Do You Want to Build an

AD Lab?

@rustla

Hi

I'm Russ / @rustla

I'm a Penetration Tester at Trustwave in Perth

You might know me from:

- WACTF challenge dev
- BSides
- SecTalks

Summary

Building an AD Lab

- Why build an AD lab?
- Location (infra)
- Methods

Populating AD Labs

- How?
- Why?

Why?

Great for:

- Learning AD
- Tinkering or yeeting the latest exploits / trying tooling safely
- Generating IOCs

Locations

High-level options:

- ~~On-premise?~~
- ~~On-premises?~~
- On-prem (your computer/server)
- Cloud (someone else’s computer/server)

Methods

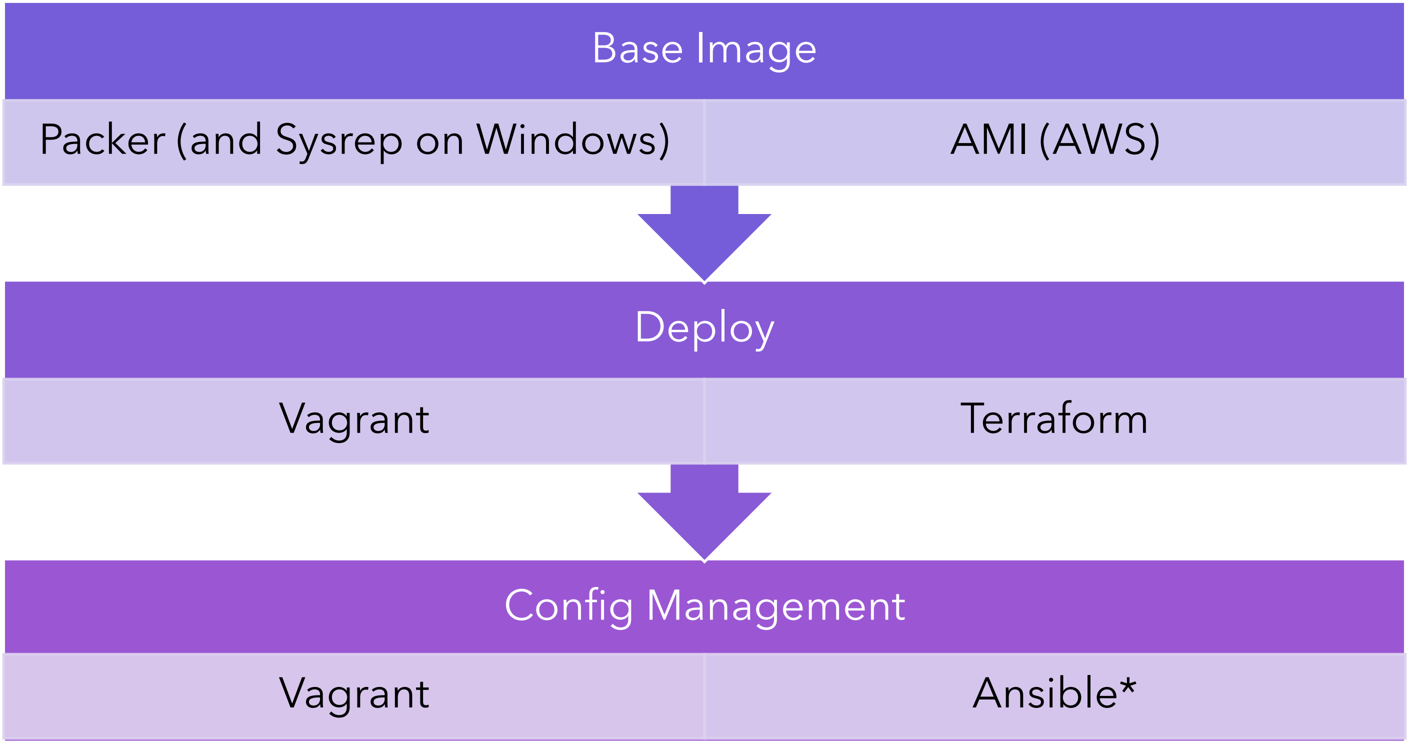
Infra as Code

+ Can see the workflow (mostly)
+ Sometimes still uses OS disk images
+ Repeatable / Works on my machine™

Snapshots

+ Cloning / point in time
+ Can't read the setup workflow
+ Can be faster from play to accessible

Infra as Code Workflow



Base Image

Packer (and Sysrep on Windows)

AMI (AWS)

Deploy

Vagrant

Terraform

Config Management

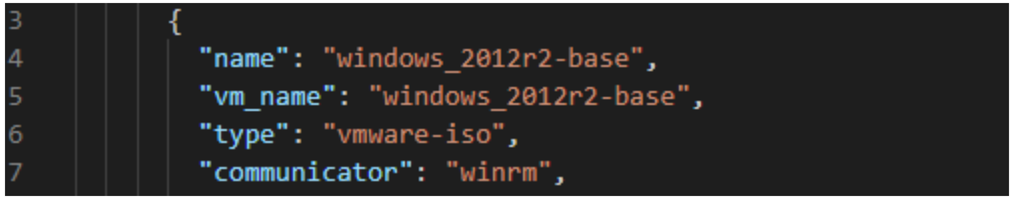
Vagrant

Ansible*

* Puppet, Chef, and SaltStack also offer Config Management. Haven't used them, YMMV

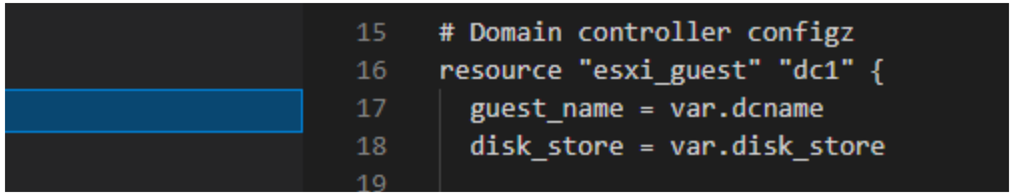
Infra as Code Examples

Packer



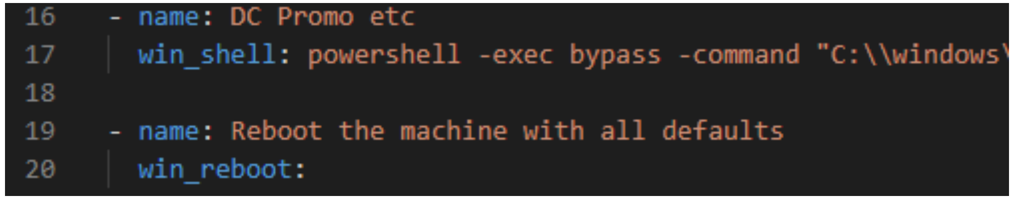
```
{
  "name": "windows_2012r2-base",
  "vm_name": "windows_2012r2-base",
  "type": "vmware-iso",
  "communicator": "winrm",
```

Terraform



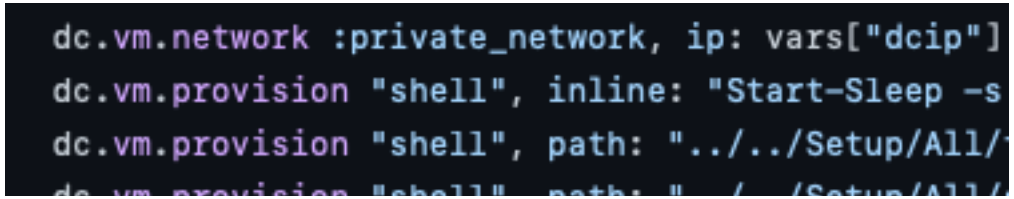
```
# Domain controller configz
resource "esxi_guest" "dc1" {
  guest_name = var.dcname
  disk_store = var.disk_store
```

Ansible



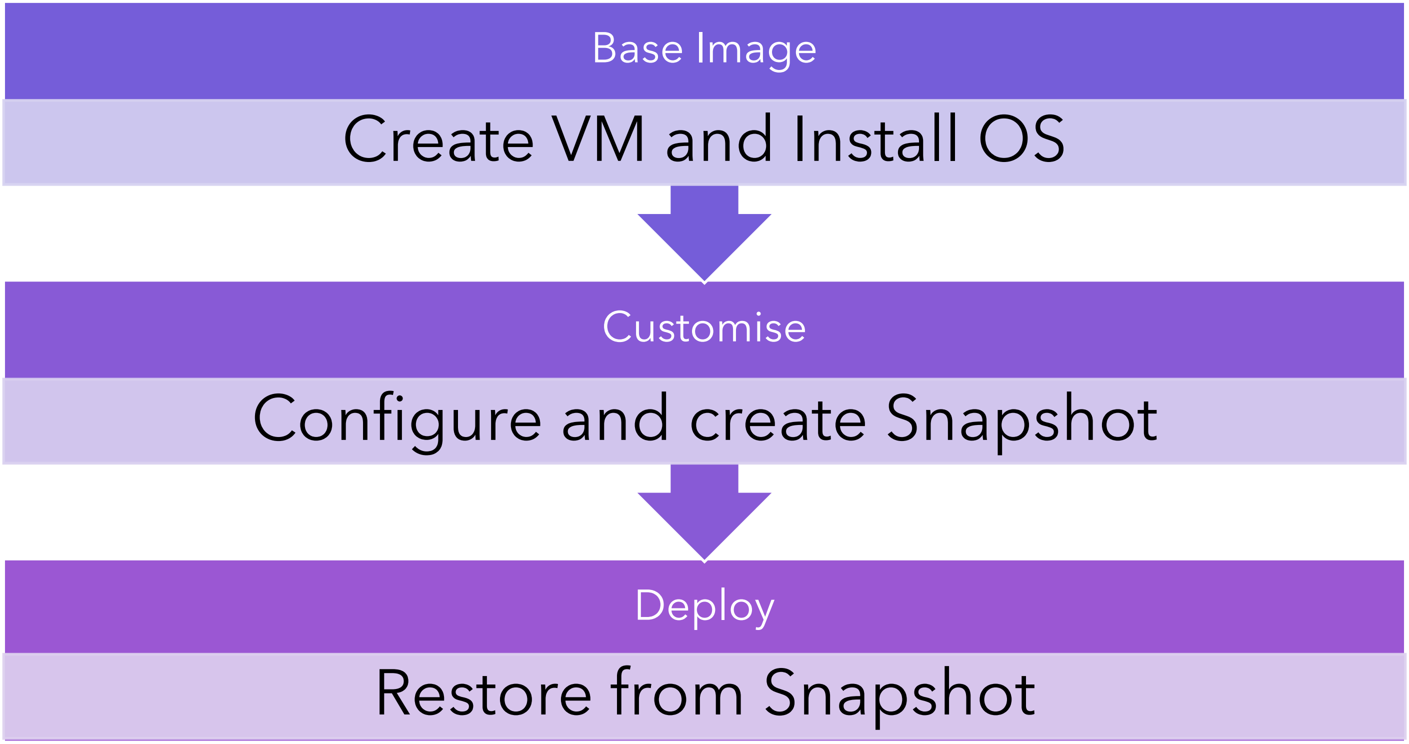
```
- name: DC Promo etc
  win_shell: powershell -exec bypass -command "C:\\windows

- name: Reboot the machine with all defaults
  win_reboot:
```

Vagrant



```
dc.vm.network :private_network, ip: vars["dcip"]
dc.vm.provision "shell", inline: "Start-Sleep -s
dc.vm.provision "shell", path: "../../Setup/All/
dc.vm.provision "shell", path: "../../Setup/All/
```

Snapshot Lab Workflow



Base Image

Create VM and Install OS

Customise

Configure and create Snapshot

Deploy

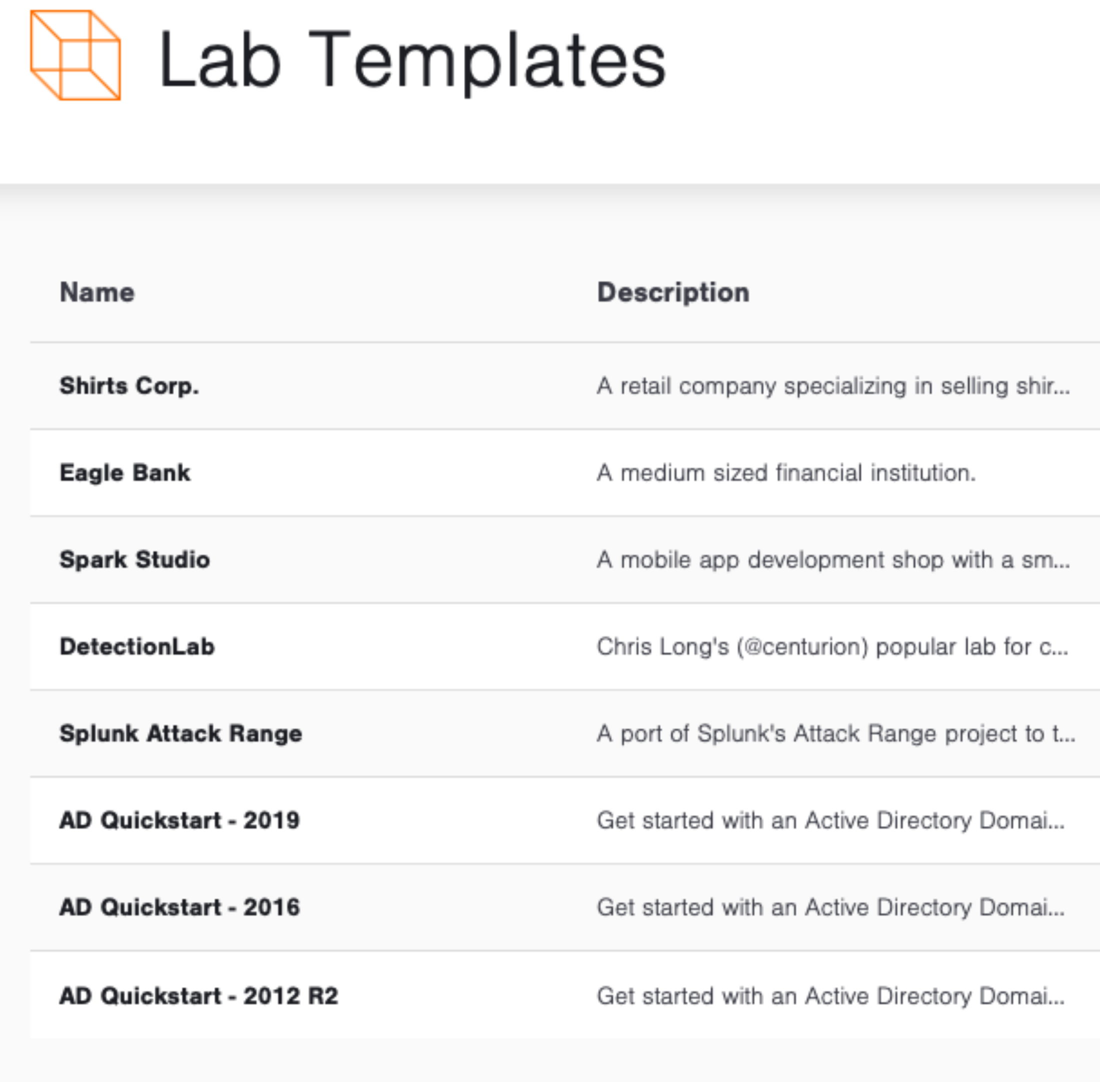
Restore from Snapshot

SnapLabs

Cloud-based Snapshots (AWS AMI)

Needs EC2 permissions

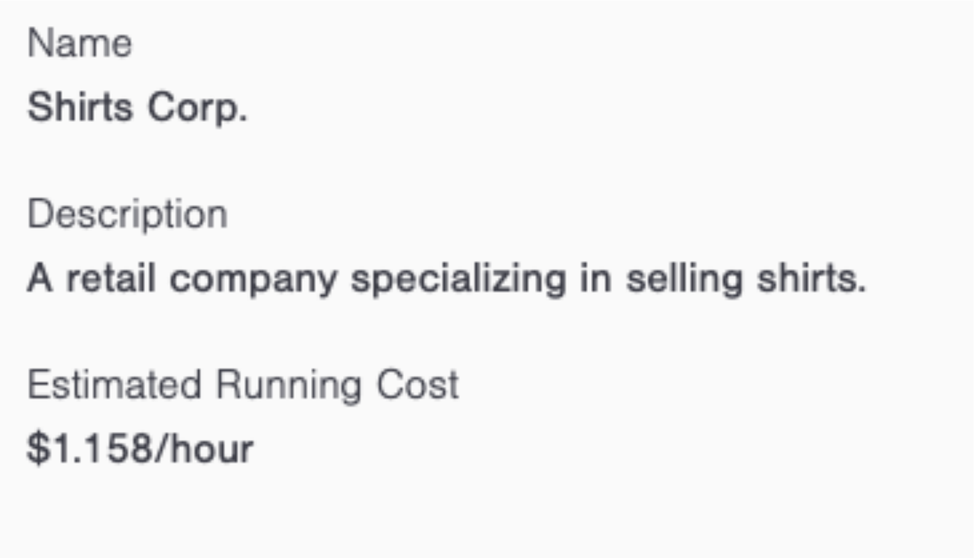
Community Tier - Pay for your AWS usage



Lab Templates

Name	Description
Shirts Corp.	A retail company specializing in selling shir...
Eagle Bank	A medium sized financial institution.
Spark Studio	A mobile app development shop with a sm...
DetectionLab	Chris Long's (@centurion) popular lab for c...
Splunk Attack Range	A port of Splunk's Attack Range project to t...
AD Quickstart - 2019	Get started with an Active Directory Domai...
AD Quickstart - 2016	Get started with an Active Directory Domai...
AD Quickstart - 2012 R2	Get started with an Active Directory Domai...

SnapLabs Example Lab



Name

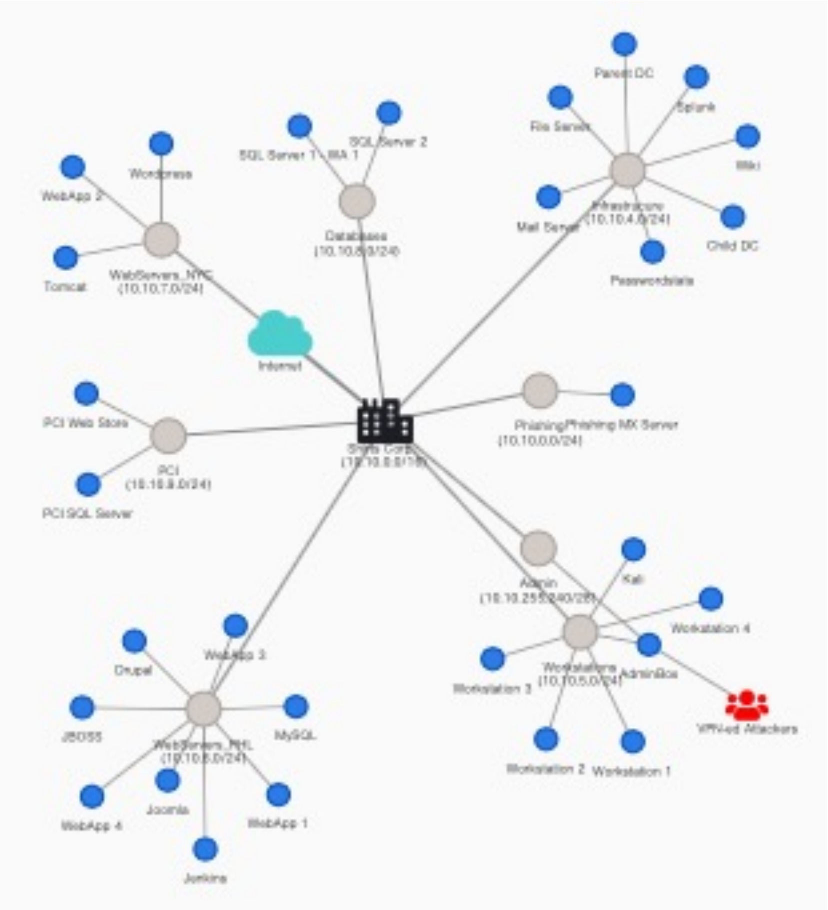
Shirts Corp.

Description

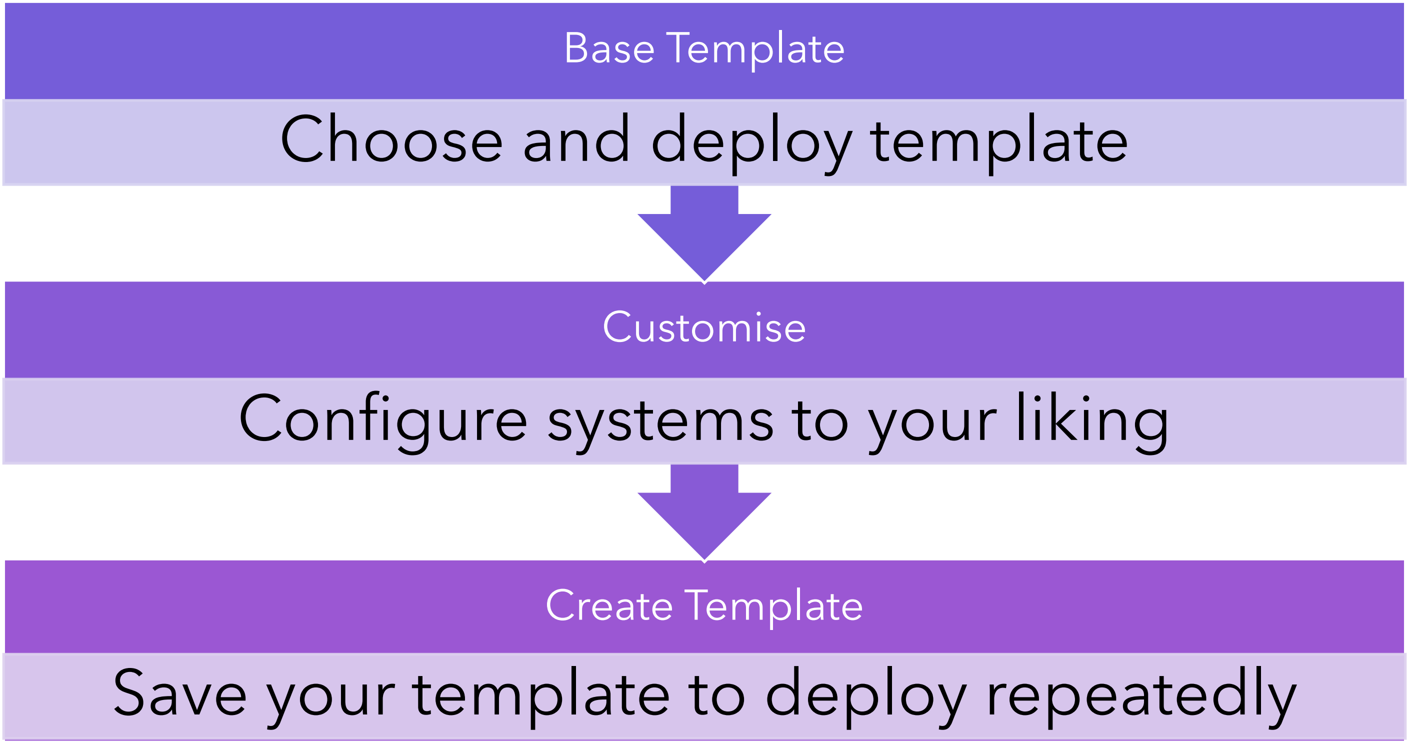
A retail company specializing in selling shirts.

Estimated Running Cost

$1.158/hour



SnapLabs Workflow



Base Template

Choose and deploy template

Customise

Configure systems to your liking

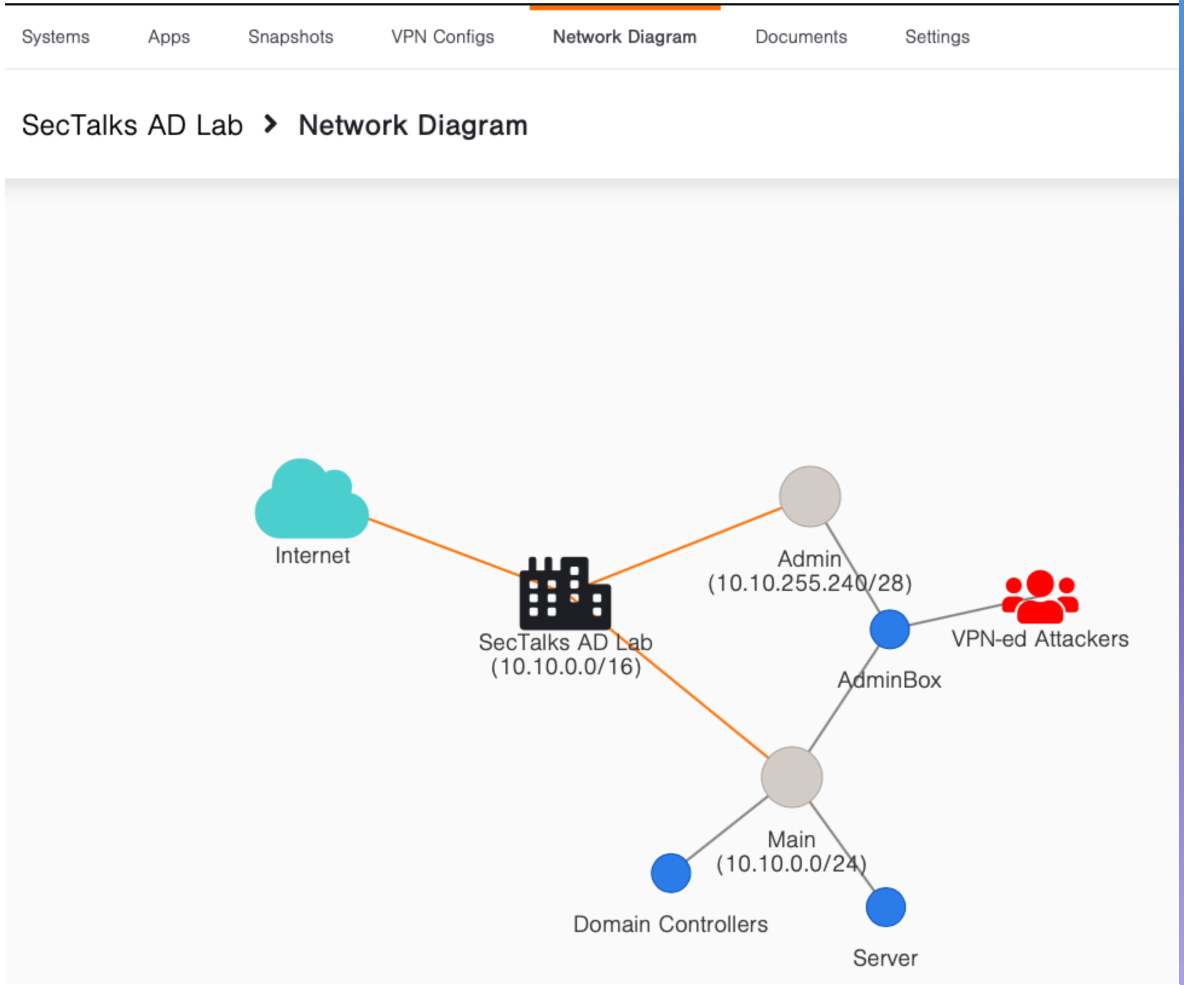
Create Template

Save your template to deploy repeatedly

Simple AD LAB

Quickstart AD Lab Template

Minutes of touch time



SecTalks AD Lab › Network Diagram

Why Populate?

AD with a single user (DA) might not help you learn

Introduce attack surface (to then analyse or exploit)

Automating – introducing unknown attack paths

How to Populate

BadBlood:

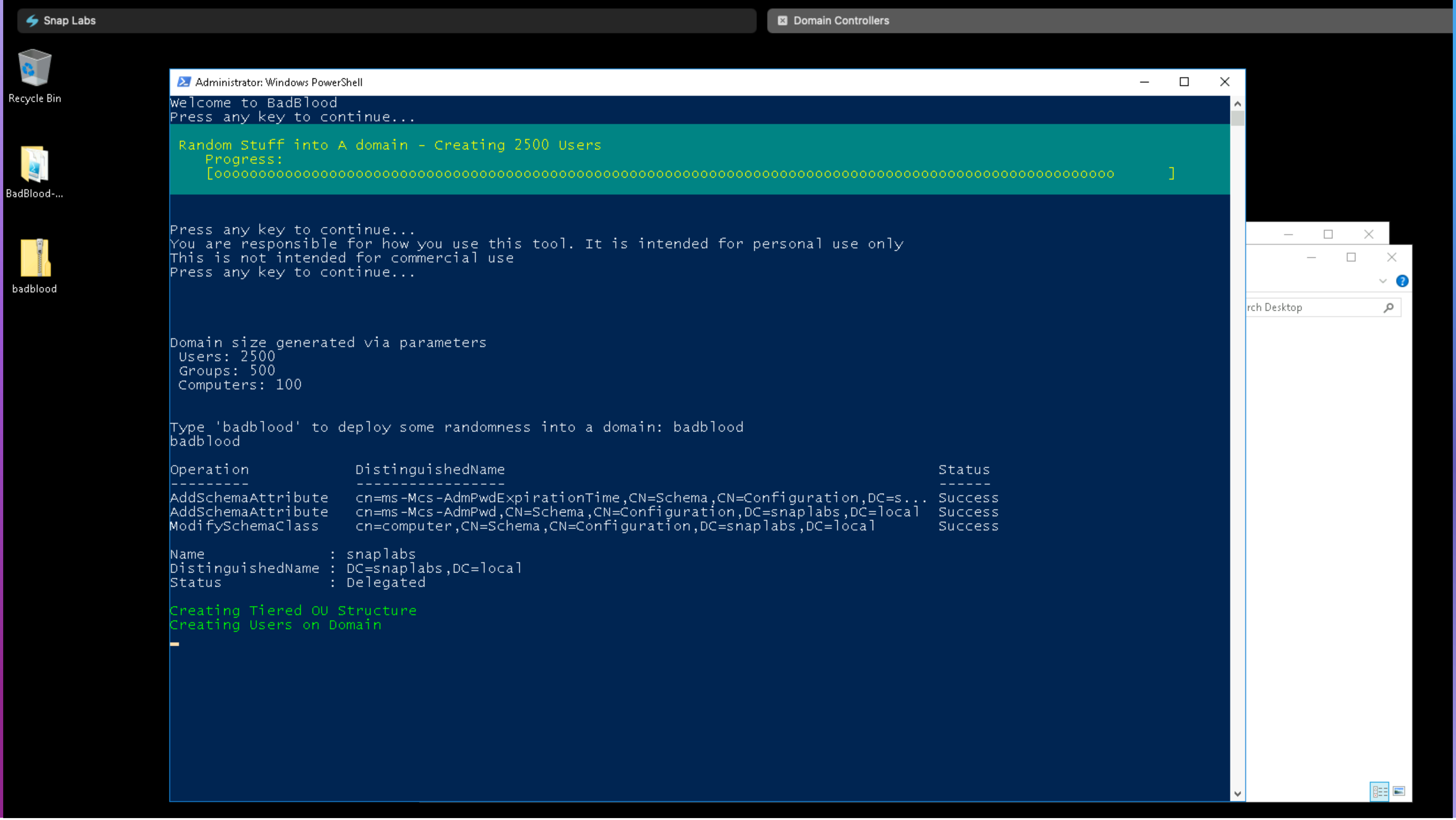
- PowerShell script
- Populates AD with attack paths
- Supposedly random each time
- github.com/davidprowe/BadBlood

BadBlood Attack Vectors

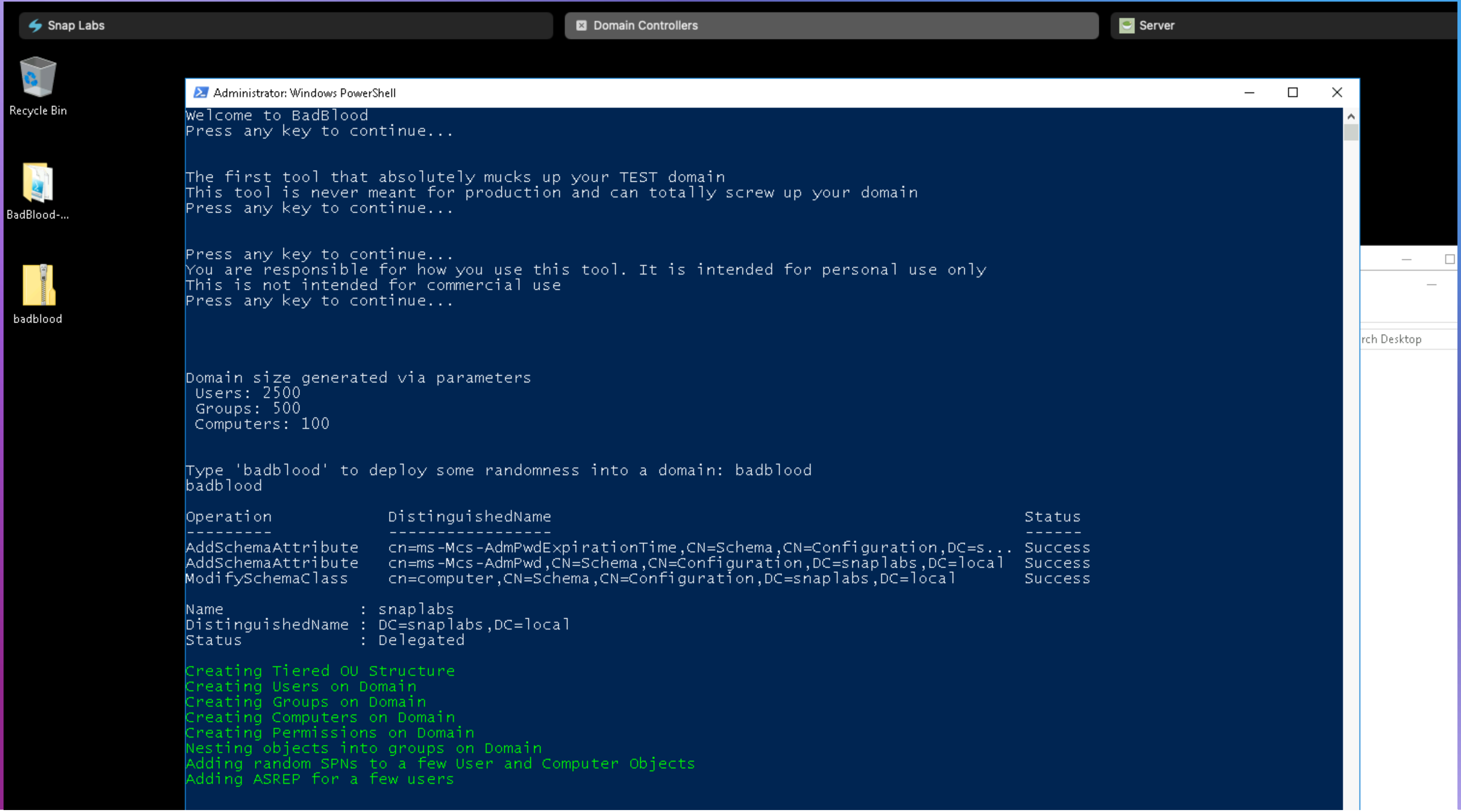
Abusable AD Permissions

Weak Passwords

Kerberoasting and AS-REP Roasting

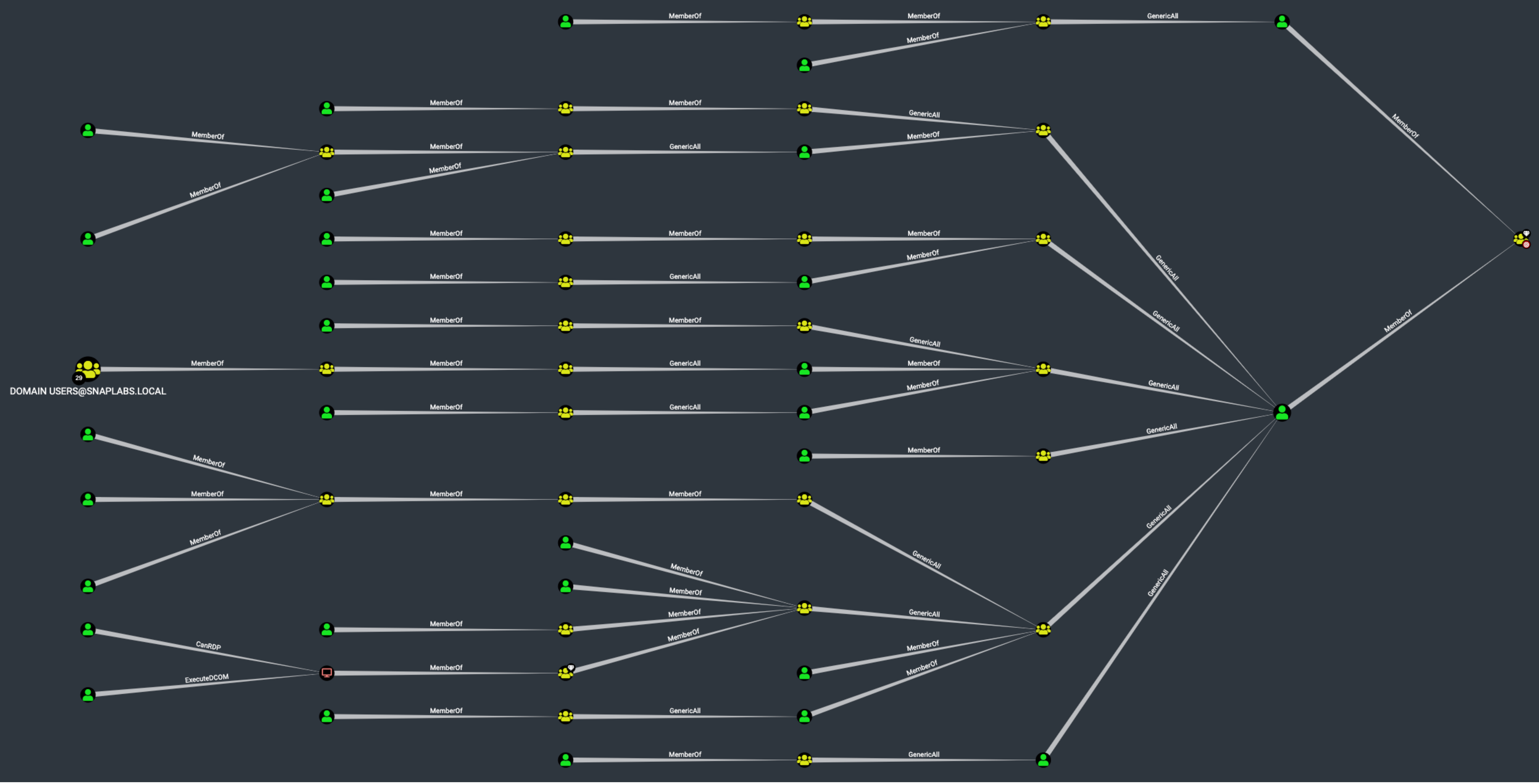


```
Welcome to BadBlood
Press any key to continue...

 Random Stuff into A domain - Creating 2500 Users
    Progress:
    [ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo      ]


Press any key to continue...
You are responsible for how you use this tool. It is intended for personal use only
This is not intended for commercial use
Press any key to continue...




Domain size generated via parameters
 Users: 2500
 Groups: 500
 Computers: 100


Type 'badblood' to deploy some randomness into a domain: badblood
badblood

Operation            DistinguishedName                                                  Status
---------            -----------------                                                  ------
AddSchemaAttribute   cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=s...  Success
AddSchemaAttribute   cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=snaplabs,DC=local   Success
ModifySchemaClass    cn=computer,CN=Schema,CN=Configuration,DC=snaplabs,DC=local        Success

Name              : snaplabs
DistinguishedName : DC=snaplabs,DC=local
Status            : Delegated

Creating Tiered OU Structure
Creating Users on Domain
_
```



```
Welcome to BadBlood
Press any key to continue...


The first tool that absolutely mucks up your TEST domain
This tool is never meant for production and can totally screw up your domain
Press any key to continue...


Press any key to continue...
You are responsible for how you use this tool. It is intended for personal use only
This is not intended for commercial use
Press any key to continue...




Domain size generated via parameters
 Users: 2500
 Groups: 500
 Computers: 100


Type 'badblood' to deploy some randomness into a domain: badblood
badblood

Operation            DistinguishedName                                                  Status
---------            -----------------                                                  ------
AddSchemaAttribute   cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=s... Success
AddSchemaAttribute   cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=snaplabs,DC=local  Success
ModifySchemaClass    cn=computer,CN=Schema,CN=Configuration,DC=snaplabs,DC=local        Success

Name              : snaplabs
DistinguishedName : DC=snaplabs,DC=local
Status            : Delegated

Creating Tiered OU Structure
Creating Users on Domain
Creating Groups on Domain
Creating Computers on Domain
Creating Permissions on Domain
Nesting objects into groups on Domain
Adding random SPNs to a few User and Computer Objects
Adding ASREP for a few users
```

@rustla

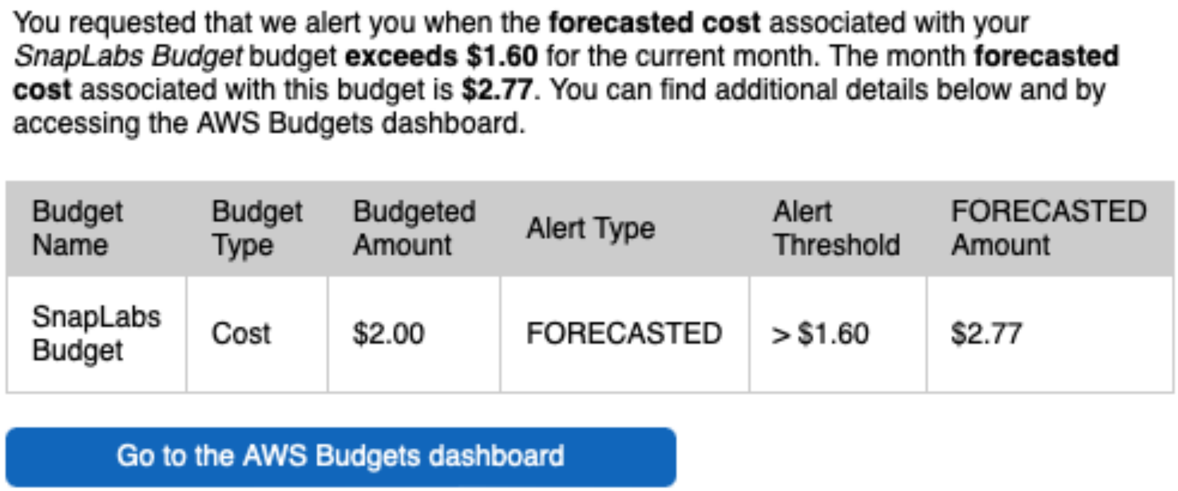

DOMAIN USERS@SNAPLABS.LOCAL
29
MemberOf
GenericAll
CanRDP
ExecuteDCOM

SnapLabs Tips

Have a dedicated AWS Account

Save those dollars:

- Configure budget alerts
- Configure Auto-Stop
- Delete when done



You requested that we alert you when the **forecasted cost** associated with your *SnapLabs Budget* budget **exceeds $1.60** for the current month. The month **forecasted cost** associated with this budget is **$2.77**. You can find additional details below and by accessing the AWS Budgets dashboard.

Budget Name	Budget Type	Budgeted Amount	Alert Type	Alert Threshold	FORECASTED Amount
SnapLabs Budget	Cost	$2.00	FORECASTED	> $1.60	$2.77

Questions?

Reach out: @rustla

References:

- snaplabs.io
- github.com/davidprowe/BadBlood