DCSM0025

APT Lab Infrastructure

Technology Overview
Design Considerations

Applied Purple Teaming Lab

- We built environment specifically for this course.

- You can build this this same lab your environment with modifications to ensure that your network specifics are similar. Consequently, Lifecycles will be tailored specifically to your environment.

Development is not done in Production

- You can destroy things.
- That would be bad.
- Really bad.
- For all of us.

- So… APT Development Lab

Lifecycles Start In Development

Lifecycles:

- First tested in Lab Environment
- Definite necessary changes in Lab Environment
- Deploy changes in lab environment
- Regression Testing? Have there been adverse effects in the Lab Environment?
- Pilot test changes in production (Change Management)
- Deploy changes to production. (Change Management)
- Retest as Fidelity Check. In Lab and Production

Lifecycles End in Production

Lifecycles:

- Lifecycle output is a Change Control application that lists the necessary changes to deploy changes (or no-changes) in production environment.
- Dependency Review
- UAT testing, etc.

APT Lab Infrastructure

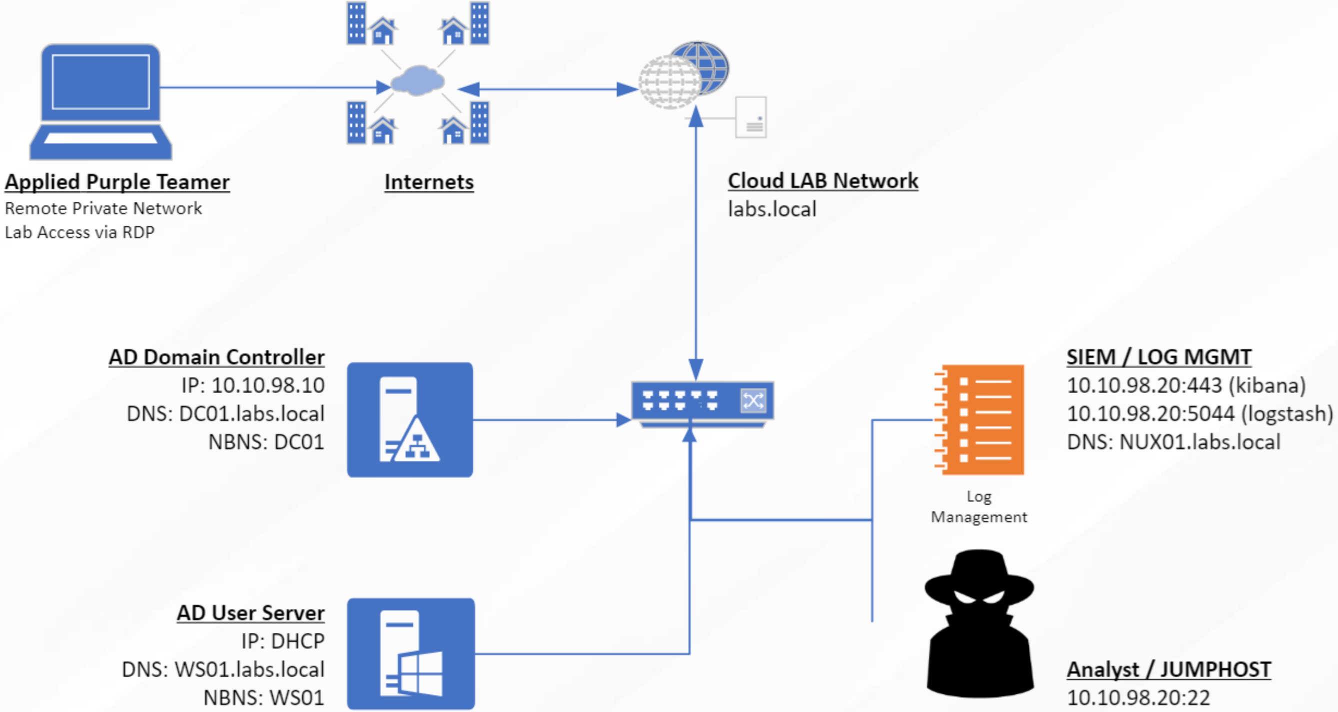
- A smaller network/infrastructure designed similar in nature to your production enterprise networks.

- The environment should use similar network infrastructure, operating system, programming, etc.

Class APT Lab Infrastructure

- Windows 2016 Member Server
- Windows 2016 Domain Controller
- Ubuntu Linux Host
  - HELK SIEM – Kibana, Kafka, Elastic Stack
  - CrackMapExec
  - John The Ripper binaries
  - Impacket toolkit
  - Responder
  - SilentTrinity C2 Framework

APT Lab Infrastructure



Applied Purple Teamer
Remote Private Network
Lab Access via RDP

Internets

Cloud LAB Network
labs.local

AD Domain Controller
IP: 10.10.98.10
DNS: DC01.labs.local
NBNS: DC01

SIEM / LOG MGMT
10.10.98.20:443 (kibana)
10.10.98.20:5044 (logstash)
DNS: NUX01.labs.local

AD User Server
IP: DHCP
DNS: WS01.labs.local
NBNS: WS01

Analyst / JUMPHOST
10.10.98.20:22

All the bits

- Atomic Purple Team Framework (Lifecycle Methodology)
- https://github.com/DefensiveOrigins/AtomicPurpleTeam

- Applied Purple Teaming Threat Optics – Terraform Build
- https://github.com/DefensiveOrigins/APT-Lab-Terraform

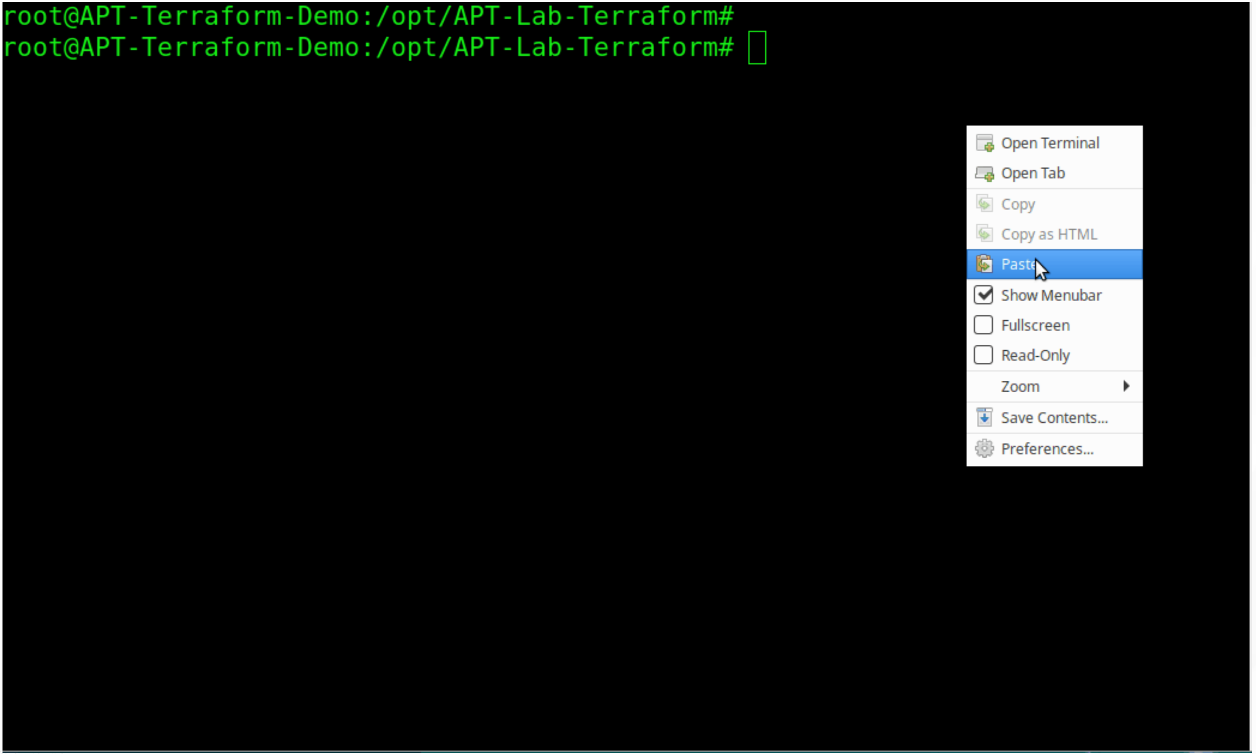
- Applied Purple Teaming Threat Optics – Fast Optic Conifguration
- https://github.com/DefensiveOrigins/APT-Lab-FastOpticsSetup

Start the clock... or... gif?

- How long does it take to build lab in Azure?
  - Domain setup – 10-12 minutes
  - Member server – 5 minutes
  - Linux (HELK) SIEM – 10-12 minutes
  - Threat optics? (secondary, and post-deployment scripts, one per system) - 6-8 minutes

Demo in gif! Step 1: Launch LabBuilder.py

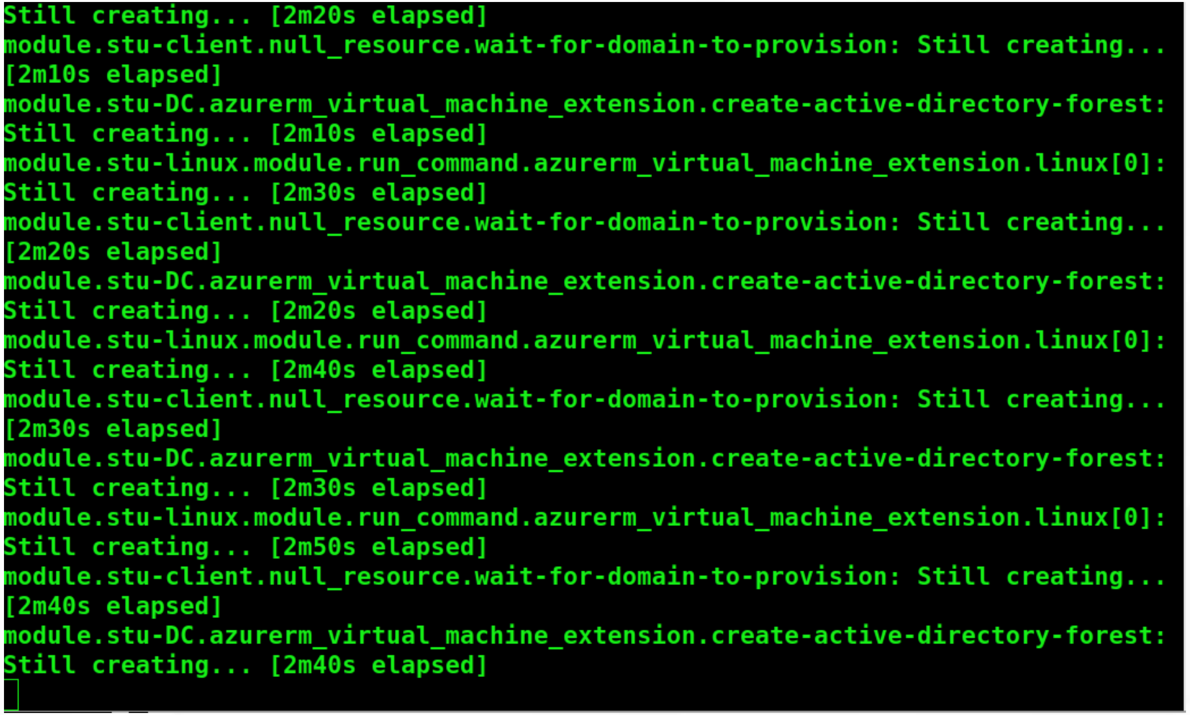
python3 LabBuilder.py -m <yourPubIP>



```
root@APT-Terraform-Demo:/opt/APT-Lab-Terraform#
root@APT-Terraform-Demo:/opt/APT-Lab-Terraform# 
```

Demo in gif! Step 2: Scrolling Rando Text

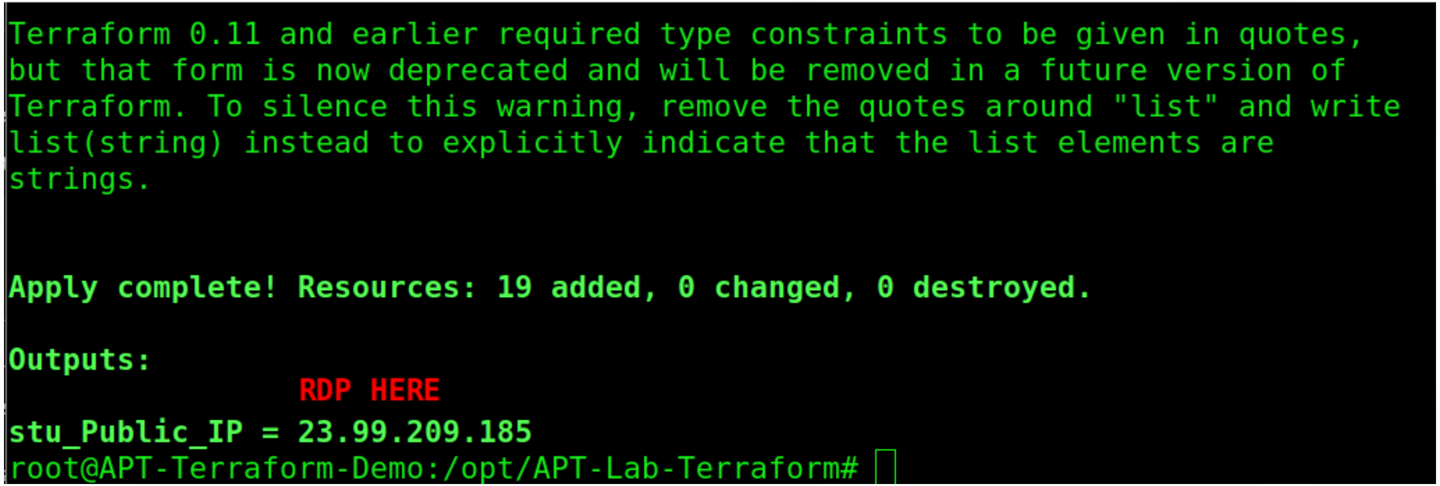
Create a forest, a linux box, provision the domain, etc.



```
Still creating... [2m20s elapsed]
module.stu-client.null_resource.wait-for-domain-to-provision: Still creating...
[2m10s elapsed]
module.stu-DC.azurerm_virtual_machine_extension.create-active-directory-forest:
Still creating... [2m10s elapsed]
module.stu-linux.module.run_command.azurerm_virtual_machine_extension.linux[0]:
Still creating... [2m30s elapsed]
module.stu-client.null_resource.wait-for-domain-to-provision: Still creating...
[2m20s elapsed]
module.stu-DC.azurerm_virtual_machine_extension.create-active-directory-forest:
Still creating... [2m20s elapsed]
module.stu-linux.module.run_command.azurerm_virtual_machine_extension.linux[0]:
Still creating... [2m40s elapsed]
module.stu-client.null_resource.wait-for-domain-to-provision: Still creating...
[2m30s elapsed]
module.stu-DC.azurerm_virtual_machine_extension.create-active-directory-forest:
Still creating... [2m30s elapsed]
module.stu-linux.module.run_command.azurerm_virtual_machine_extension.linux[0]:
Still creating... [2m50s elapsed]
module.stu-client.null_resource.wait-for-domain-to-provision: Still creating...
[2m40s elapsed]
module.stu-DC.azurerm_virtual_machine_extension.create-active-directory-forest:
Still creating... [2m40s elapsed]
```

Demo in gif! Step 3: Done, RDP to Azure IP

Wait for the builds. Once done, the script output is your RDP destination IP.



```
Terraform 0.11 and earlier required type constraints to be given in quotes,
but that form is now deprecated and will be removed in a future version of
Terraform. To silence this warning, remove the quotes around "list" and write
list(string) instead to explicitly indicate that the list elements are
strings.


Apply complete! Resources: 19 added, 0 changed, 0 destroyed.

Outputs:
                RDP HERE
stu_Public_IP = 23.99.209.185
root@APT-Terraform-Demo:/opt/APT-Lab-Terraform# 
```

Demo in gif! Next up: Lab Optics Configuration

Landing zone: WS01.labs.local (domain member server)

RDP to DC01 and download this thing: https://github.com/DefensiveOrigins/APT-Lab-FastOpticsSetup/blob/master/DC-Configurator.ps1

Execute it!

First step downloads, unpacks:

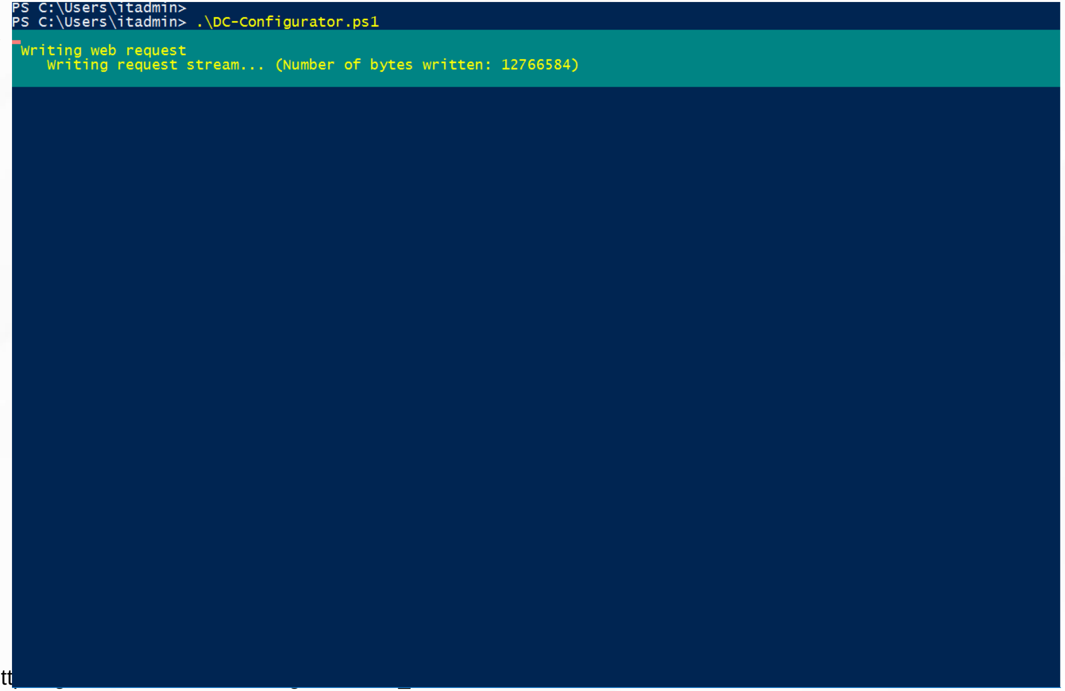
Sysmon + Sysmon Modular

Palantir's WEC/WEF Repo

Winlogbeat

Configs

Group Policies



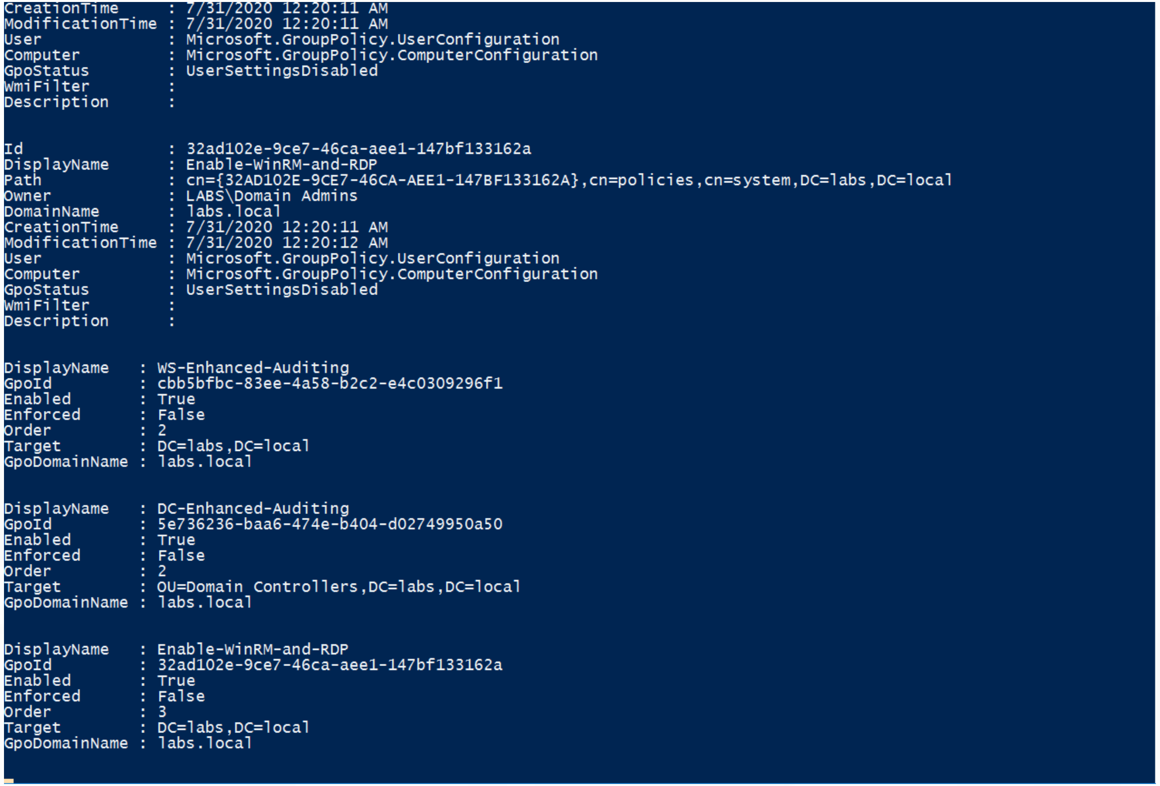
```
PS C:\Users\itadmin>
PS C:\Users\itadmin> .\DC-Configurator.ps1

 Writing web request
    Writing request stream... (Number of bytes written: 12766584)
```

Demo in gif! Next step: Configuration

Once things are unpacked, the script installs and configures

- Sysmon
- WinLogBeat
- Group Policies
- WEC / WEF
- Custom Event Channels



```
CreationTime     : 7/31/2020 12:20:11 AM
ModificationTime : 7/31/2020 12:20:11 AM
User             : Microsoft.GroupPolicy.UserConfiguration
Computer         : Microsoft.GroupPolicy.ComputerConfiguration
GpoStatus        : UserSettingsDisabled
WmiFilter        :
Description      :


Id               : 32ad102e-9ce7-46ca-aee1-147bf133162a
DisplayName      : Enable-WinRM-and-RDP
Path             : cn={32AD102E-9CE7-46CA-AEE1-147BF133162A},cn=policies,cn=system,DC=labs,DC=local
Owner            : LABS\Domain Admins
DomainName       : labs.local
CreationTime     : 7/31/2020 12:20:11 AM
ModificationTime : 7/31/2020 12:20:12 AM
User             : Microsoft.GroupPolicy.UserConfiguration
Computer         : Microsoft.GroupPolicy.ComputerConfiguration
GpoStatus        : UserSettingsDisabled
WmiFilter        :
Description      :


DisplayName   : WS-Enhanced-Auditing
GpoId         : cbb5bfbc-83ee-4a58-b2c2-e4c0309296f1
Enabled       : True
Enforced      : False
Order         : 2
Target        : DC=labs,DC=local
GpoDomainName : labs.local


DisplayName   : DC-Enhanced-Auditing
GpoId         : 5e736236-baa6-474e-b404-d02749950a50
Enabled       : True
Enforced      : False
Order         : 2
Target        : OU=Domain Controllers,DC=labs,DC=local
GpoDomainName : labs.local


DisplayName   : Enable-WinRM-and-RDP
GpoId         : 32ad102e-9ce7-46ca-aee1-147bf133162a
Enabled       : True
Enforced      : False
Order         : 3
Target        : DC=labs,DC=local
GpoDomainName : labs.local
```

Demo in gif! Next Step: Configure the Workstation

- Install Sysmon
- Check for logs
- Run gpupdate
- Reboot

```
PS C:\Users\itadmin> _
```

defensiveorigins.com

Demo in gif! Final Step: Confirm Logging

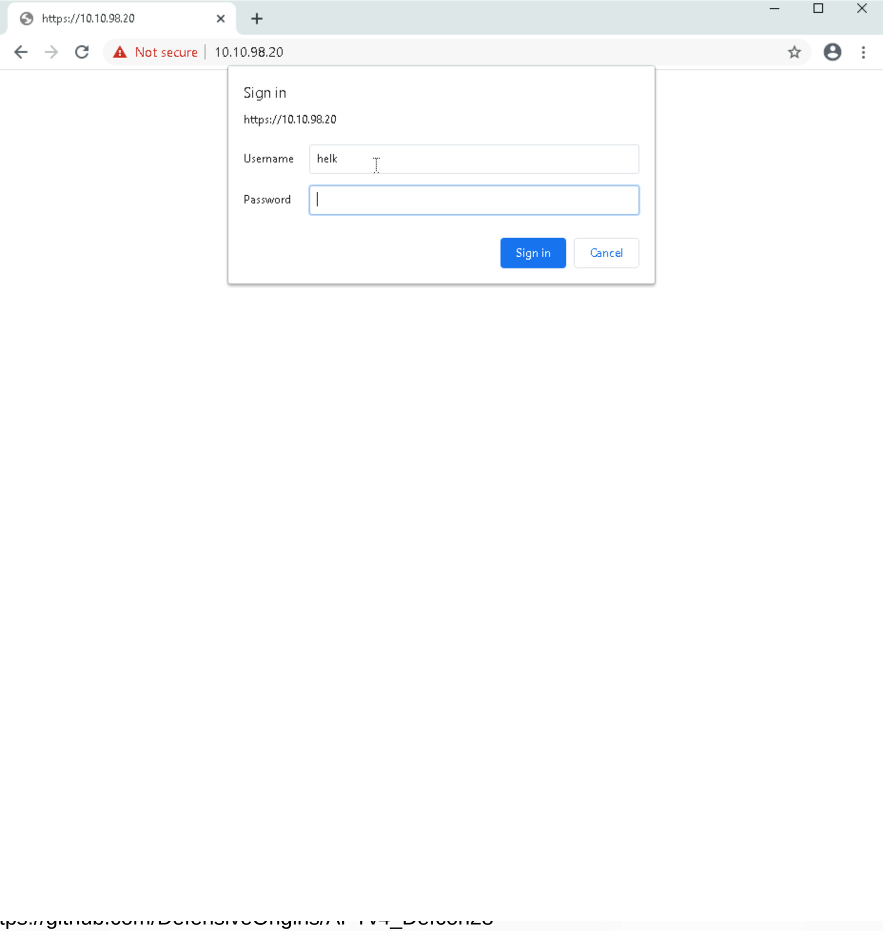
Auth to HELK

Click Discover

Search WS01

Refresh

OPTICS!



Sign in

https://10.10.98.20

Username: helk

Password:

defensiveorigins.com