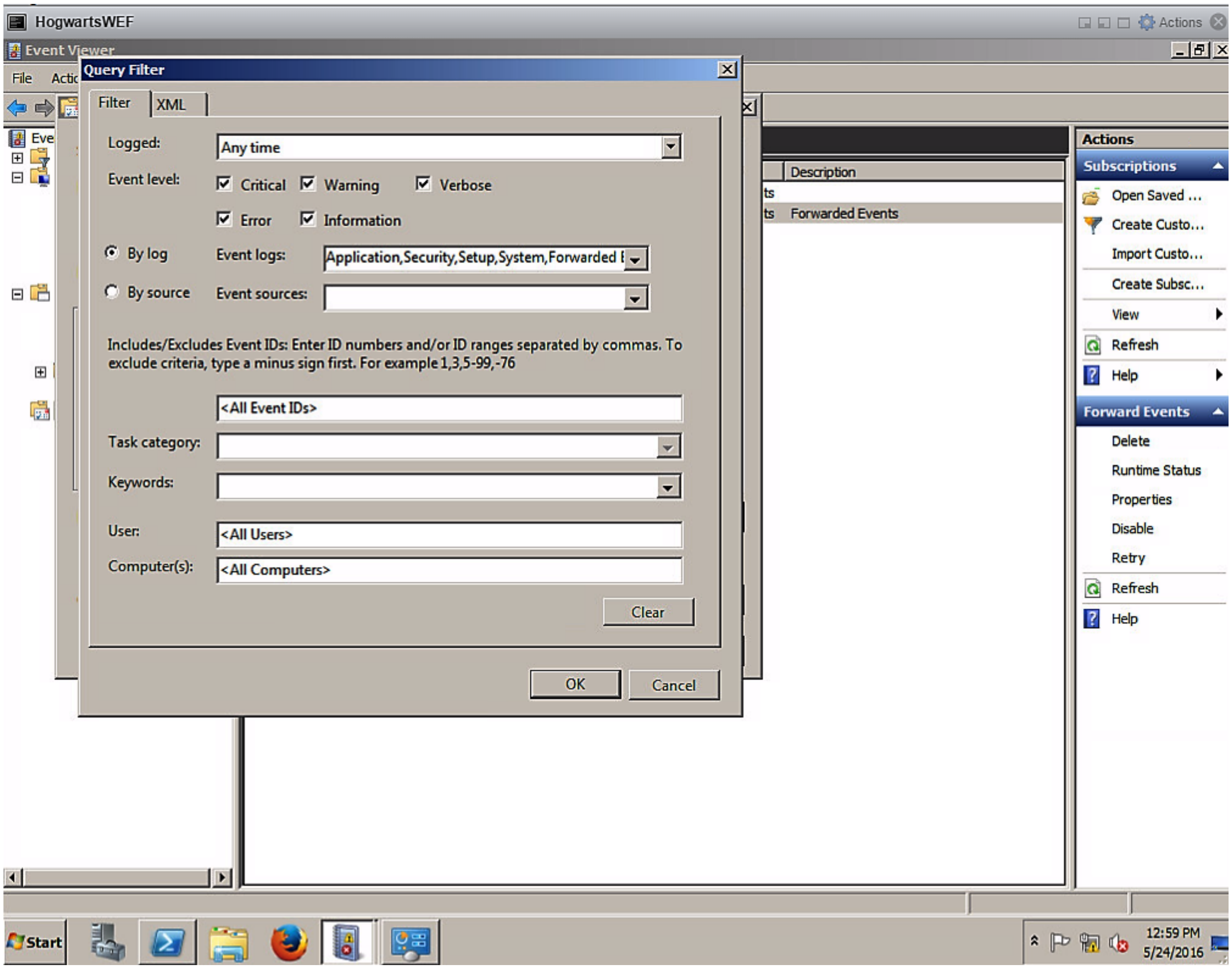
● Source computer initiated — Select Computer Groups...

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect: Select Events...

Configure advanced settings: Advanced...

OK Cancel



Logged: Any time

Event level: ☑ Critical ☑ Warning ☑ Verbose ☑ Error ☑ Information

● By log Event logs: Application,Security,Setup,System,Forwarded E

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

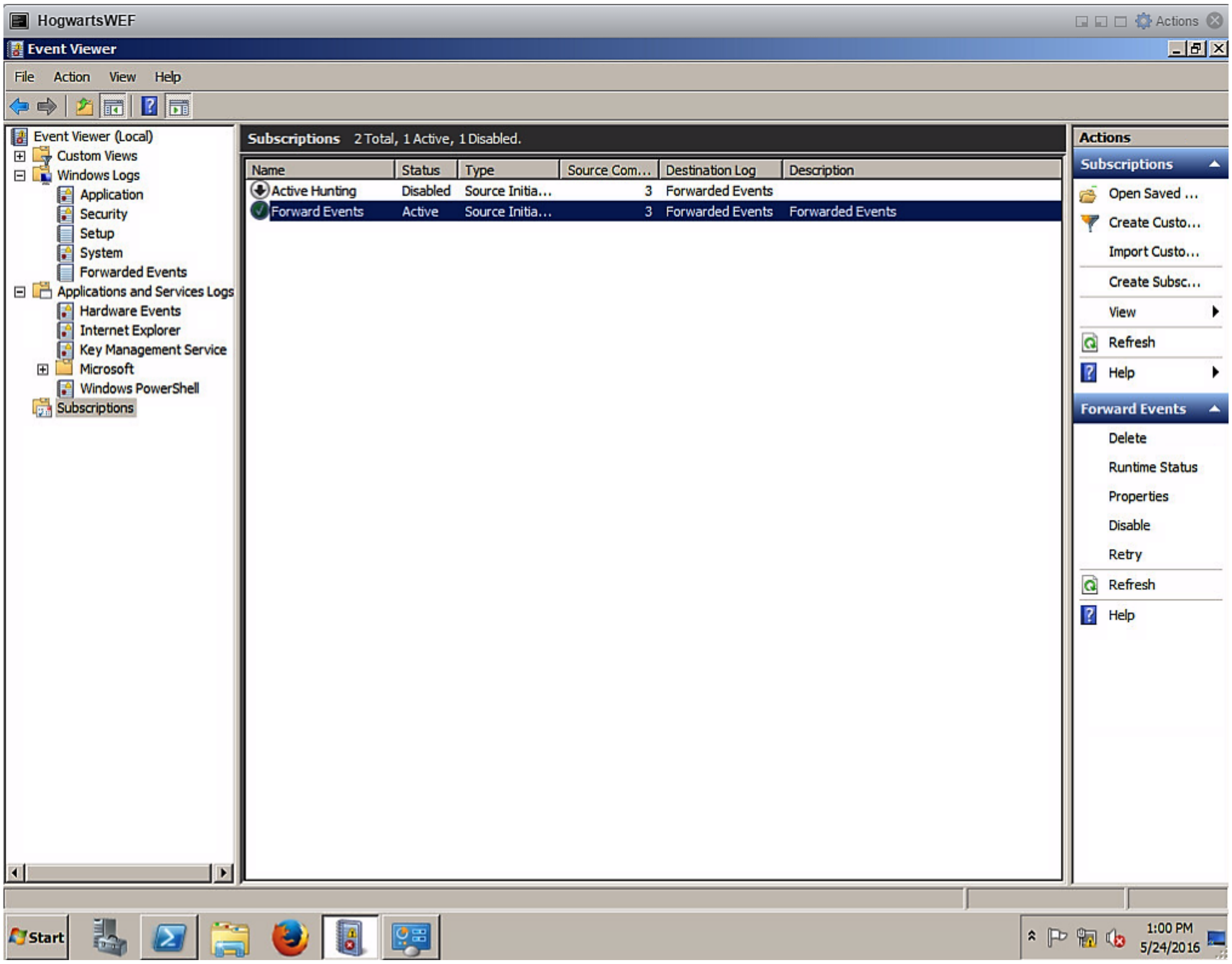
<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>



Subscriptions 2 Total, 1 Active, 1 Disabled.

Name	Status	Type	Source Com...	Destination Log	Description
Active Hunting	Disabled	Source Initia...	3	Forwarded Events	
Forward Events	Active	Source Initia...	3	Forwarded Events	Forwarded Events

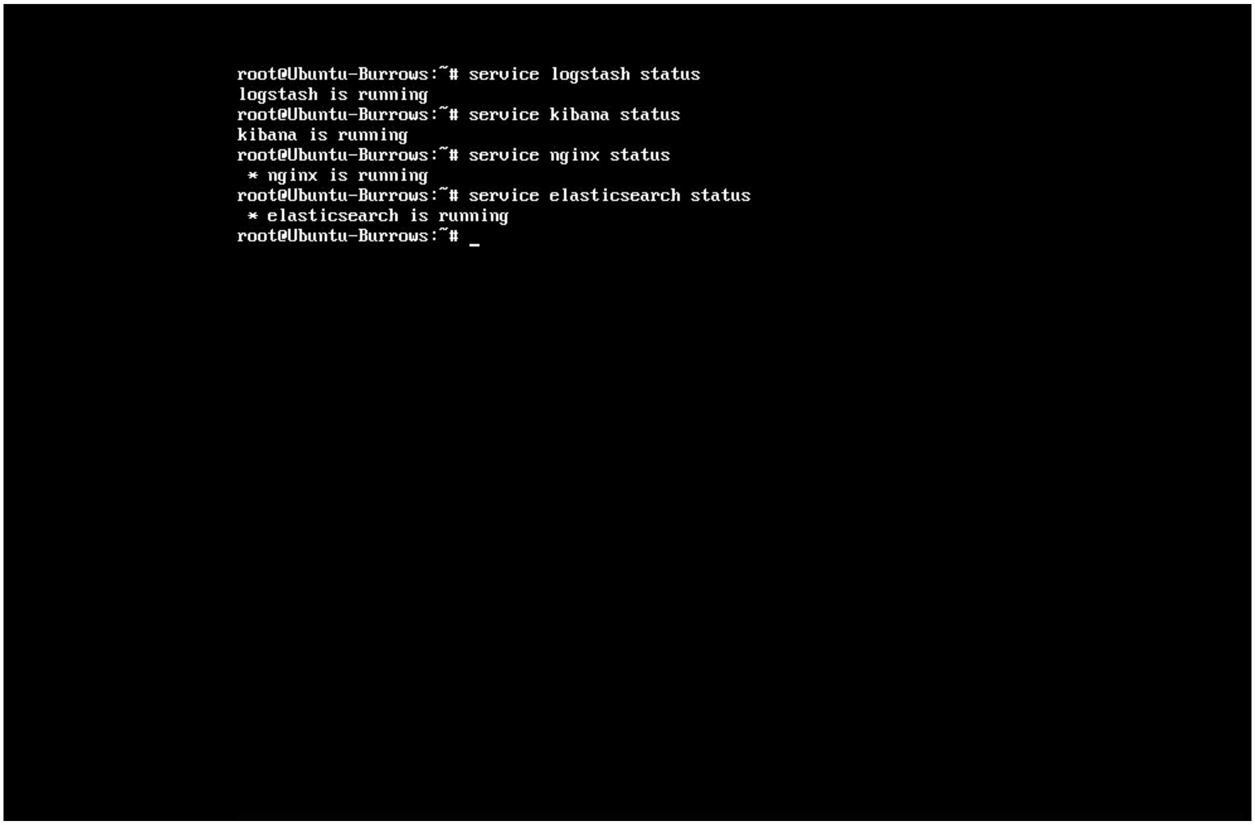
3.5 ELK Server

An Ubuntu 14.04 Server hosts ELK. The following tools and softwares are installed on it along with their respective latest updates

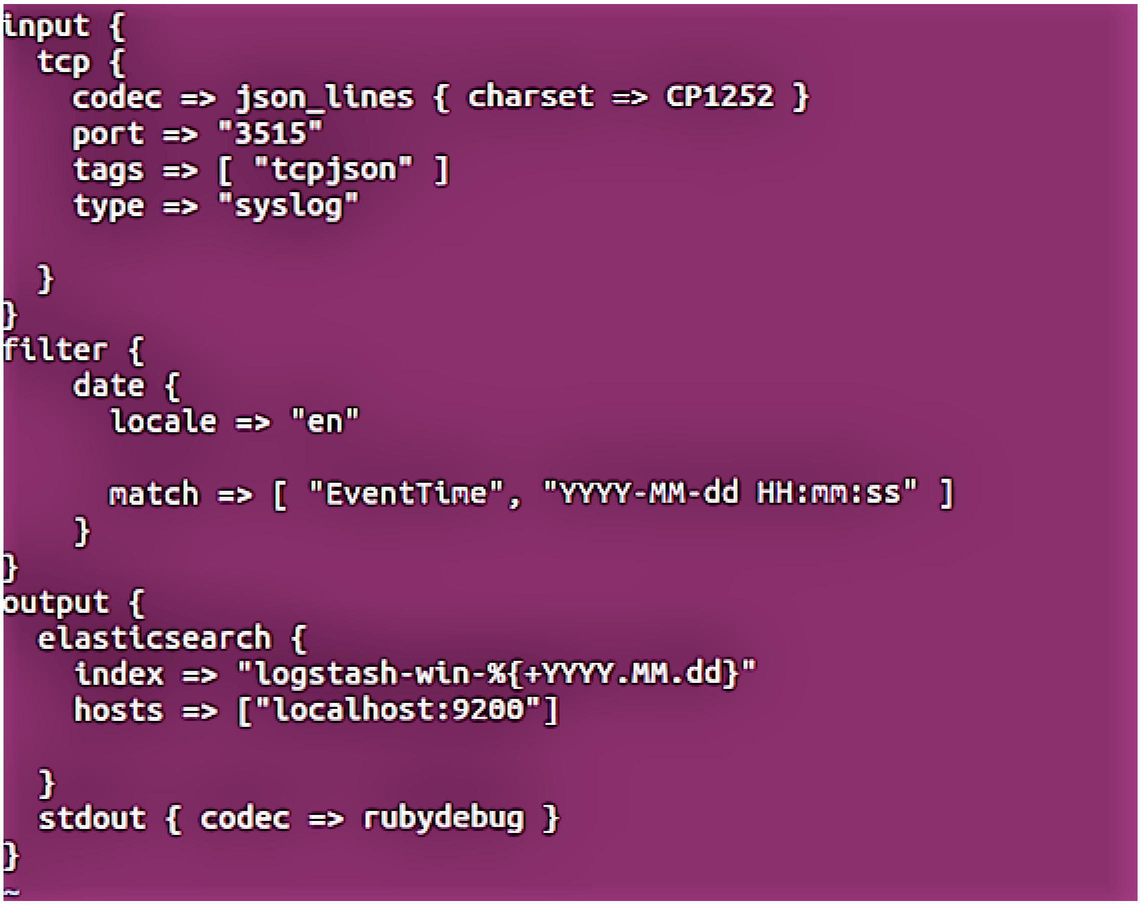
1. Java 8
2. Elasticsearch 2.2.x
3. Kibana 4.4.x
4. Nginx and Apache2-utils
5. Logstash 2.2.x

Incoming logs from WEF are stored into logstash and in turn passed to Elasticsearch with the provided config for analysis. Kibana is configured to listen on “localhost” and Nginx is installed to set up a reverse proxy to allow external access to it.

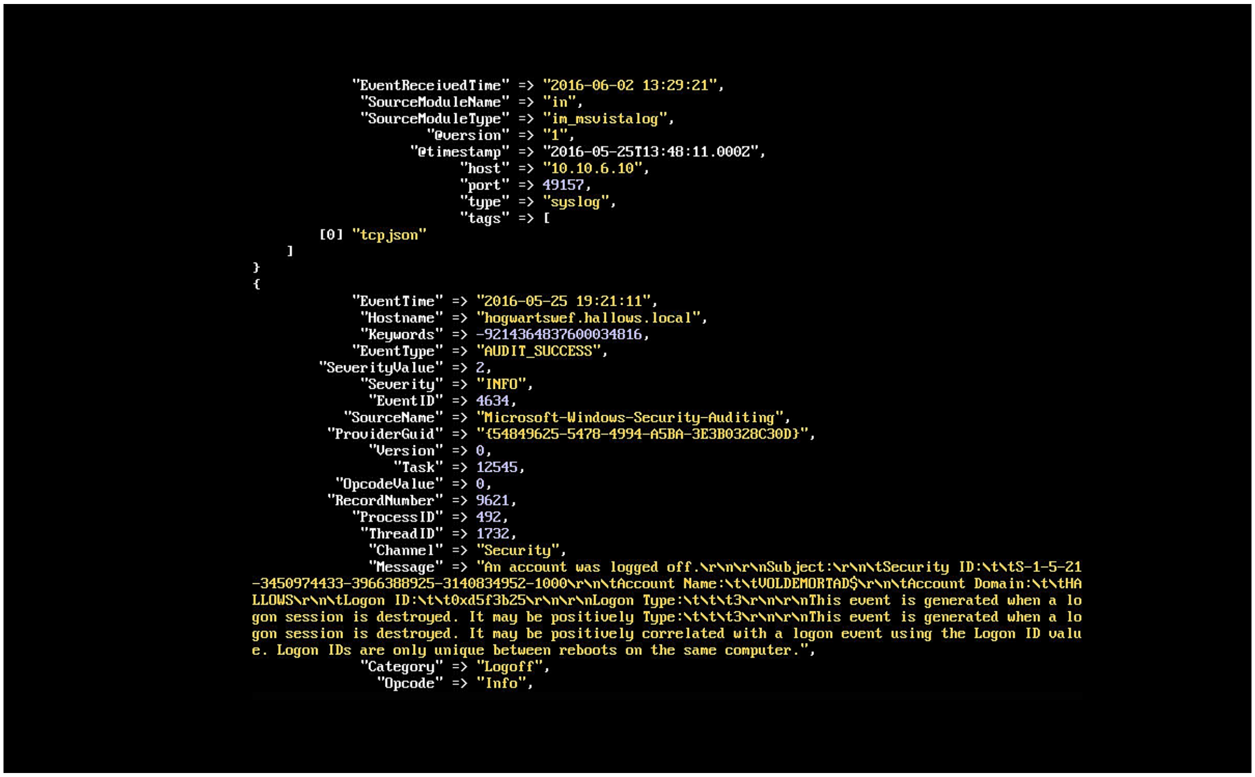
After starting all the aforementioned services on the ELK server, a configuration file is loaded into logstash to specifying the plugins for input,filters and output. Multiple configuration files can loaded to create several customised indexes.



```
root@Ubuntu-Burrows:~# service logstash status
logstash is running
root@Ubuntu-Burrows:~# service kibana status
kibana is running
root@Ubuntu-Burrows:~# service nginx status
 * nginx is running
root@Ubuntu-Burrows:~# service elasticsearch status
 * elasticsearch is running
root@Ubuntu-Burrows:~# _
```



```
input {
  tcp {
    codec => json_lines { charset => CP1252 }
    port => "3515"
    tags => [ "tcpjson" ]
    type => "syslog"

  }
}
filter {
    date {
      locale => "en"

      match => [ "EventTime", "YYYY-MM-dd HH:mm:ss" ]
    }
}
output {
  elasticsearch {
    index => "logstash-win-%{+YYYY.MM.dd}"
    hosts => ["localhost:9200"]

  }
  stdout { codec => rubydebug }
}
~
```



```
            "EventReceivedTime" => "2016-06-02 13:29:21",
             "SourceModuleName" => "in",
             "SourceModuleType" => "im_msvistalog",
                     "@version" => "1",
                   "@timestamp" => "2016-05-25T13:48:11.000Z",
                         "host" => "10.10.6.10",
                         "port" => 49157,
                         "type" => "syslog",
                         "tags" => [
        [0] "tcpjson"
    ]
}
{
            "EventTime" => "2016-05-25 19:21:11",
             "Hostname" => "hogwartswef.hallows.local",
             "Keywords" => -9214364837600034816,
            "EventType" => "AUDIT_SUCCESS",
        "SeverityValue" => 2,
             "Severity" => "INFO",
              "EventID" => 4634,
           "SourceName" => "Microsoft-Windows-Security-Auditing",
         "ProviderGuid" => "{54849625-5478-4994-A5BA-3E3B0328C30D}",
              "Version" => 0,
                 "Task" => 12545,
          "OpcodeValue" => 0,
         "RecordNumber" => 9621,
            "ProcessID" => 492,
             "ThreadID" => 1732,
              "Channel" => "Security",
              "Message" => "An account was logged off.\r\n\r\nSubject:\r\n\tSecurity ID:\t\tS-1-5-21
-3450974433-3966388925-3140834952-1000\r\n\tAccount Name:\t\tVOLDEMORTAD$\r\n\tAccount Domain:\t\tHA
LLOWS\r\n\tLogon ID:\t\t0xd5f3b25\r\n\r\nLogon Type:\t\t\t3\r\n\r\nThis event is generated when a lo
gon session is destroyed. It may be positively Type:\t\t\t3\r\n\r\nThis event is generated when a lo
gon session is destroyed. It may be positively correlated with a logon event using the Logon ID valu
e. Logon IDs are only unique between reboots on the same computer.",
             "Category" => "Logoff",
               "Opcode" => "Info",
```

4. Breach Simulations

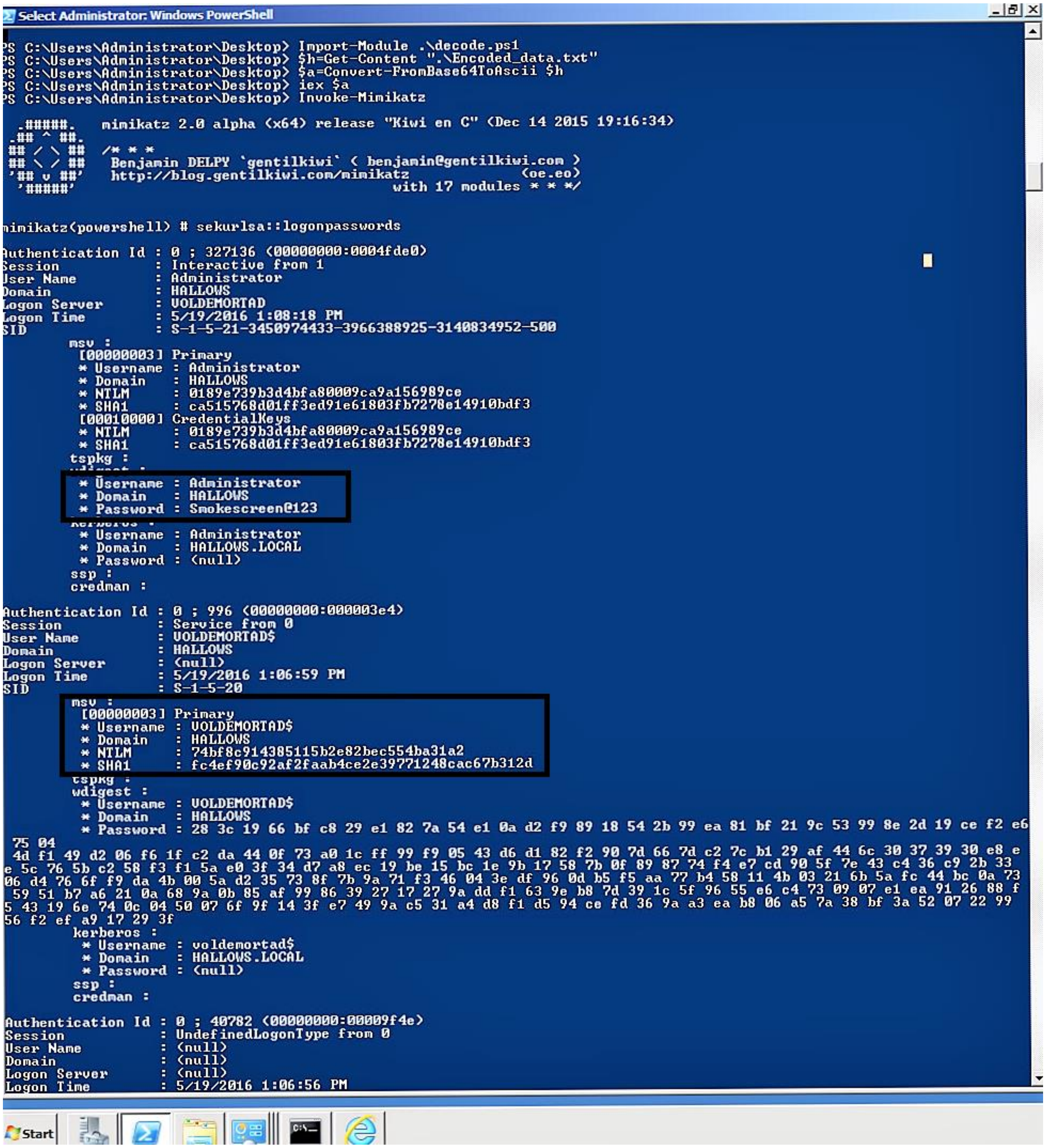
In order to simulate active hunting, we will perform certain attacks on the domain which in turn will be logged and forwarded as Windows Events, warnings or errors and show up in Kibana by adding the required filters.

5.1 Powershell Attacks

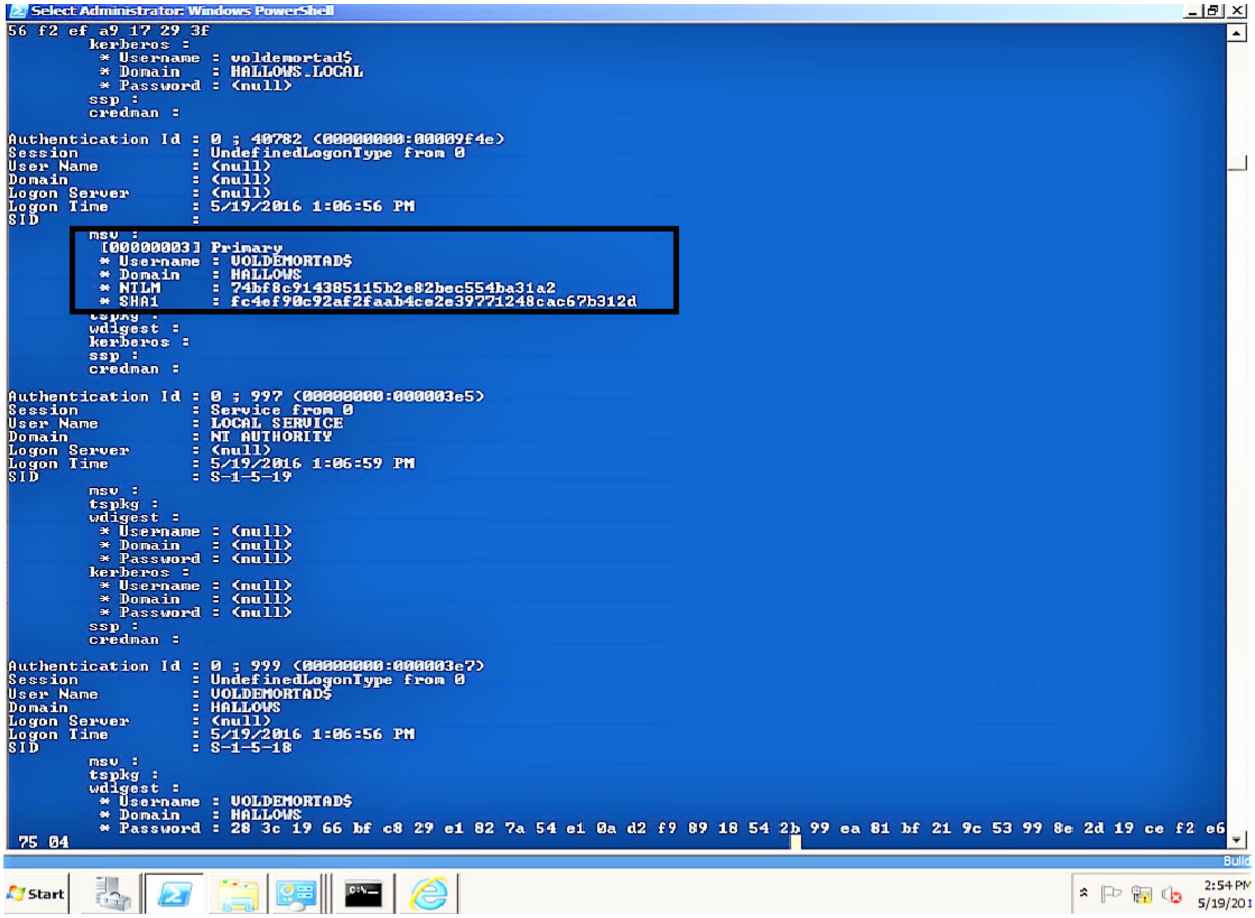
Windows Powershell (PS) is a legitimate tool in Windows. It is seldom used to carry out internal lateral movement and PS scripts are used to attack the system as they do not raise a red flag.

This is a Powershell attack to obtain the access credentials of a system by dumping the Active Directory logs and goes undetected by the system. We track this Powershell activity as it anomalous to be coming from certain domain computers which are not supposed to use Powershell

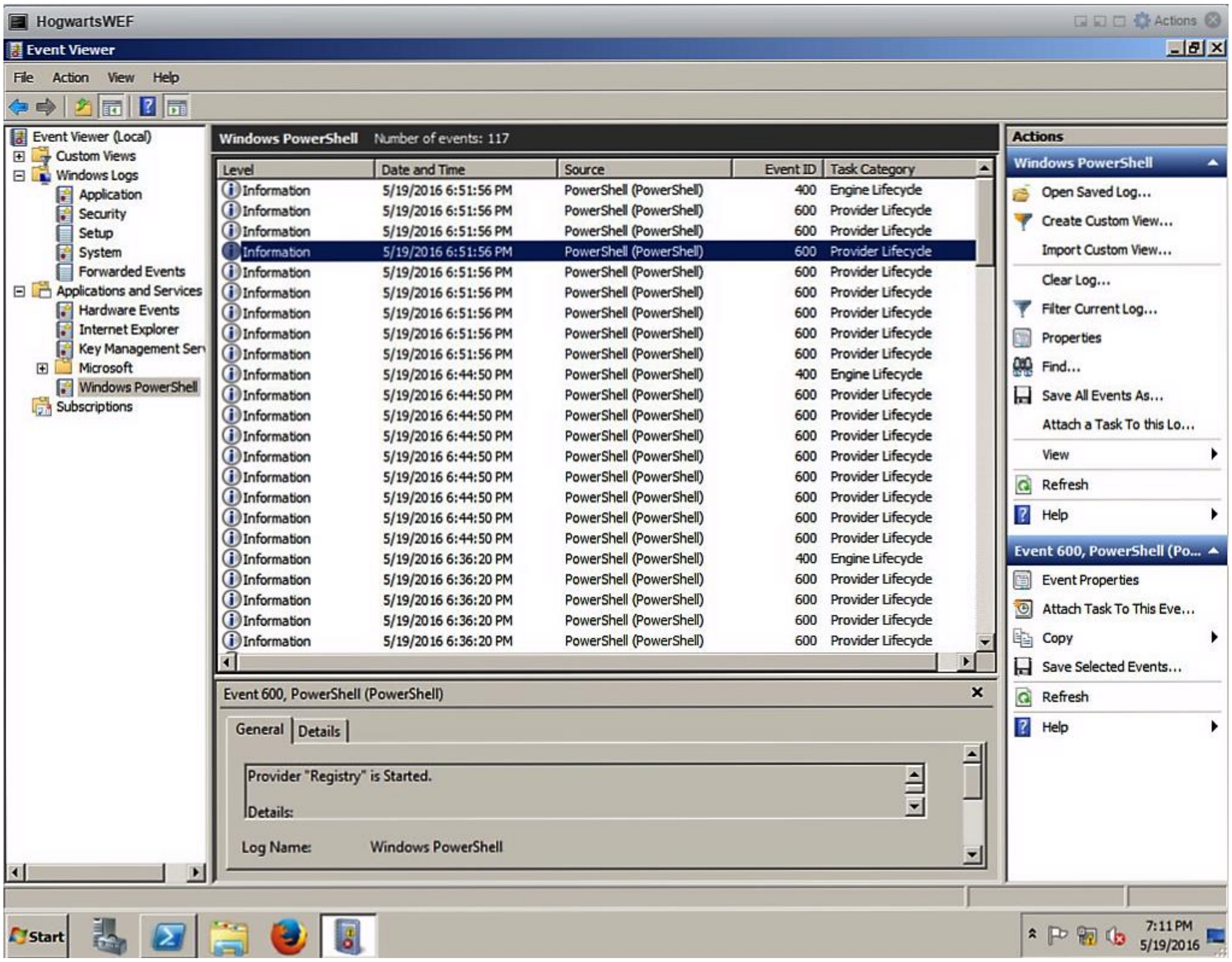
Mimikatz is the tool used for this purpose. Mimikatz,if executed directly, is caught by Windows Defender. We encode it as a Base64 string to bypass Windows security.



```
PS C:\Users\Administrator\Desktop> Import-Module .\decode.ps1
PS C:\Users\Administrator\Desktop> $h=Get-Content ".\Encoded_data.txt"
PS C:\Users\Administrator\Desktop> $a=Convert-FromBase64ToAscii $h
PS C:\Users\Administrator\Desktop> iex $a
PS C:\Users\Administrator\Desktop> Invoke-Mimikatz

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Dec 14 2015 19:16:34)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 17 modules * * */

mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 327136 (00000000:0004fde0)
Session           : Interactive from 1
User Name         : Administrator
Domain            : HALLOWS
Logon Server      : VOLDEMORTAD
Logon Time        : 5/19/2016 1:08:18 PM
SID               : S-1-5-21-3450974433-3966388925-3140834952-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : HALLOWS
         * NTLM     : 0189e739b3d4bfa80009ca9a156989ce
         * SHA1     : ca515768d01ff3ed91e61803fb7278e14910bdf3
         [00010000] CredentialKeys
         * NTLM     : 0189e739b3d4bfa80009ca9a156989ce
         * SHA1     : ca515768d01ff3ed91e61803fb7278e14910bdf3
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : HALLOWS
         * Password : Smokescreen@123
        kerberos :
         * Username : Administrator
         * Domain   : HALLOWS.LOCAL
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : VOLDEMORTAD$
Domain            : HALLOWS
Logon Server      : (null)
Logon Time        : 5/19/2016 1:06:59 PM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : VOLDEMORTAD$
         * Domain   : HALLOWS
         * NTLM     : 74bf8c914385115b2e82bec554ba31a2
         * SHA1     : fc4ef90c92af2faab4ce2e39771248cac67b312d
        tspkg :
        wdigest :
         * Username : VOLDEMORTAD$
         * Domain   : HALLOWS
         * Password : 28 3c 19 66 bf c8 29 e1 82 7a 54 e1 0a d2 f9 89 18 54 2b 99 ea 81 bf 21 9c 53 99 8e 2d 19 ce f2 e6
 75 04
 4d f1 49 d2 06 f6 1f c2 da 44 0f 73 a0 1c ff 99 f9 05 43 d6 d1 82 f2 90 7d 66 7d c2 7c b1 29 af 44 6c 30 37 39 30 e8 e
e 5c 76 5b c2 58 f3 f1 5a e0 3f 34 d7 a8 ec 19 be 15 bc 1e 9b 17 58 7b 0f 89 87 74 f4 e7 cd 90 5f 7e 43 c4 36 c9 2b 33
06 d4 76 6f f9 da 4b 00 5a d2 35 73 8f 7b 9a 71 f3 46 04 3e df 96 0d b5 f5 aa 77 b4 58 11 4b 03 21 6b 5a fc 44 bc 0a 73
 59 51 b7 a6 21 0a 68 9a 0b 85 af 99 86 39 27 17 27 9a dd f1 63 9e b8 7d 39 1c 5f 96 55 e6 c4 73 09 07 e1 ea 91 26 88 f
5 43 19 6e 74 0c 04 50 07 6f 9f 14 3f e7 49 9a c5 31 a4 d8 f1 d5 94 ce fd 36 9a a3 ea b8 06 a5 7a 38 bf 3a 52 07 22 99
56 f2 ef a9 17 29 3f
        kerberos :
         * Username : voldemortad$
         * Domain   : HALLOWS.LOCAL
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 40782 (00000000:00009f4e)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 5/19/2016 1:06:56 PM
```



```
56 f2 ef a9 17 29 3f
         kerberos :
          * Username : voldemortad$
          * Domain   : HALLOWS.LOCAL
          * Password : (null)
         ssp :
         credman :

Authentication Id : 0 ; 40782 (00000000:00009f4e)
Session           : UndefinedLogonType from 0
User Name         : (null)
Domain            : (null)
Logon Server      : (null)
Logon Time        : 5/19/2016 1:06:56 PM
SID               :
         msv :
          [00000003] Primary
          * Username : VOLDEMORTAD$
          * Domain   : HALLOWS
          * NTLM     : 74bf8c914385115b2e82bec554ba31a2
          * SHA1     : fc4ef90c92af2faab4ce2e39771248cac67b312d
         tspkg :
         wdigest :
         kerberos :
         ssp :
         credman :

Authentication Id : 0 ; 997 (00000000:000003e5)
Session           : Service from 0
User Name         : LOCAL SERVICE
Domain            : NT AUTHORITY
Logon Server      : (null)
Logon Time        : 5/19/2016 1:06:59 PM
SID               : S-1-5-19
         msv :
         tspkg :
         wdigest :
          * Username : (null)
          * Domain   : (null)
          * Password : (null)
         kerberos :
          * Username : (null)
          * Domain   : (null)
          * Password : (null)
         ssp :
         credman :

Authentication Id : 0 ; 999 (00000000:000003e7)
Session           : UndefinedLogonType from 0
User Name         : VOLDEMORTAD$
Domain            : HALLOWS
Logon Server      : (null)
Logon Time        : 5/19/2016 1:06:56 PM
SID               : S-1-5-18
         msv :
         tspkg :
         wdigest :
          * Username : VOLDEMORTAD$
          * Domain   : HALLOWS
          * Password : 28 3c 19 66 bf c8 29 e1 82 7a 54 e1 0a d2 f9 89 18 54 2b 99 ea 81 bf 21 9c 53 99 8e 2d 19 ce f2 e6
 75 04
```



Windows PowerShell Number of events: 117

Level	Date and Time	Source	Event ID	Task Category
Information	5/19/2016 6:51:56 PM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	5/19/2016 6:51:56 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:51:56 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:51:56 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:51:56 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:51:56 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:51:56 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:51:56 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:51:56 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:44:50 PM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	5/19/2016 6:44:50 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:44:50 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:44:50 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:44:50 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:44:50 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:44:50 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:44:50 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:44:50 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:36:20 PM	PowerShell (PowerShell)	400	Engine Lifecycle
Information	5/19/2016 6:36:20 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:36:20 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:36:20 PM	PowerShell (PowerShell)	600	Provider Lifecycle
Information	5/19/2016 6:36:20 PM	PowerShell (PowerShell)	600	Provider Lifecycle

Event 600, PowerShell (PowerShell)

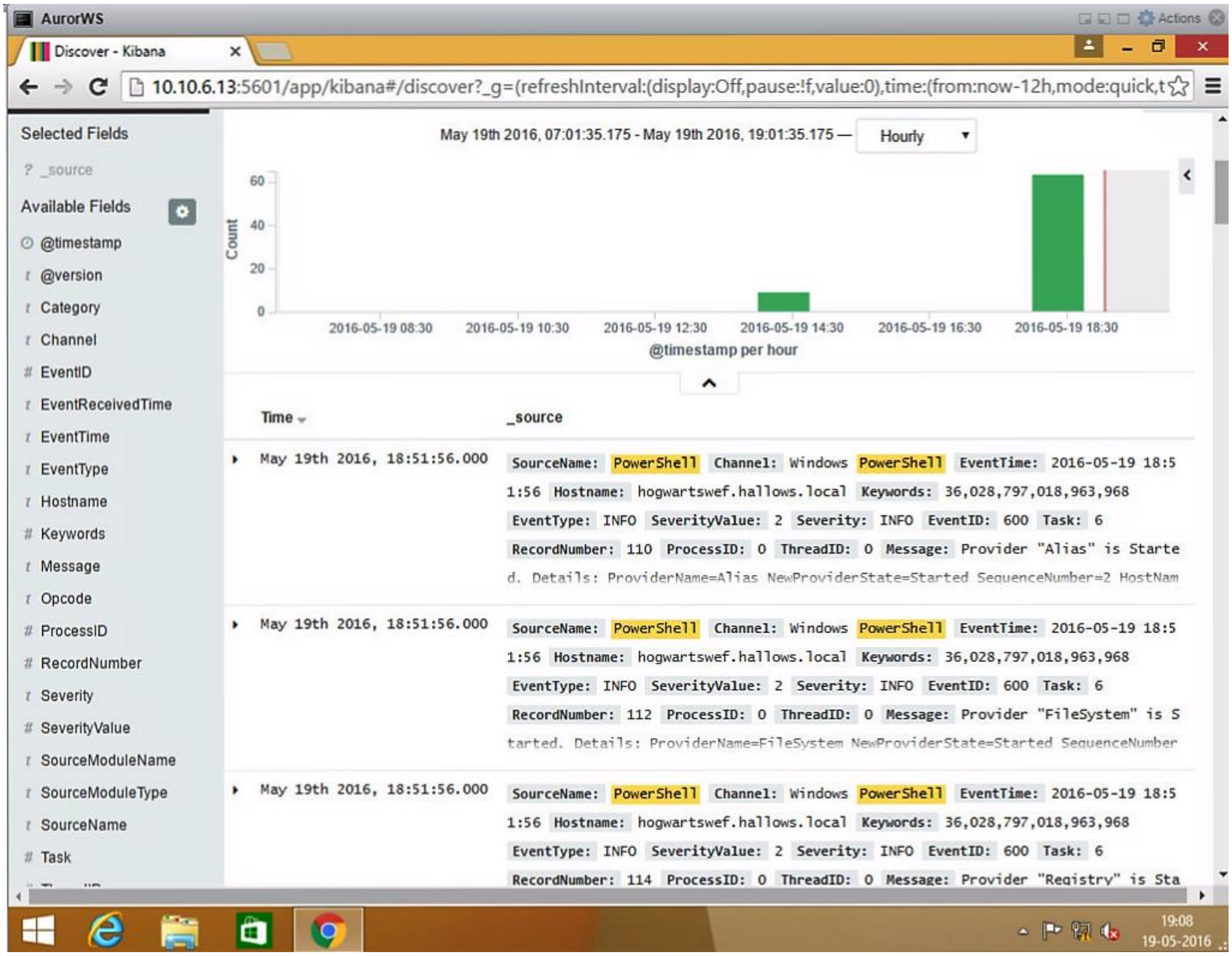
General | Details

Provider "Registry" is Started.

Details:

Log Name: Windows PowerShell

PS Tracked on Kibana

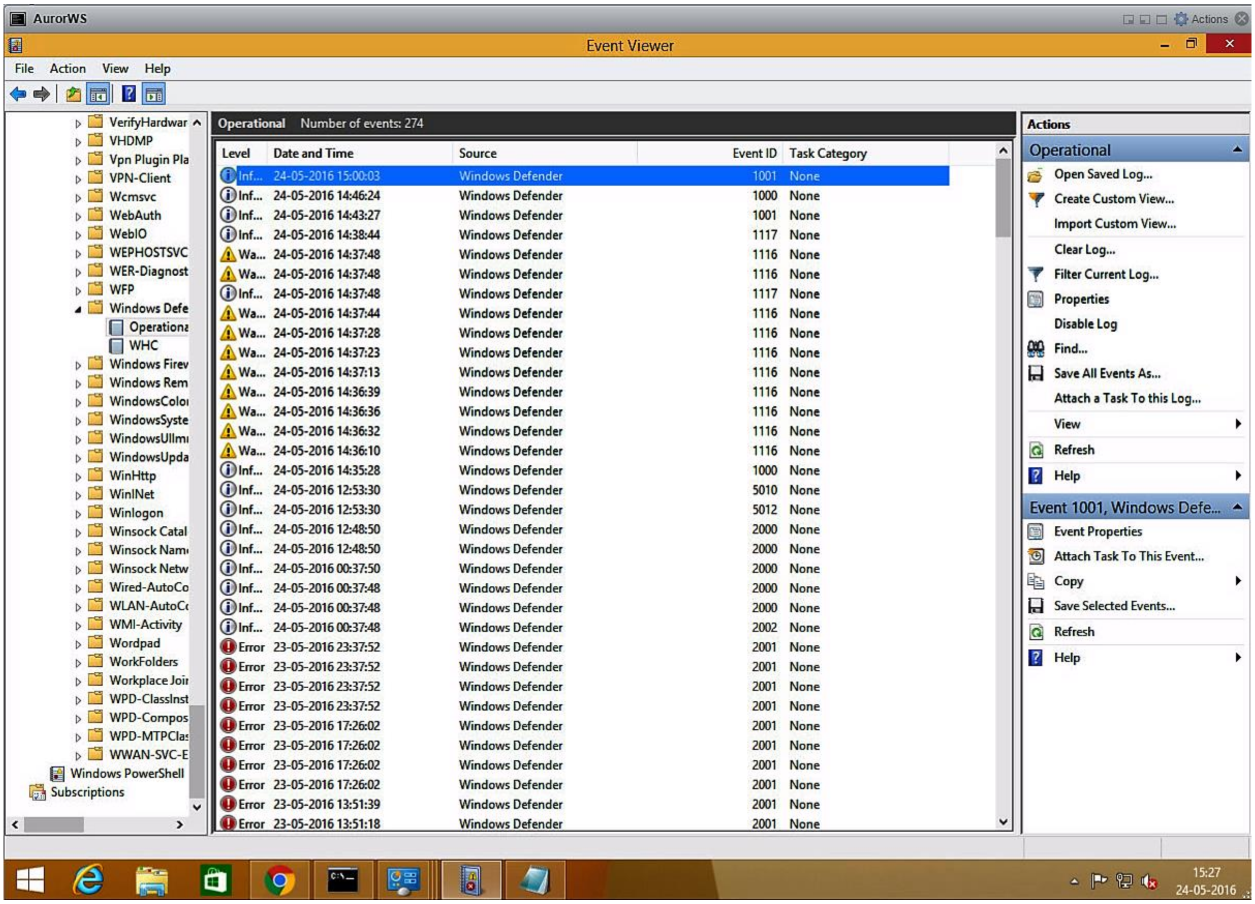


```
May 19th 2016, 18:51:56.000   SourceName: PowerShell Channel: Windows PowerShell EventTime: 2016-05-19 18:5
                              1:56 Hostname: hogwartswef.hallows.local Keywords: 36,028,797,018,963,968
                              EventType: INFO SeverityValue: 2 Severity: INFO EventID: 600 Task: 6
                              RecordNumber: 110 ProcessID: 0 ThreadID: 0 Message: Provider "Alias" is Starte
                              d. Details: ProviderName=Alias NewProviderState=Started SequenceNumber=2 HostNam

May 19th 2016, 18:51:56.000   SourceName: PowerShell Channel: Windows PowerShell EventTime: 2016-05-19 18:5
                              1:56 Hostname: hogwartswef.hallows.local Keywords: 36,028,797,018,963,968
                              EventType: INFO SeverityValue: 2 Severity: INFO EventID: 600 Task: 6
                              RecordNumber: 112 ProcessID: 0 ThreadID: 0 Message: Provider "FileSystem" is S
                              tarted. Details: ProviderName=FileSystem NewProviderState=Started SequenceNumber

May 19th 2016, 18:51:56.000   SourceName: PowerShell Channel: Windows PowerShell EventTime: 2016-05-19 18:5
                              1:56 Hostname: hogwartswef.hallows.local Keywords: 36,028,797,018,963,968
                              EventType: INFO SeverityValue: 2 Severity: INFO EventID: 600 Task: 6
                              RecordNumber: 114 ProcessID: 0 ThreadID: 0 Message: Provider "Registry" is Sta
```

5.2 Triggering Windows Defender

Known malware files are downloaded which are caught and deleted by windows defender before they are opened. These triggers are logged as Windows events as warnings and critical errors and they can be filtered in Elasticsearch and looked up in Kibana using their Event IDs.

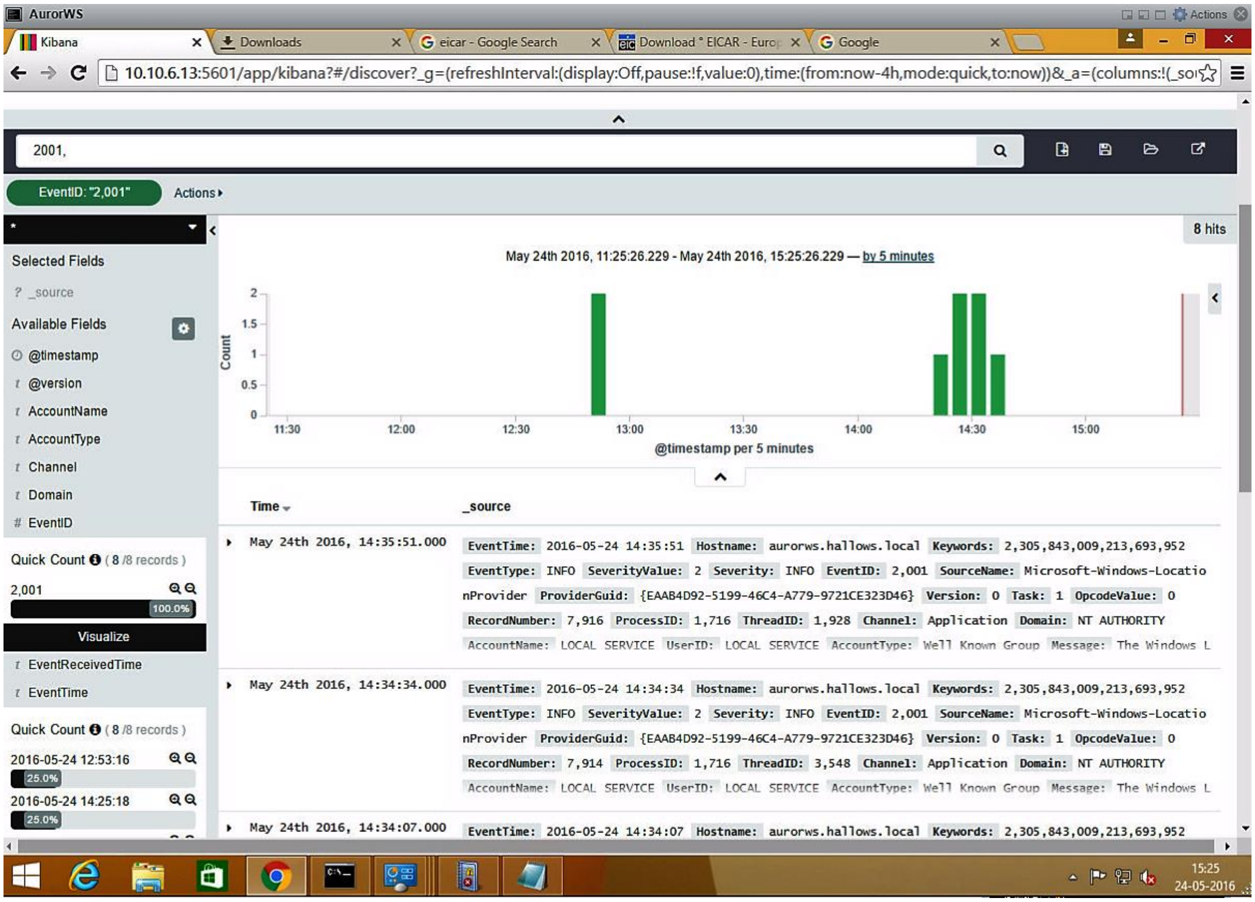
Windows Defender Logs in Event Viewer



Operational Number of events: 274

Level	Date and Time	Source	Event ID	Task Category
Inf...	24-05-2016 15:00:03	Windows Defender	1001	None
Inf...	24-05-2016 14:46:24	Windows Defender	1000	None
Inf...	24-05-2016 14:43:27	Windows Defender	1001	None
Inf...	24-05-2016 14:38:44	Windows Defender	1117	None
Wa...	24-05-2016 14:37:48	Windows Defender	1116	None
Wa...	24-05-2016 14:37:48	Windows Defender	1116	None
Inf...	24-05-2016 14:37:48	Windows Defender	1117	None
Wa...	24-05-2016 14:37:44	Windows Defender	1116	None
Wa...	24-05-2016 14:37:28	Windows Defender	1116	None
Wa...	24-05-2016 14:37:23	Windows Defender	1116	None
Wa...	24-05-2016 14:37:13	Windows Defender	1116	None
Wa...	24-05-2016 14:36:39	Windows Defender	1116	None
Wa...	24-05-2016 14:36:36	Windows Defender	1116	None
Wa...	24-05-2016 14:36:32	Windows Defender	1116	None
Wa...	24-05-2016 14:36:10	Windows Defender	1116	None
Inf...	24-05-2016 14:35:28	Windows Defender	1000	None
Inf...	24-05-2016 12:53:30	Windows Defender	5010	None
Inf...	24-05-2016 12:53:30	Windows Defender	5012	None
Inf...	24-05-2016 12:48:50	Windows Defender	2000	None
Inf...	24-05-2016 12:48:50	Windows Defender	2000	None
Inf...	24-05-2016 00:37:50	Windows Defender	2000	None
Inf...	24-05-2016 00:37:48	Windows Defender	2000	None
Inf...	24-05-2016 00:37:48	Windows Defender	2000	None
Inf...	24-05-2016 00:37:48	Windows Defender	2002	None
Error	23-05-2016 23:37:52	Windows Defender	2001	None
Error	23-05-2016 23:37:52	Windows Defender	2001	None
Error	23-05-2016 23:37:52	Windows Defender	2001	None
Error	23-05-2016 23:37:52	Windows Defender	2001	None
Error	23-05-2016 17:26:02	Windows Defender	2001	None
Error	23-05-2016 17:26:02	Windows Defender	2001	None
Error	23-05-2016 17:26:02	Windows Defender	2001	None
Error	23-05-2016 17:26:02	Windows Defender	2001	None
Error	23-05-2016 13:51:39	Windows Defender	2001	None
Error	23-05-2016 13:51:18	Windows Defender	2001	None

Windows Defender Tracked in Kibana Using Event ID



```
10.10.6.13:5601/app/kibana?#/discover?_g=(refreshInterval:(display:Off,pause:!f,value:0),time:(from:now-4h,mode:quick,to:now))&_a=(columns:!(_so
```

2001,

EventID: "2,001"

May 24th 2016, 11:25:26.229 - May 24th 2016, 15:25:26.229 — by 5 minutes

Quick Count (8 /8 records)

2,001 100.0%

Quick Count (8 /8 records)

2016-05-24 12:53:16 25.0%

2016-05-24 14:25:18 25.0%

```
May 24th 2016, 14:35:51.000  EventTime: 2016-05-24 14:35:51 Hostname: aurorws.hallows.local Keywords: 2,305,843,009,213,693,952
                             EventType: INFO SeverityValue: 2 Severity: INFO EventID: 2,001 SourceName: Microsoft-Windows-Locatio
                             nProvider ProviderGuid: {EAAB4D92-5199-46C4-A779-9721CE323D46} Version: 0 Task: 1 OpcodeValue: 0
                             RecordNumber: 7,916 ProcessID: 1,716 ThreadID: 1,928 Channel: Application Domain: NT AUTHORITY
                             AccountName: LOCAL SERVICE UserID: LOCAL SERVICE AccountType: Well Known Group Message: The Windows L

May 24th 2016, 14:34:34.000  EventTime: 2016-05-24 14:34:34 Hostname: aurorws.hallows.local Keywords: 2,305,843,009,213,693,952
                             EventType: INFO SeverityValue: 2 Severity: INFO EventID: 2,001 SourceName: Microsoft-Windows-Locatio
                             nProvider ProviderGuid: {EAAB4D92-5199-46C4-A779-9721CE323D46} Version: 0 Task: 1 OpcodeValue: 0
                             RecordNumber: 7,914 ProcessID: 1,716 ThreadID: 3,548 Channel: Application Domain: NT AUTHORITY
                             AccountName: LOCAL SERVICE UserID: LOCAL SERVICE AccountType: Well Known Group Message: The Windows L

May 24th 2016, 14:34:07.000  EventTime: 2016-05-24 14:34:07 Hostname: aurorws.hallows.local Keywords: 2,305,843,009,213,693,952
```

Advantages of Active Hunting with ELK

1. Splunk (similar data logging and analysis tool) costs millions of dollars as data collected by organizations. ELK open-source and hence free.
2. Logs are complicated to read.

   Log= data + timestamp

   They are difficult to read and comprehend and as they are not parsed. ELK allows you to ELK allows you to select individual fields according to your preference.
3. Configuration files can be customized to your needs.
4. It is neither limited as grep nor complicated as RegEx.
5. Active hunting secures an organization’s intranet from internal compromise.

CONCLUSIONS

1. ELK stack is an open source, neatly compiled, state of the art tool for data logging and analytics.
2. Corporations are deploying it as it saves them millions of dollars.
3. It is not complicated as grep or RegEx.
4. Kibana is a text, not script based search dashboard which allows ease of use.

Bibliography

References:

1. https://www.digitalocean.com/community/tutorials/how-to-install-elasticsearch-logstash-and-kibana-elk-stack-on-ubuntu-14-04
2. http://packages.elastic.co
3. http://joshuadlewis.blogspot.in/2014/10/advanced-threat-detection-with-sysmon_74.html
4. http://www.eicar.org/85-0-Download.html
5. https://www.youtube.com/watch?v=U3m0jKygAqU
6. https://www.youtube.com/watch?v=Kqs7UcCJquM
7. https://www.youtube.com/watch?v=7d54zc6WPLc
8. https://www.youtube.com/watch?v=96og3aIgyrc&list=PLhLSfisesZIvA8ad1J2DSdLWnTPtzWSfI
9. https://www.elastic.co/guide/en/logstash/current/configuration.html
10. https://sematext.com/blog/2013/12/19/getting-started-with-logstash/