



Detecting BloodHound



February 11, 2019

My original post is no longer available. I have posted it on my personal blog now. It's a couple of years old, but I have been asked about it so here it is:

Regardless of what attack life cycle you follow there are couple items which everyone can agree on:

- 1. Companies have to assume they are already compromised.
- 2. The earlier in the lifecycle that you can catch an attacker the lower the overall cost of remediation will be.

After a host is compromised, the attacker has to create a command and control channel, establish persistence and start to do internal reconnaissance.

SpectorOps continues to raise the bar with the way they (ab)use PowerShell for reconnaissance, lateral movement, and privilege exploitation. Their tools are meant to mimic advanced attackers and help the blue team see how they can improve. Many red teams/pentesters use their tools and at least one hacker, Phineas Fisher, used it when he successfully hacked Hacking Team.

BloodHound

John Lambert’s blog post “[Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.](#)” explains it well:

“Defenders don’t have a list of assets—they have a graph. Assets are connected to each other by security relationships. Attackers breach a network by landing somewhere in the graph using a technique such as spearphishing and they hack, finding vulnerable systems by navigating the graph.”

BloodHound takes Active Directory reconnaissance and exploitation down a slightly different path through the use of graph theory. By using graph theory and applying it to information extracted from Active Directory, they are able to see how many hops and the exact path it takes to get to a Domain Admin. This allows them to focus on specific targets to keep their noise at a minimum.

As defenders, this tool can be used to identify the ways their environments would allow an attacker to get to Domain Admin and possibly eliminate some of the easier paths, but just because the easy path(s) can perhaps be removed doesn’t mean that we shouldn’t be watching for this type of activity though.

Detection Through Dissection

As we look at various ways to detect Bloodhound and tools like it we need to keep a few things in mind:

- Don’t look for signatures/hashes of a file. While this may have some merit, it is too easy to bypass. Just because a vendor does it doesn’t mean it’s a good choice:



- The ratio of false positives/actual attacks

No matter how much defenders get right, there is the never-ending game of cat and mouse as the attackers continually find ways to bypass enforcement and/or detection. At Derbycon 6, Ben OXA’s talk, “PowerShell Secrets and Tactics,” goes into some of these bypasses. Casey Smith (@subtee) regularly posts innovative ways to run PowerShell without running powershell.exe or bypassing AppLocker policies to get PowerShell scripts to run.

To get a better understanding of what BloodHound is doing and how/where to detect it we need to do a few things:

1. Set up a lab environment that will allow us to run BloodHound and get some ideas of how it works. For this, I have set up a Windows 2012R2 Domain Controller, a Windows 2012 R2 member server, a Windows 2012 R2 server with SQL 2012 and a Windows 10 client. All of them are part of the ‘learning.net’ domain. To make it a little more realistic, I created 20,000 users and 20,000 groups.
2. Look at the source code4, read the Github Wiki5, and watch the presentation6.
3. To see the events in near real-time, I set up ArcSight ESM 6.9.1c Patch1 and am using the ArcSight SmartConnector (Windows Native) to monitor the security, application and system logs of the domain controller.

Bloodhound is broken up into two distinct parts: data ingestion (i.e. gathering/pilfering) and data visualization. Data gathering can be done by itself with the output sent to CSV files or sent right into the backend Neo4J graph database.

Under the hood BloodHound’s reconnaissance is a specialized version of Powerview7. One of the exciting features of Powerview is that it only needs Powershell version 2.0 to work; no additional modules or RSTAT (Remote Server Administration Tools). This means that it can run by default on any Windows 7 or newer OS. It can also be run by a regular user on the network. There are no exclusive rights required to get the information.

While there are eight different collection methods, all of them the enumerate the users and groups. All of this enumeration is done using LDAP (Lightweight Directory Access Protocol) via ADSI (Active Directory Services Interface). From a defensive standpoint, this is a nightmare since there is no logging for this, as we will see during the testing.

To start understanding when we run BloodHound, we are going to enable Windows Event Logging on the Domain Controller. To enable all the categories/subcategories for both success and failure auditing, I run the command “AUDITPOL /SET /CATEGORY:* /SUCCESS:ENABLE /FAILURE:ENABLE.” To validate that everything is set properly I run the command “AUDITPOL /GET CATEGORY:*”.

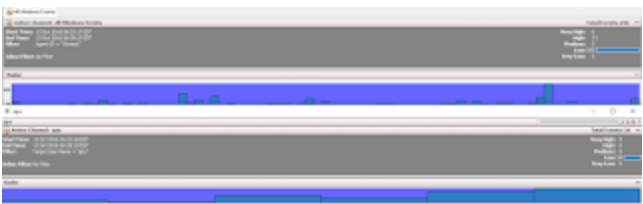
System audit policy Category/Subcategory	Setting
Security System Extension	Success and Failure
System Integrity	Success and Failure
System Driver	Success and Failure
System System Events	Success and Failure
Security State Change	Success and Failure
Logon/Logoff	Success and Failure
Logoff	Success and Failure
Account Lockout	Success and Failure
Process Main Mode	Success and Failure
Process Switch Mode	Success and Failure
Process Extended Mode	Success and Failure
Special Logon	Success and Failure
Other Logon/Logoff Events	Success and Failure
Network Policy Server	Success and Failure
User / Service Claims	Success and Failure
Object Access	Success and Failure
File System	Success and Failure
Registry	Success and Failure
Process Object	Success and Failure
COM	Success and Failure
Certification Services	Success and Failure
Application Generated	Success and Failure
Handle Manipulation	Success and Failure
File Share	Success and Failure
Filtering Platform Packet Drop	Success and Failure
Filtering Platform Connections	Success and Failure
Other Object Access Events	Success and Failure
Remote File Share	Success and Failure
Removable Storage	Success and Failure
Control Panel Settings	Success and Failure
Privilege Use	Success and Failure
Non-Sensitive Privilege Use	Success and Failure
Other Privilege Use Events	Success and Failure
Sensitive Privilege Use	Success and Failure
Process Creation	Success and Failure
Process Termination	Success and Failure
WMI Activity	Success and Failure
RPC Events	Success and Failure
Policy Change	Success and Failure
Authentication Policy Change	Success and Failure
Authorization Policy Change	Success and Failure
NTFS File-Level Policy Change	Success and Failure
Filtering Platform Policy Change	Success and Failure
Other Policy Change Events	Success and Failure
Mail Policy Change	Success and Failure
Account Management	Success and Failure
Group Account Management	Success and Failure
Computer Account Management	Success and Failure
Security Group Management	Success and Failure
Directory Group Management	Success and Failure
Application Group Management	Success and Failure
Other Account Management Events	Success and Failure
AD Access	Success and Failure
Directory Service Changes	Success and Failure
Directory Service Replication	Success and Failure
Directory Service Replication	Success and Failure
Directory Service Access	Success and Failure
Network Logon	Success and Failure
Network Service Ticket Operations	Success and Failure
Other Account Logon Events	Success and Failure
Directory Authentication Service	Success and Failure
Credential Validation	Success and Failure

Before I run BloodHound, I baseline the events. I have two separate continuous active channels running; one for all Windows events and one for “Target UserName = apu” (the account I am using to test with). The number of events generated before running BloodHound is minimal as seen in the screenshots below.

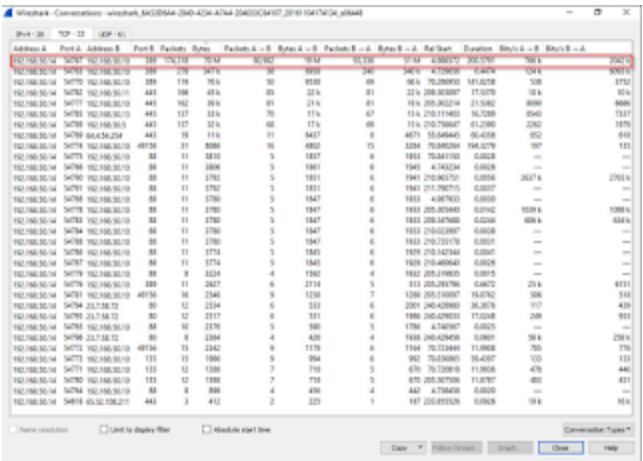


Before I run BloodHound, I will start Wireshark with no capture filters applied to see what we can learn about its traffic

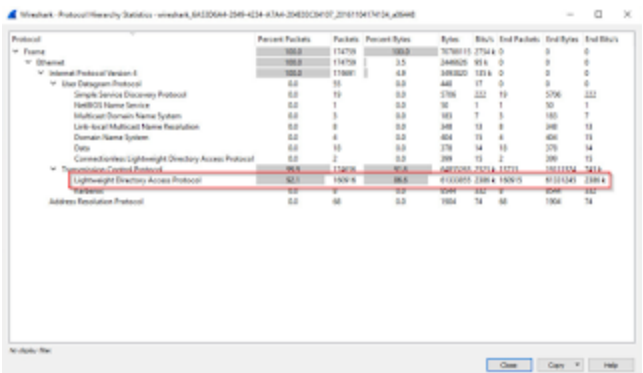
BloodHound.



Using Wireshark to generate some statistics on the capture we can notice that there is one particular conversation that is significantly larger than the rest. At 70M it is larger than the rest of the TCP flows combined.



Looking at the protocol breakdown of the traffic we can see that most of it is LDAP (TCP port 389).



Using the information we gained from the event logging and Wireshark we can see that regular event logging is not going to provide us with any events that would be useful. The reason for this is all the traffic is LDAP (Lightweight Directory Access Protocol) related and will not trigger any Kerberos or NTLM (NT Lan Manager) events outside of a logon event when the LDAP query first authenticates.

Network Traffic Analysis

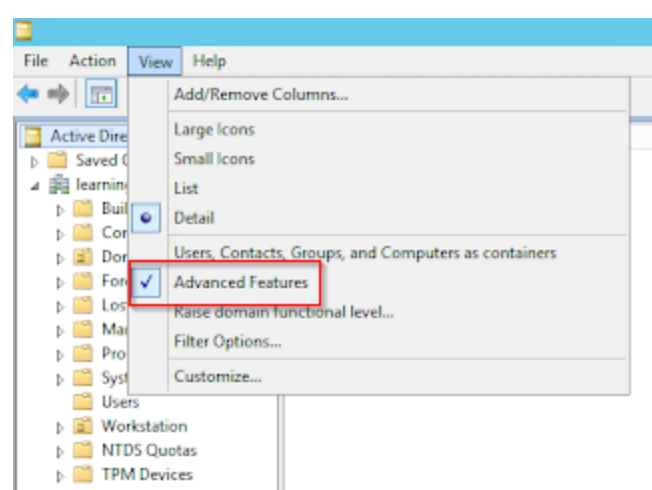
If you have flow (NetFlow/sflow) logs you can look for high volumes of LDAP traffic to your DC’s or if you have firewalls between your DC’s and parts of the network that you want to monitor for you can enable a rule that would log that traffic and look for high volumes of LDAP traffic. You will also want to look for LDAP sessions that take significantly longer than the rest. Each environment will be different. To see what you should be looking for, run BloodHound in your network while monitoring the traffic with any network capture program and then see how much data was sent (total and each direction) and the time taken for Bloodhound to do its LDAP query(s). Since LDAP is primarily used for searching for information, the queries should be specific to certain item(s), and as a result, they should be quick and transfer minimal amounts of data. The query that BloodHound enumerates all user accounts which is abnormal, especially when it comes from the user segment.

HoneyTokens

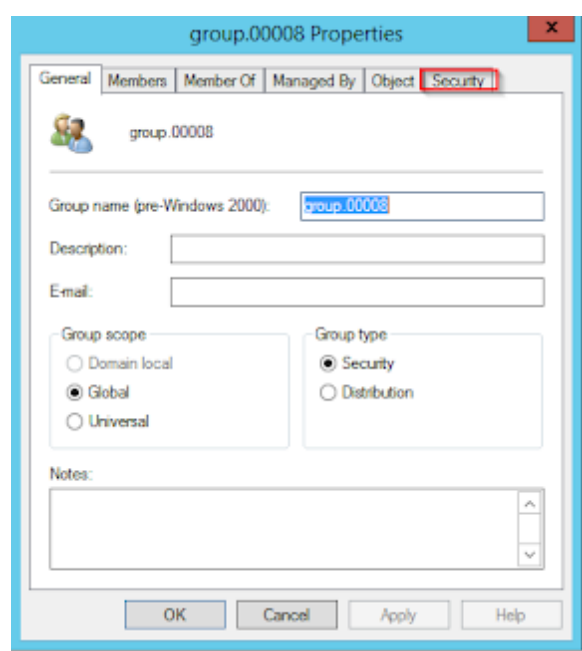
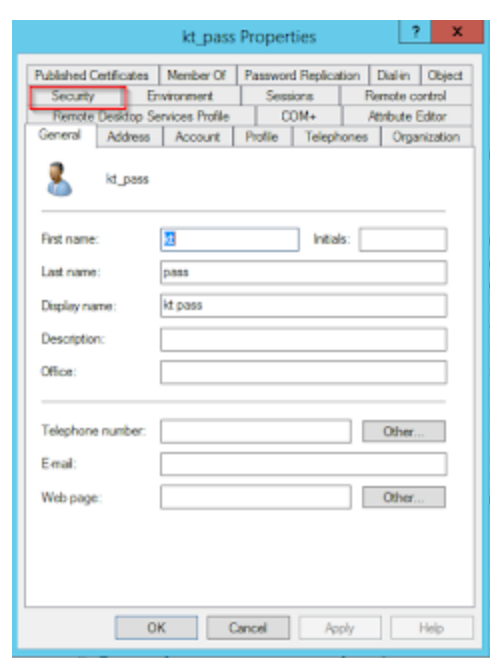
Using honeytokens to detect malicious activity is nothing new. However, the detection is centered around the use of the information, not the enumeration of them. User and groups are directory objects and can be audited just like files/folders giving valuable audit information. To enable this first ensure that the “Directory Service Access” subcategory is enabled under “DS Access.”

- Group accounts should contain regular user accounts as well as honeypot user accounts.

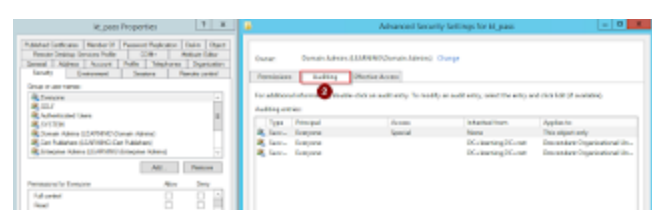
To enable auditing the “Advanced Features” option needs to be enabled on the “Active Directory Users and Computers” MMC.



This will expose the “Security” tab for the object:

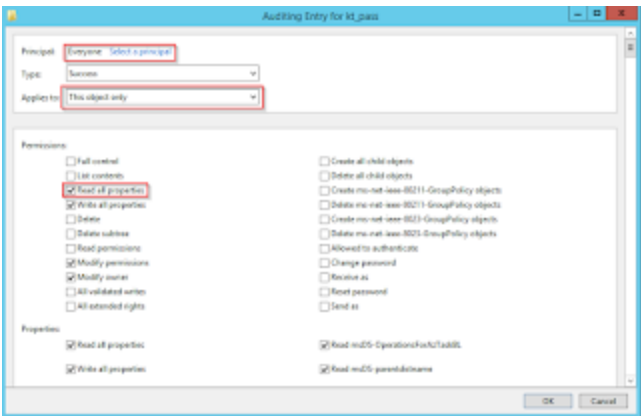


After clicking on the Security tab click on “Advanced (1)-> Auditing (2) -> Add (3)”

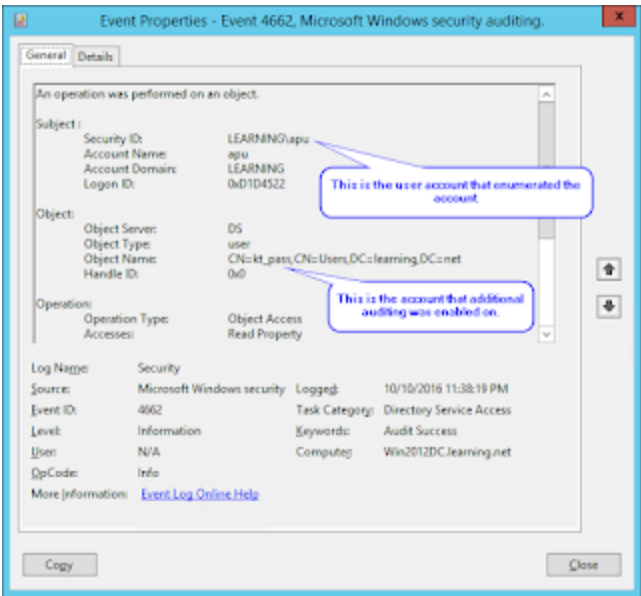
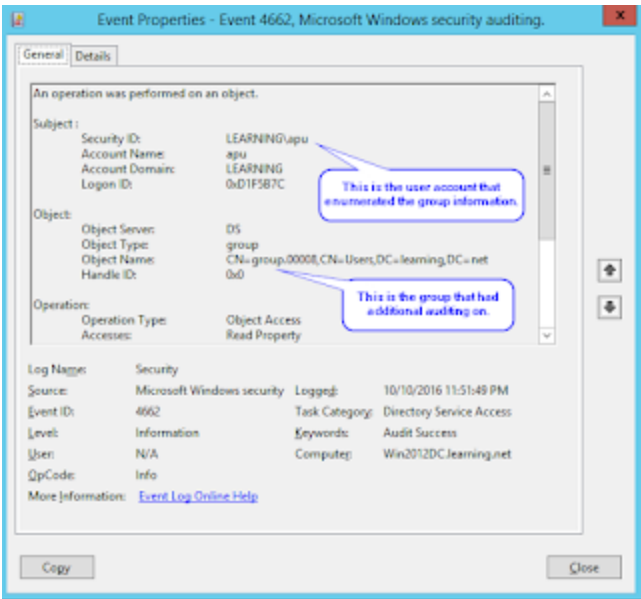


Set the following properties:

- Principal = Everyone
- Applies to = This object only
- Permissions = Read all properties



After enabling all the proper settings event ID 4662's will be logged anytime one of these objects is enumerated.



Before the logs can be consumed by ESM there are some customizations that need to be done on the Connector. The information shown in the Event Viewer is easy to digest, but when viewing the “Details” tab you will see the events in their raw form.

```
+ System
- EventData
  SubjectUserSid S-1-5-21-511651333-3180284375-749010354-1610
  SubjectUserName apu
  SubjectDomainName LEARNING
  SubjectLogonId 0x1c3cc93
  ObjectServer DS
  ObjectType %[bf967aba-0de6-11d0-a285-00aa003049e2]
  ObjectName %[57b69bfb-dda6-46be-976b-1e6e37f6b58e]
  OperationType Object Access
  HandleId 0x0
  AccessList %[7684
```

As you can see the GUIDs for “ObjectType” and “ObjectName” are given. While the SmartConnector can look up GUIDs there can be some issues with this (i.e. unresolved GUID, GUID not found, GUID lookup timeout, etc.) in a busy environment. Since this information is critical for us I added a parser override to normalize the GUID and a two map files: one to map the schema GUID’s (user and group) and one to map the user/group specific information. A zip file with the three files is provided at the end of this post.

After the auditing is turned on I run BloodHound again to see what information is logged. There were 37 4662 audit events generated.

This gives us the user name of the person who enumerated the objects, not the host/IP/device that they are on. A simple pivot off the user name will give us possibly compromised hosts. When first implementing this, a one week bake in period should be observed. During this time investigate any accounts that are enumerating AD user/group objects and document them. There will be servers/applications that need to do this type of activity as part of their function, but they should be filtered out after have been vetted.

Conclusion

With BloodHound advancing the state of internal reconnaissance and being nearly invisible we need to understand how it works to see where we can possibly detect it. By moving the detection to the network and AD event logs, we can stay hidden. Attackers can't see the monitoring or even know they are monitored until they have triggered the events. By dissecting the tool, we can better understand the functionality and then monitor for that instead of signatures that are easily defeated.



Kayal March 28, 2019 at 1:38 AM

Really too good! This is much more helps to grow my knowledge. I got huge info in this blog, the author was done the well said and I like this blog.

- Tableau Training in Chennai
Tableau Course in Chennai
Excel Training in Chennai
Corporate Training in Chennai
Pega Training in Chennai
Power BI Training in Chennai
Embedded System Course Chennai
Linux Training in Chennai
Tableau Training in Chennai
Tableau Course in Chennai

REPLY



sandeep saxena May 3, 2019 at 4:59 AM

Good job. This will be useful for others who want to know more about technology. Useful one.

- Spring Training in Chennai
Spring framework Training in Chennai
spring Training in Anna Nagar
Hibernate Training in Chennai
Hibernate course in Chennai
Struts Training in Chennai
Wordpress Training in Chennai
Spring Training in Chennai

REPLY



chandhran March 12, 2020 at 2:53 AM

[AWS Training in Bangalore](#)
[Data Science Courses in Bangalore](#)
[DevOps Training in Bangalore](#)
[PHP Training in Bangalore](#)
[REPLY](#)



jeya sofia *March 27, 2020 at 6:27 AM*

Nice article you have posted here.Thank you for sharing this information. Share more like this.
[RPA Training in T nagar](#)
[RPA Training in Anna Nagar](#)
[Software testing training in Tambaram](#)
[Dot Net Training in Velachery](#)
[Web Designing Course in T Nagar](#)
[Spoken English Classes in Velachery](#)
[German Classes in T Nagar](#)
[SEO Training in OMR](#)
[AWS Training in Velachery](#)
[Python course in Tambaram](#)

[REPLY](#)



chitra *June 1, 2021 at 2:55 AM*

Intersting Information... keep sharing your blog
[RPA Course in Chennai](#)
[RPA Course in Bangalore](#)

[REPLY](#)



chitra *June 7, 2021 at 5:09 AM*

abulous post... Keep sharing
[Spoken English in Chennai](#)
[English Speaking Courses in Chennai](#)

[REPLY](#)



technews *July 1, 2021 at 5:14 AM*

This site was... how would I say it? Applicable!! At long last I have discovered something that encouraged me. Good wishes![best interiors](#)

[REPLY](#)



chitra *July 8, 2021 at 4:17 AM*

Wonderful Blog.. keep updating
[AWS Training in Chennai](#)
[Amazon web services Training in Chennai](#)
[AWS Training Institutes in Bangalore](#)
[AWS Certification Training in Bangalore](#)

[REPLY](#)



bruce wayne *October 21, 2021 at 5:28 AM*

Great post. Keep sharing such a worthy information
[best java training in chennai](#)

[REPLY](#)



barbrajacek *March 4, 2022 at 10:39 AM*

What are the minimum deposit and withdrawal limits at Casino City
Withdrawal restrictions. In [태백 출장안마](#) accordance with [춘천 출장마사지](#) the rules of Casino [경기도 출장샵](#) City, players must only be at least 10 days before they [울산광역시 출장샵](#) have their funds ready to be [과천 출장마사지](#) processed.

[REPLY](#)

Anonymous *June 3, 2022 at 2:31 AM*

[maltepe toshiba klima servisi](#)
[kadıköy toshiba klima servisi](#)
[beykoz toshiba klima servisi](#)
[üsküdar toshiba klima servisi](#)
[tuzla beko klima servisi](#)



Hi Every One *September 12, 2022 at 10:43 PM*

It may be used to check the network's security or determine whether someone is stealing your WiFi. Hacking is a rather routine task, [Wifi Hack Online](#)

[REPLY](#)



Cyberz Pc *September 12, 2022 at 11:45 PM*

Pandora MOD APK. For those of you looking for a quick way to relax and enjoy your free time, enjoy listening to your favourite songs, radio, or podcasts. [Pandora One APK](#)

[REPLY](#)



Silent Girl *September 14, 2022 at 8:16 AM*

I have not only given my heart away to you, I have also dedicated and given away my soul, my prayers and my very being to you. I don't have anything else left [Good Morning SMS](#)

[REPLY](#)

Anonymous *December 4, 2022 at 12:46 AM*

Many gamers expanded their on-line playing offerings, and bingo operators moved their offerings on-line, positively impacting the market. Major software suppliers to on-line [코인카지노](#) playing websites embrace WagerLogic, Boss Media, Micro-gaming Systems, and World Gaming. Unlike traditional casinos, on-line playing websites usually are not licensed or taxed by state governments. Therefore, they supply no income for social and academic packages.

[REPLY](#)

Anonymous *December 7, 2022 at 12:36 PM*

Following a set of tips for slot recreation improvement will ensure the the} success of the slot recreation. This slot machine tutorial has detailed the steps needed for slot recreation improvement. In addition, extra [바카라사이트](#) info like slot recreation features, advantages, and prices have been defined.

[REPLY](#)



Best Hiking Backpacks *April 9, 2024 at 10:07 AM*

[The Best Hiking Backpack](#)

[REPLY](#)

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

SIGN IN WITH GOOGLE

 [Powered by Blogger](#)

Theme images by [Michael Elkan](#)