

Proxmox Lab: Game of Active Directory - Attacking GOAD

 benheater.com/proxmox-lab-goad-attacking-goad

August 26, 2024

In the final module of the lab, we'll be taking steps to ensure that we can access our attack box in certain conditions and successfully ensure connectivity to Game of Active Directory (GOAD) v3 targets in the lab.

0xBEN

Aug 26, 2024 4 min read

This module is part of a larger project on setting up **Game of Active Directory (GOAD) v3** on Proxmox alongside our existing lab infrastructure. [Click here to be taken back to the project landing page.](#)

Previous Step

[Proxmox Lab: Game of Active Directory - Configure with Ansible](#)

[In this module, we'll be taking steps to configure the Windows hosts in the Proxmox Game of Active Directory lab using Ansible](#)

 [0xBEN0xBEN](#)

Objectives for this Step

Ensure that we can access the target environment using our attack box

Reviewing the Setup

[Reviewing the network diagram](#) for the GOAD environment, note the following about the lab environment

The original lab environment had the following

- VLANs
 - **native** — 10.0.0.0/24 (LAN)
 - **666** — 10.6.6.0/24 (SEC_EGRESS)
 - **999** — 10.9.9.0/24 (SEC_ISOLATED)
 - **80** — 10.80.80.0/24 (AD_LAB)
- The attack box is on the **native** VLAN and can reach any of the other VLANs

The GOAD lab environment adds

- VLANs
 - 10 — 192.168.10.0/24 (GOAD)
- The provisioning CT is on native
- The GOAD hosts are on 10
- The attack box can still reach all of the VLANs, including 10

Positioning the Attack Box

Why this Matters

Certain network attacks only work when the attack box is on the same Local Area Network as the target(s), because some attacks require broadcasts and snooping at layer 2.



If the attack box is on 10.0.0.0/24 and the targets are on 192.168.10.0/24, then certain attacks won't work, but there is still a wide variety of attacks you can try on the GOAD lab from this position

Leaving Attack Box on Native VLAN

This will keep the attack box on the pfSense internal LAN of 10.0.0.0/24. In the original lab design we give the attack box — Kali Linux — a DHCP reservation of 10.0.0.2.



If you've configured static routes in your environment, you should be able to access 10.0.0.2 from your home network via SSH or some remote desktop protocol.

Log into your attack box and you should be able to begin the penetration test against the 192.168.10.0/24 network.

Putting Attack Box on VLAN 10

This will move the attack box to VLAN 10 — 192.168.10.0/24 — and put it on the same LAN as the rest of the GOAD hosts.



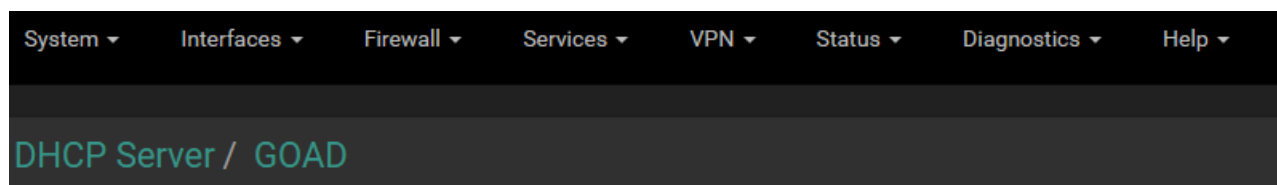
The original lab design does not factor for GOAD, so we have not yet added a static route to the GOAD LAN

Configure the Static Route

Refer to the [documentation on configuring static routes](#) and add the following:

- **Destination Network:** 192.168.10.0/24
- **Gateway:** pfSense WAN IP address


Give Attack Box a DHCP Reservation



Log into your lab pfSense VM and go to Services > DHCP Server > GOAD

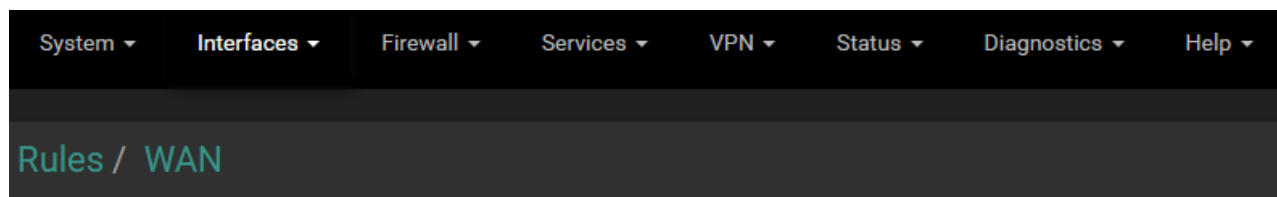
 Add Static Mapping

Click the "Add Static Mapping" button at the bottom of the page

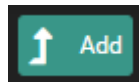
Static DHCP Mapping on GOAD	
DHCP Backend	Kea DHCP
MAC Address	<input type="text" value="3e:b9:3a:4f:24:10"/>  Copy My MAC MAC address of the client to match (6 hex octets separated by colons).
Client Identifier	<input type="text"/> An optional identifier to match based on the value sent by the client (RFC 2132). Kea DHCP will only match on MAC address if both MAC address and client identifier are set for a static reservation.
IP Address	<input type="text" value="192.168.10.2"/> IPv4 address to assign this client. Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool. The same IP address may be assigned to multiple mappings.
ARP Table Static Entry	<input type="checkbox"/> Create an ARP Table Static Entry for this MAC & IP Address pair.
Hostname	<input type="text" value="kali"/> Name of the client host without the domain part.
Description	<input type="text"/> A description for administrative reference (not parsed).

Fill out the mapping details and save, then "Apply Changes"

Configure a WAN Firewall Rule



Go to Firewall > Rules > WAN



Click the "Add (up)" button

Edit Firewall Rule

Action	Pass
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned whereas with block the packet is dropped silently. In either case, the original packet is discarded.	
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	WAN Choose the interface from which packets must come to match this rule.
Address Family	IPv4 Select the Internet Protocol version this rule applies to.
Protocol	Any Choose which IP protocol this rule should match.

Source

Source	<input type="checkbox"/> Invert match	WAN subnets	Source Address
---------------	---------------------------------------	-------------	----------------

Destination

Destination	<input type="checkbox"/> Invert match	Address or Alias	192.168.10.2
--------------------	---------------------------------------	------------------	--------------

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider the Status: System Logs: Settings page).
Description	Allow WAN hosts to reach Kali in GOAD subnet A description may be entered here for administrative reference. A maximum of 52 characters will be used in the rule firewall log.
Advanced Options	Display Advanced

Click "Save" and then, "Apply Changes"

Connecting to Kali on VLAN 10

Now that you've added the firewall rule on the WAN, use a SSH or remote desktop client of your preference and target **192.168.10.2**. With the static route, this will send the traffic to pfSense WAN IP, which will pass the traffic internally to complete the connection.

Connectivity Check

```
(ben@kali-ct)-[~]
$ sudo nmap -Pn -p- --min-rate 5000 192.168.10.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-26 13:02 EDT
Nmap scan report for 192.168.10.12
Host is up (0.00044s latency).
Not shown: 65508 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
```

```
(ben@kali-ct)-[~]
$ sudo nmap -Pn -p389 --script ldap-rootdse 192.168.10.12 | grep 'Naming'
| defaultNamingContext: DC=essos,DC=local
| schemaNamingContext: CN=Schema,CN=Configuration,DC=essos,DC=local
| configurationNamingContext: CN=Configuration,DC=essos,DC=local
| rootDomainNamingContext: DC=essos,DC=local
```

Attacking the Lab

Archives

Yes another pentester blog...

 Mayfly



20 Dec	GOAD - part 12 - Trusts
06 Dec	GOAD - part 11 - ACL
12 Nov	GOAD - part 10 - Delegations
08 Nov	Active Directory Mindmap Upgrade
31 Oct	GOAD - part 9 - Lateral move
02 Oct	GLPI htmlawed (CVE-2022-35914)
24 Sep	GOAD - part 8 - Privilege escalation
11 Sep	GOAD - part 7 - MSSQL
06 Sep	GOAD - part 6 - ADCS
19 Jul	GOAD - part 5 - exploit with user
11 Jul	GOAD - part 4 - poison and relay
06 Jul	GOAD - part 3 - enumeration with user
03 Jul	GOAD - part 2 - find users
02 Jul	GOAD - part 1 - reconnaissance and scan

Head to the link above and follow along with different attacks as demonstrated by Mayfly

Conclusion

That was quite the adventure getting everything built and configured ... 😄

I tried my best to think of most cases where someone reading may get stuck, but if I have missed anything, if there are any errors, please do let me know and I'll work to get it corrected. However, at this point, that should be about it. I hope you have lots of fun pwning GOAD!