Lab Environments for Red Teamers with Dynamic Labs

Black Hat Europe 2022

David Turco | Accenture Security @endle__

Who Am I?

David Turco

Security Delivery Senior Manager

Accenture Security

@endle__

Simulated Attack Capability Development

Simulated Attack Engagements

Copyright © 2022 Accenture. All rights reserved.

Agenda

Quickly deploy transient lab environments for simulated attacks, self-studying, training and research.

01 Introduction

02 Dynamic Labs 101
- Design and architecture
- Usage

03 Development
- Templates
- Release

04 Conclusion

Copyright © 2022 Accenture. All rights reserved.

01

Introduction

Copyright © 2022 Accenture. All rights reserved.

Scenarios

Traditional solutions can be clumsy and inefficient

01 **Simulated Attack engagements**

Testing toolchains against ‘digital twin’ environments

02 **Self-studying**

Practicing an existing or new technique

03 **Research**

- Researching a new technique
- Sharing research

04 **Formal training**

- Delivering internal training
- Delivering scalable external training

Copyright © 2022 Accenture. All rights reserved.

Dynamic Labs

An **open source** tool aimed at red teamers and penetration testers for the rapid **deployment of transient lab environments to the cloud.**

https://github.com/ctxis/DynamicLabs

Copyright © 2022 Accenture. All rights reserved.

Dynamic Labs

Uses **simple configuration files (lab templates)** to abstract the complexities of building **realistic corporate environments**, vulnerabilities included.

https://github.com/ctxis/DynamicLabs

Copyright © 2022 Accenture. All rights reserved.

Scenarios

Modern approach with Dynamic Labs

01 Simulated Attack engagements

- Define environment by tailoring an existing lab template
- Deploy environment
- Manual final touches
- Destroy environment

Copyright © 2022 Accenture. All rights reserved.

Scenarios

Modern approach with Dynamic Labs

02 Self-studying

- Choose existing community lab template
- Deploy environment
- Practice technique
- Destroy environment

Copyright © 2022 Accenture. All rights reserved.

Scenarios

Modern approach with Dynamic Labs

03 Research

- Define environment by tailoring an existing lab template
- Deploy environment
- Manual updates to the environment
- Destroy environment
- **Implement lab template** to **share research**

Copyright © 2022 Accenture. All rights reserved.

Scenarios

Modern approach with Dynamic Labs

04 Formal Training

- Define complex lab environments during development of training
- Deploy **multiple clones** of the environment
- Deliver training
- Destroy environments
- **Distribute lab template** to attendees

Copyright © 2022 Accenture. All rights reserved.

02

Dynamic Labs 101

Copyright © 2022 Accenture. All rights reserved.

Design and Architecture Roles

Management

- Lab owner
- Deployment of lab environment
- Full administrative access
- Automation

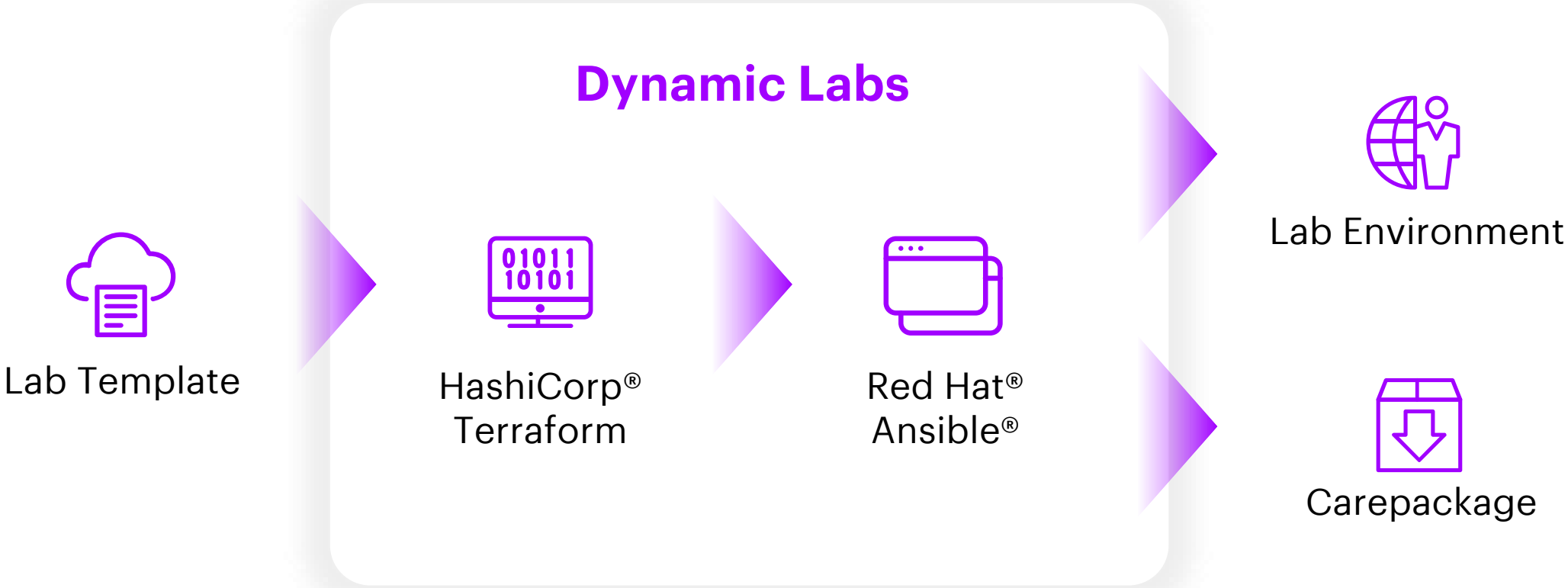
Candidate

- End user of the deployed lab environment
- Entry point

Copyright © 2022 Accenture. All rights reserved.

Design and Architecture

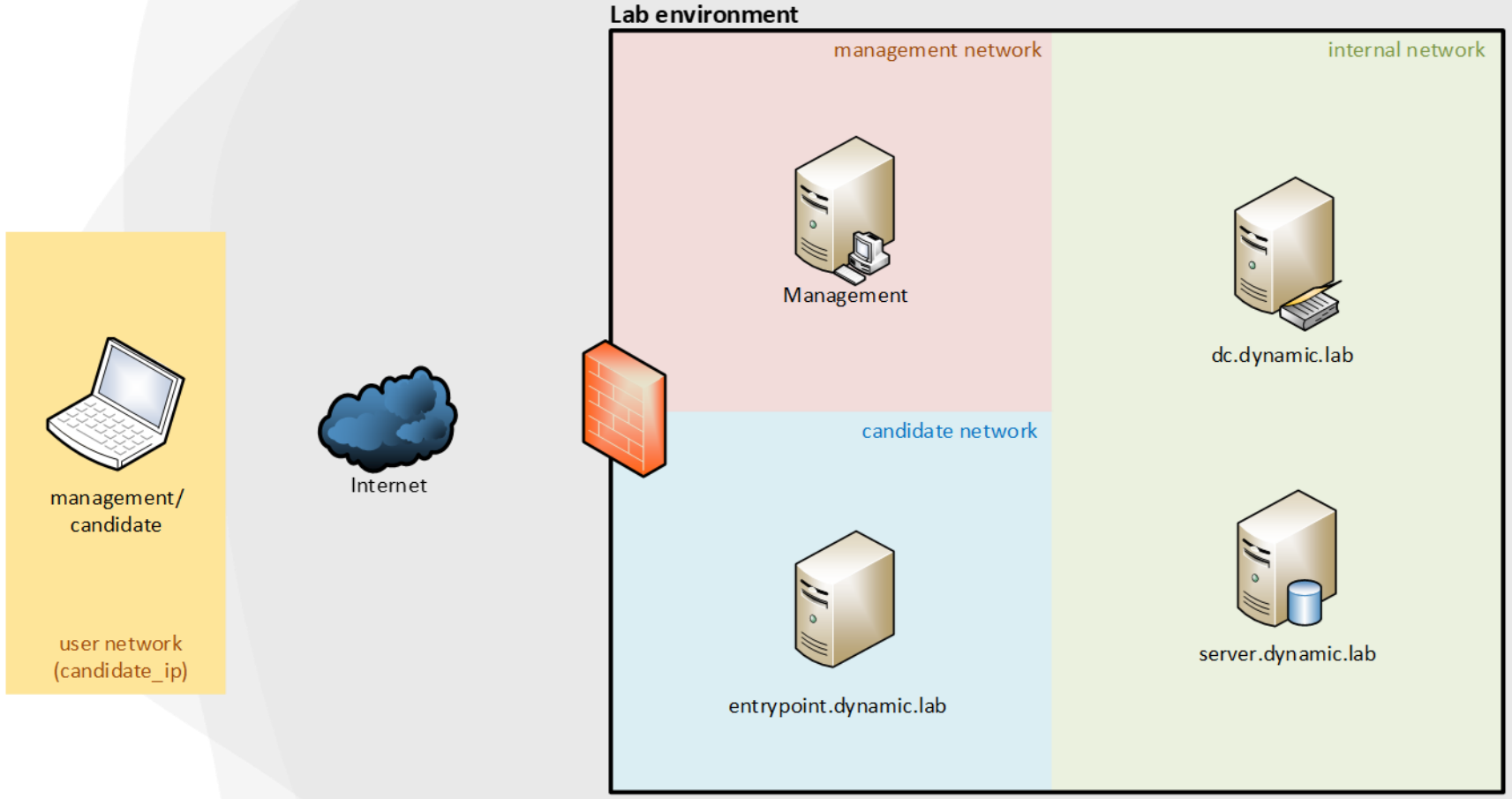
Deployment overview



Copyright © 2022 Accenture. All rights reserved.

Design and Architecture

Typical simple lab environment



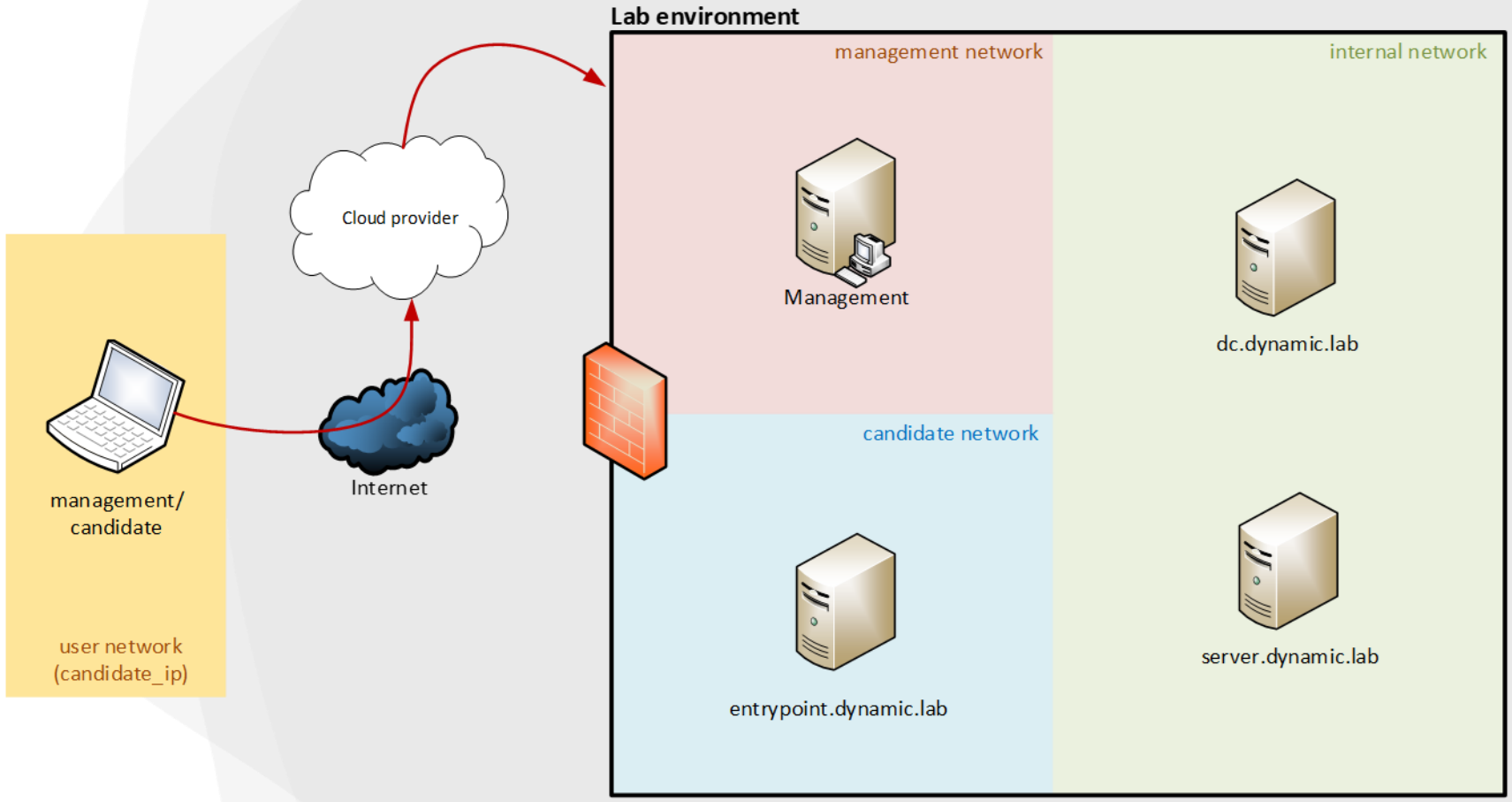
"Copyright © 2022 Accenture. All rights reserved."

Copyright © 2022 Accenture. All rights reserved.

Design and Architecture

Typical simple lab environment

Terraform deploys lab networks and systems in the cloud

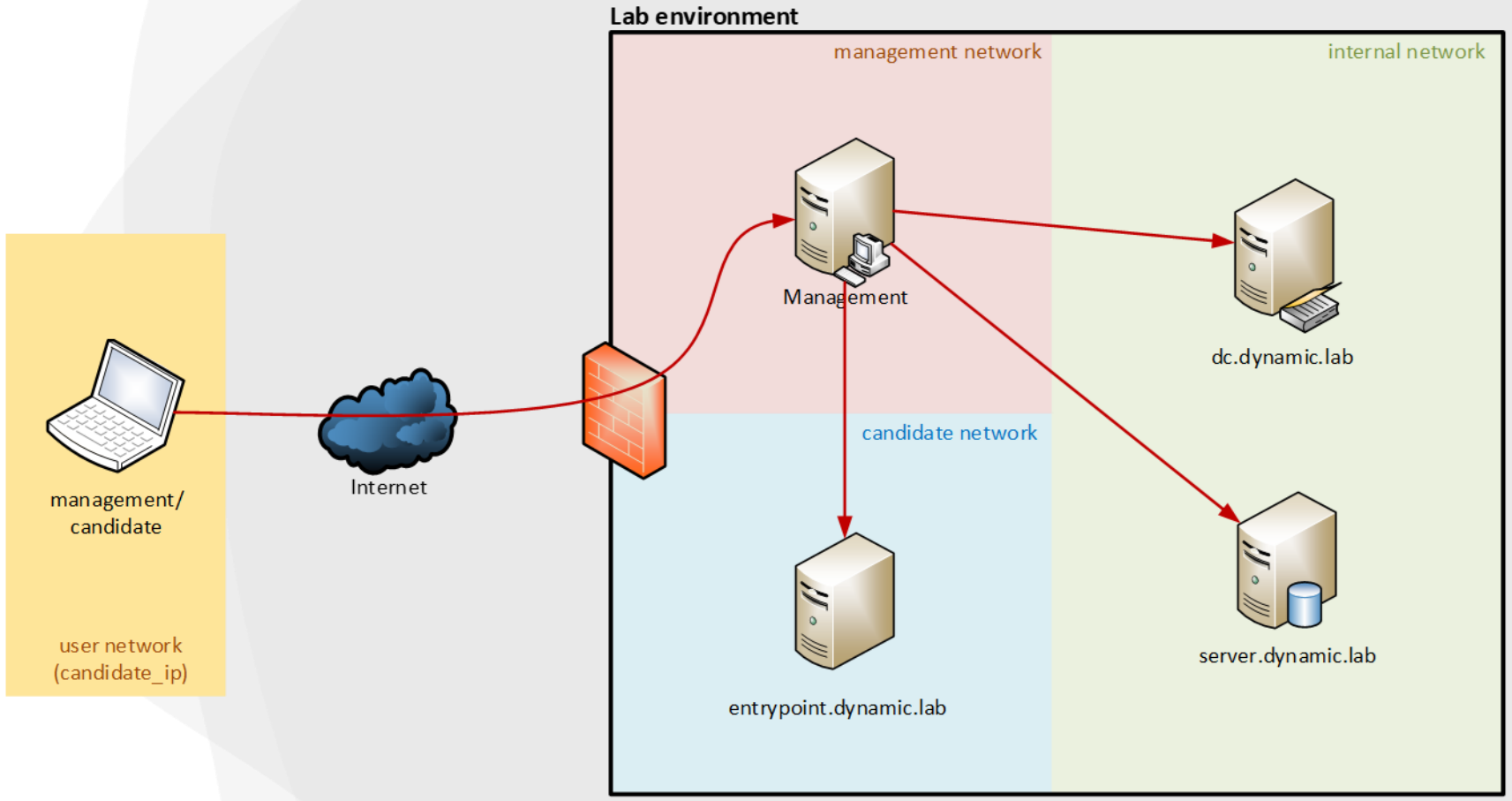


Copyright © 2022 Accenture. All rights reserved.

Design and Architecture

Typical simple lab environment

Ansible configures lab systems



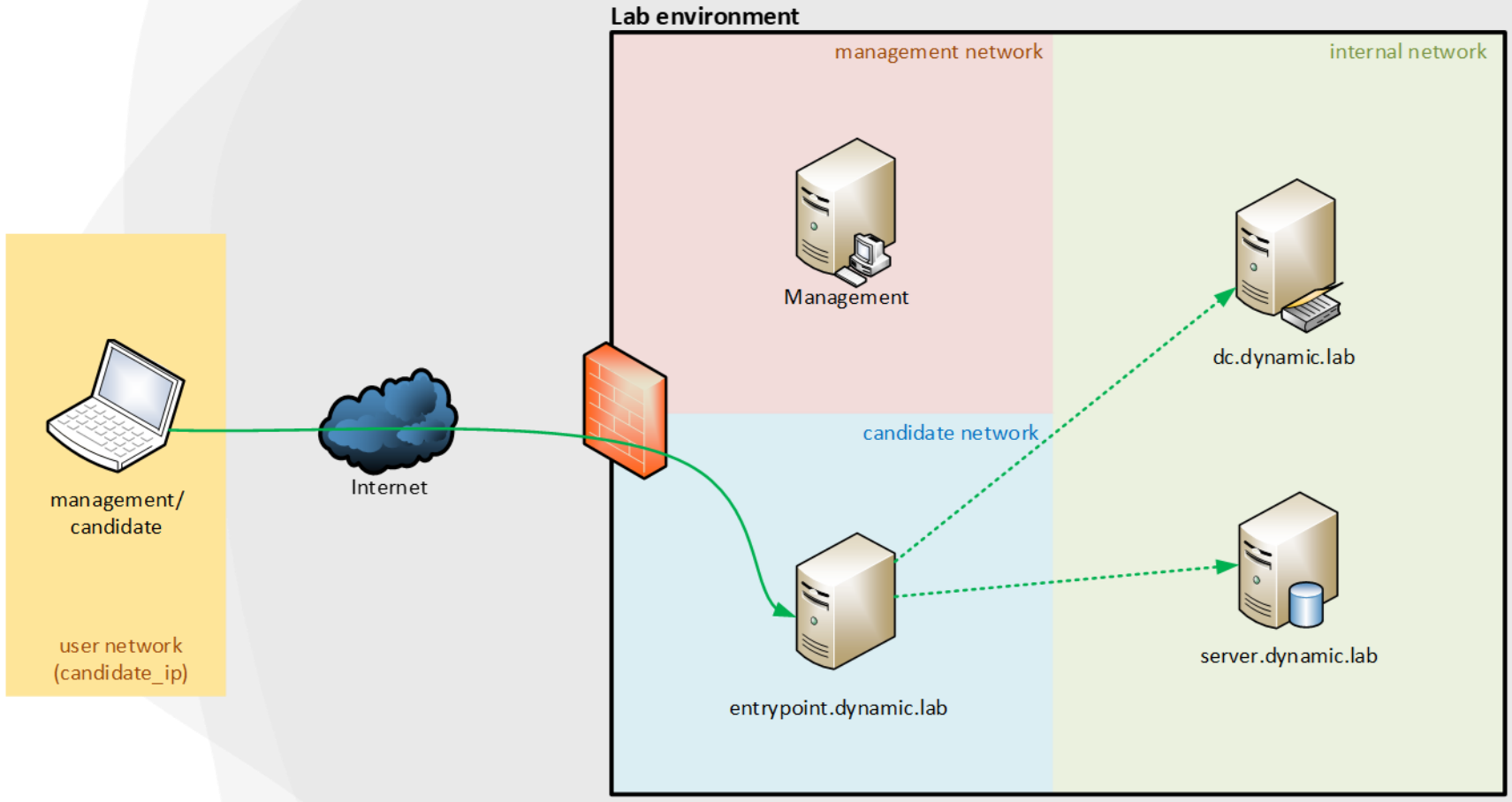
"Copyright © 2022 Accenture. All rights reserved."

Copyright © 2022 Accenture. All rights reserved.

Design and Architecture

Typical simple lab environment

Candidate accesses lab environment



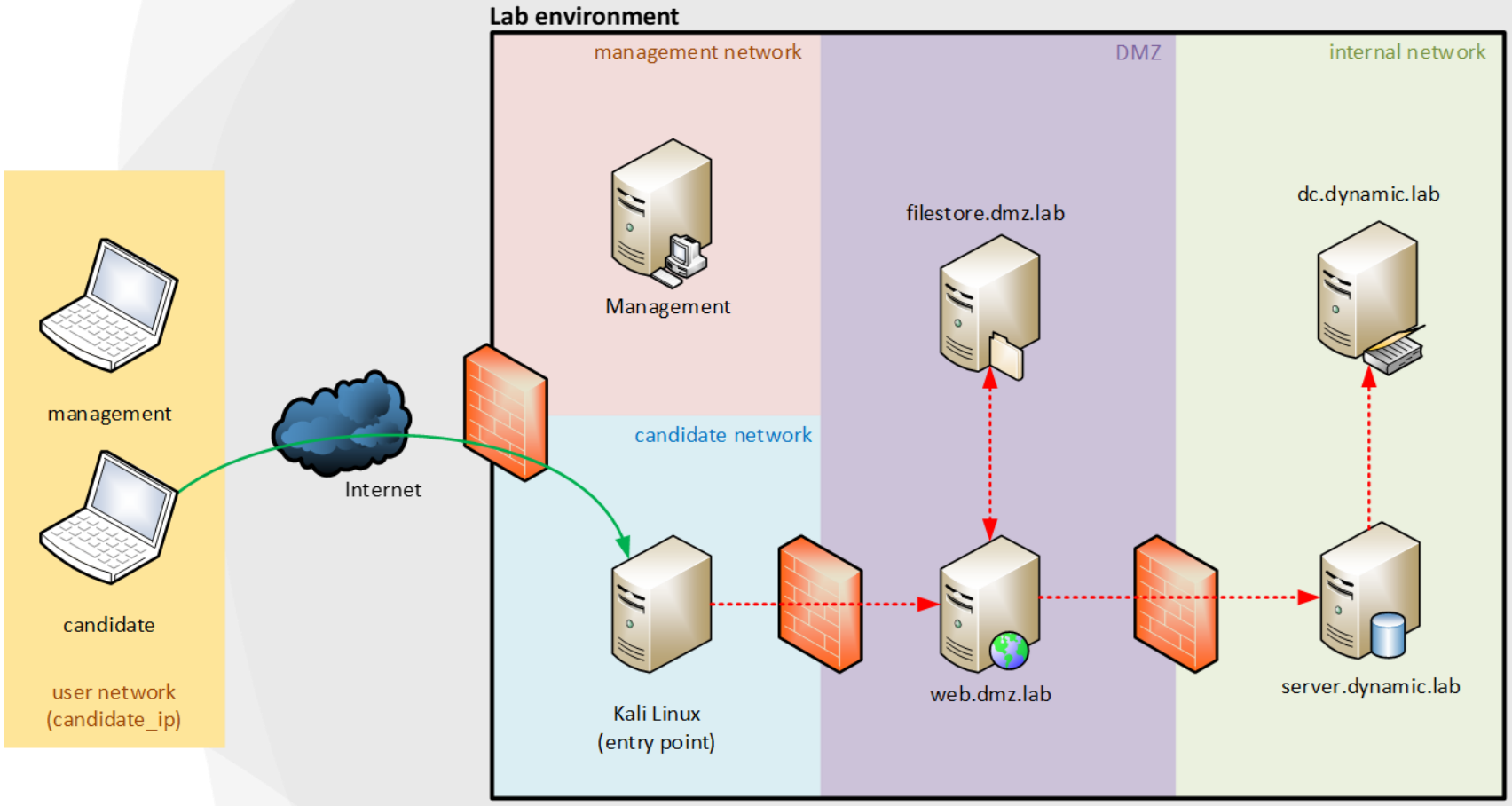
"Copyright © 2022 Accenture. All rights reserved."

Copyright © 2022 Accenture. All rights reserved.

Design and Architecture

Slightly more complex lab environment

Multiple network segments, management and candidate are distinct



"Copyright © 2022 Accenture. All rights reserved."

Copyright © 2022 Accenture. All rights reserved.

Usage

High-Level Deployment Steps

- Install pre-requisites
- Choose a lab template
- Update the configuration variables
- Deploy the lab environment
- Use the lab environment
- Destroy the lab

Copyright © 2022 Accenture. All rights reserved.

Usage Example: simple-AD on AWS

Step 1 - **Install pre-requisites**

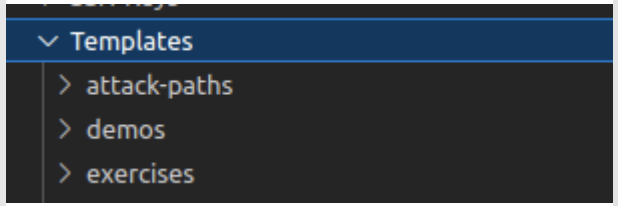
- Download a copy of Dynamic Labs from GitHub
- Install Terraform for your platform
- Install the AWS CLI

Copyright © 2022 Accenture. All rights reserved.

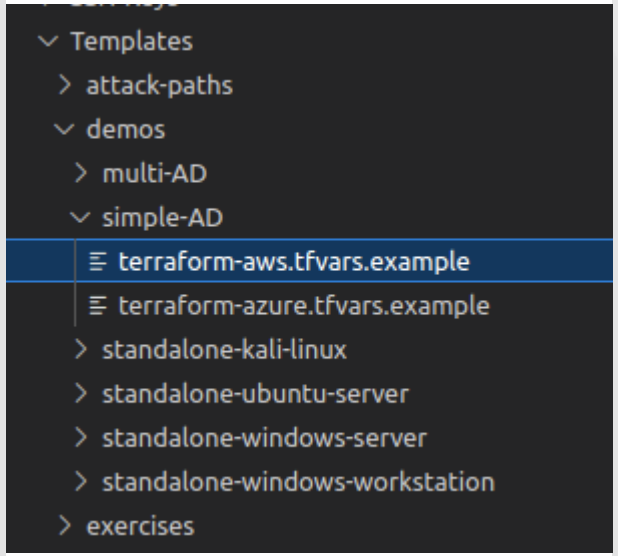
Usage Example: simple-AD on AWS

Step 2 - **Choose a lab template**

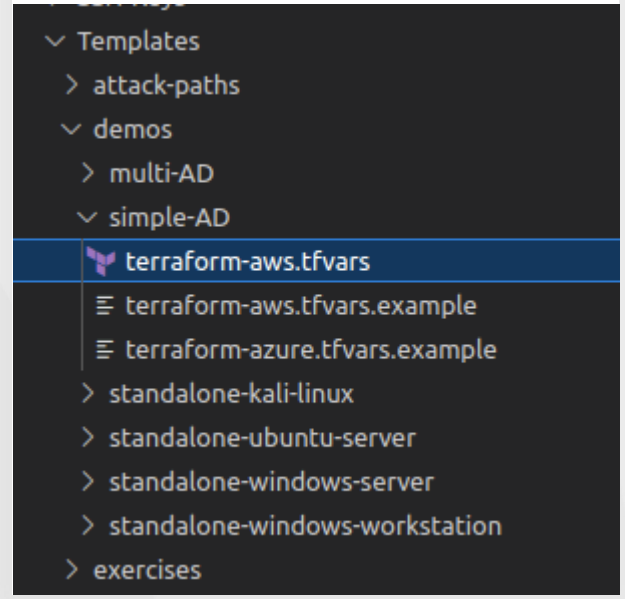
From the Templates directory



Select a suitable template *.tfvars.example file



Create a copy of the example file as *.tfvars



Copyright © 2022 Accenture. All rights reserved.

Usage Example: simple-AD on AWS

Step 3 - **Update the configuration variables**

```
1  ############ / AWS Credentials
2  AWS_ACCESS_KEY          = ""
3  AWS_SECRET_KEY          = ""
4  AWS_REGION              = "eu-west-2"
5
6  ############ / Attacker IP Range
7  # Permitted to SSH and RDP to management network (ID 0) and candidate network (ID 1).
8  candidate_ip = ["XXX.XXX.XXX.XXX/XX"] # Replace with your IP.
9
```

Copyright © 2022 Accenture. All rights reserved.

Usage Example: simple-AD on AWS

Step 4 - **Deploy the lab environment** (1/3)

```
$ cd Terraform/AWS

$ terraform workspace new demo

$ terraform init

$ terraform apply -var-file=../../Templates/demos/simple-
AD/terraform-aws.tfvars
```

Copyright © 2022 Accenture. All rights reserved.

Usage Example: simple-AD on AWS

Step 4 - **Deploy the lab environment** (2/3)

```
demo@dynamiclabs:~/dynamic-labs$ cd Terraform/AWS
demo@dynamiclabs:~/dynamic-labs/Terraform/AWS$ terraform workspace new demo
Created and switched to workspace "demo"!

You're now on a new, empty workspace. Workspaces isolate their state,
so if you run "terraform plan" Terraform will not see any existing state
for this configuration.
demo@dynamiclabs:~/dynamic-labs/Terraform/AWS$ terraform init
Initializing modules...
- ansible_inventory in Core/Ansible

[...]

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
demo@dynamiclabs:~/dynamic-labs/Terraform/AWS$
```

Copyright © 2022 Accenture. All rights reserved.

Usage Example: simple-AD on AWS

Step 4 - **Deploy the lab environment** (3/3)

```
demo@dynamiclabs:~/dynamic-labs/Terraform/AWS$ terraform apply -var-file=../../Templates/demos/simple-AD/terraform-aws.tfvars
module.windows_server.data.aws_ami.windows_server_2019: Reading...
module.management_server.data.aws_ami.ubuntu: Reading...
module.ubuntu_server.data.aws_ami.ubuntu_20_04: Reading...
module.windows_server.data.aws_ami.windows_server_2016: Reading...
module.kali.data.aws_ami.kali: Reading...
module.ubuntu_server.data.aws_ami.ubuntu_22_04: Reading...
module.windows_server.data.aws_ami.windows_server_2022: Reading...
module.windows_server.data.aws_ami.windows_server_2019: Read complete after 0s [id=ami-0685ae995ef3c2224]
module.ubuntu_server.data.aws_ami.ubuntu_22_04: Read complete after 1s [id=ami-0acf1b3e8253d4481]
module.management_server.data.aws_ami.ubuntu: Read complete after 1s [id=ami-0acf1b3e8253d4481]
module.windows_server.data.aws_ami.windows_server_2022: Read complete after 1s [id=ami-04e0ebd20d57a72c1]
module.ubuntu_server.data.aws_ami.ubuntu_20_04: Read complete after 1s [id=ami-05bfd03d0709e3ecb]
module.windows_server.data.aws_ami.windows_server_2016: Read complete after 1s [id=ami-0e91d2bbbb46eb7c5]
module.kali.data.aws_ami.kali: Read complete after 1s [id=ami-0b12b19de4b259d25]

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the follow
  + create
 <= read (data resources)

Terraform will perform the following actions:

  # aws_key_pair.candidate will be created
  + resource "aws_key_pair" "candidate" {
      + arn             = (known after apply)
      + fingerprint     = (known after apply)
      + id              = (known after apply)
```

Copyright © 2022 Accenture. All rights reserved.

Usage Example: simple-AD on AWS

Step 5 - **Use the lab environment** - Terraform Output

```
Apply complete! Resources: 1 added, 0 changed, 1 destroyed.

Outputs:

Candidate_Credentials = {
  "Kali Candidate SSH Key" = "../../SSH-Keys/demo-candidate_key.pem"
  "Kali Candidate Username" = "kali"
}
Carepackage = {
  "INFO" = <<-EOT
  Information about lab-specific account credentials, including the autogenerated ones, is included in the '[Environment Carepackage]',
  which is printed oput to screen slighly above this output message.
  The carepackage is also available on the management server at ~/carepackage.json"

  EOT
}
Lab_Systems = [
  {
    "name" = "demoDC101"
    "private_ip" = "10.1.1.10"
  },
  {
    "name" = "demoGS201"
    "private_ip" = "10.1.2.104"
  },
]
Management_Credentials = {
  "Kali Candidate SSH Key" = "../../SSH-Keys/demo-candidate_key.pem"
  "Kali Candidate Username" = "kali"
  "Management SSH Key" = "../../SSH-Keys/demo-management_key.pem"
  "Management Username" = "ubuntu"
  "Management Windows Password" = "OQ5tQIJr^Y1o@QHr"
  "Management Windows Username" = "ansible"
}
Management_Server = {
  "name" = "demoOverlord"
  "public_ip" = "18.130.16.35"
  "user" = "ubuntu"
}
Public_Lab_Systems = [
  {
    "name" = "demoGS201"
    "private_ip" = "10.1.2.104"
    "public_ip" = "35.176.97.207"
  },
]
```

```
Public_Lab_Systems = [
  {
    "name" = "demoGS201"
    "private_ip" = "10.1.2.104"
    "public_ip" = "35.176.97.207"
  },
```

Copyright © 2022 Accenture. All rights reserved.

Usage Example: simple-AD on AWS

Step 5 - **Use the lab environment** – Environment Carepackage

```
TASK [################## Environment Carepackage ##################] ***************
task path: /home/ubuntu/Ansible/plays/carepackage.yml:21
ok: [localhost] => {
    "carepackage.stdout": [
        {
            "host_or_domain_name": "dynamic.lab",
            "type": "domain",
            "users": [
                {
                    "password": "Sup3rSecretString.2022!",
                    "username": "LowPriv"
                }
            ]
        }
    ]
}
```

Copyright © 2022 Accenture. All rights reserved.

Usage Example: simple-AD on AWS

Step 6 – **Destroy the lab environment**

```
demo@dynamiclabs:~/dynamic-labs/Terraform/AWS$ terraform destroy -var-file=../../Templates/demos/simple-AD/terraform-aws.tfvars
module.candidate.tls_private_key.private_key: Refreshing state... [id=a6a7a1709290f429239ff20398819dc1bb0afe7b]
module.management.tls_private_key.private_key: Refreshing state... [id=72b1759d742b1c23a406e7eabf5633191b87fa9c]
random_password.system_password: Refreshing state... [id=none]
module.candidate.local_sensitive_file.public_key_openssh: Refreshing state... [id=2ba040e2c622d64e3da85cdd6ba255be5b318ed3]
module.management.local_sensitive_file.private_key: Refreshing state... [id=4a2ecbb3fc87ab95174077705bfe64d6b8c77b54]
module.management.local_sensitive_file.public_key_openssh: Refreshing state... [id=c97484ae519bd52a919fd4d75b7e9d497ea63a88]
module.candidate.local_sensitive_file.private_key: Refreshing state... [id=bfc5cb4955bfb87afab5bd073b65afc829dd3e33]
module.windows_server.data.template_file.base_config: Reading...
module.windows_server.data.template_file.base_config: Read complete after 0s [id=69ba4ef6cbd71dd906c8446553d8953bb7a72abe3afc1607
aws_key_pair.management: Refreshing state... [id=demo_management]
aws_key_pair.candidate: Refreshing state... [id=demo_candidate]
module.ubuntu_server.data.aws_ami.ubuntu_22_04: Reading...
module.management_server.data.aws_ami.ubuntu: Reading...
```

```
Do you really want to destroy all resources in workspace "demo"?
  Terraform will destroy all your managed infrastructure, as shown above.
  There is no undo. Only 'yes' will be accepted to confirm.

  Enter a value:
```

Copyright © 2022 Accenture. All rights reserved.

03

Development

Copyright © 2022 Accenture. All rights reserved.

Core Concepts - Lab Templates

- Single configuration file that defines a lab
- Lab templates are Terraform variable files (tfvars)
- Templates are structured as follows:
  - User configurable settings
  - Networks
  - Systems

Copyright © 2022 Accenture. All rights reserved.

Core Concepts - Networks

```
14  ############ / Networking
15  address_space_lab         = "10.1.0.0/16"
16  address_space_management  = "10.1.254.0/24"
17
18  networks = [
19      {
20          network_id    = "1"
21          network_name  = "INTERNAL"
22          network_template = "internal_permissive"
23          address_space = "10.1.1.0/24"
24      },
25      {
26          # Exposes RDP and SSH ports to the candidate IP ranges
27          network_id    = "2"
28          network_name  = "CANDIDATE_EXTERNAL"
29          network_template = "candidate"
30          address_space = "10.1.2.0/24"
31      }
32  ]
33
34  security_rules = [
35  ]
```

Copyright © 2022 Accenture. All rights reserved.

Core Concepts - Network Templates

Currently available network templates

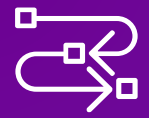
candidate

Allows inbound SSH and RDP traffic from the from the public IP ranges defined in `candidate_ip`

internal_permissive

Allows inbound connections from all lab networks.

No direct access from the Internet



internal_segregated

Only allows traffic within the same lab network.

`security_rules` are required to define allowed traffic

Copyright © 2022 Accenture. All rights reserved.

Core Concepts - Systems

```
37  ############ / Systems
38  systems = [
39      {
40          module      = "microsoft_windows_server"
41          os_version  = "2022"
42          size        = "t2.medium"
43          network_id  = "1"
44          hostname    = null
45          private_ip  = "10.1.1.10"
46          public_ip   = false
47          class       = "DC"
48          id          = "01"
49          features    = [ ]
50      },
51      {
52          module      = "microsoft_windows_server"
53          os_version  = "2022"
54          size        = "t2.small"
55          network_id  = "2"
56          hostname    = null
57          private_ip  = null
```

Copyright © 2022 Accenture. All rights reserved.

Core Concepts - Systems

Supported Operating Systems

Operating System	Module Name	OS Version	AWS	Azure
Windows Server 2016	microsoft_windows_server	2016	X	X
Windows Server 2019	microsoft_windows_server	2019	X	X
Windows Server 2022	microsoft_windows_server	2022	X	X
Windows 10 (21H2)	microsoft_windows_desktop	10		X
Windows 11 (22H2)	microsoft_windows_desktop	11		X
Ubuntu Server 20.04	canonical_ubuntu_server	20.04	X	X
Ubuntu Server 22.04	canonical_ubuntu_server	22.04	X	X
Kali Linux (latest)	offensivesecurity_kalilinux	latest	X	X

Copyright © 2022 Accenture. All rights reserved.

Core Concepts – System Features

Defining a domain and its users

```
features    = [
    {
        name = "AD_Forest"
        value = [
            {name = "domain_name", value = "dynamic.lab"},
            {name = "domain_netbios_name", value = "dynamic"}
        ]
    },
    {
        name = "AD_User"
        value = [
            {name = "HighPriv", password = "TheSkyIsTheLimit.2022?"},
            {name = "LowPriv", password = "Sup3rSecretString.2022!"}
        ]
    },
    {
        name = "AD_Group_Membership"
        value = [{name = "Domain Admins", value = "HighPriv"}]
    }
]
```

Copyright © 2022 Accenture. All rights reserved.

Core Concepts – System Features

Joining a machine to the domain

```
80          features    = [
81              {
82                  name = "AD_Join"
83                  value = [
84                      {name = "domain_name", value = "dynamic.lab"},
85                      {name = "domain_dns_server", value = "10.1.1.10"},
86                  ]
87              },
88              {
89                  name = "Win_Group_Membership"
90                  value = [{name = "Remote Desktop Users", value = "LowPriv"}]
91              }
92          ]
```

Copyright © 2022 Accenture. All rights reserved.

Core Concepts – System Features

Implemented features

AD_Forest
AD_Domain
AD_Join
AD_User
AD_User_Password
AD_User_Right
AD_Group
AD_Group_Membership
AD_SecEdit_Access
AD_MSA
AD_MSA_AllowRetrieve
AD_SetSPN
AD_GPO
AD_GPO_ACL
AD_Object_ACL
AD_Organizational_Unit
AD_Object_Organizational_Unit
AD_Unconstrained_Delegation
AD_Constrained_Delegation
AD_DNS_Forwarder_Zone
AD_DNS_Record
AD_Trust
AD_CleanUp
Win_User
Win_User_Password
Win_Group
Win_Group_Membership
Win_Directory
Win_Simple_File
Win_Dirtree_Copy
Win_Filesystem_ACL
Win_File_Share
Win_Defender_Disable
Win_PowerShell_Script
Win_EARLY_PowerShell_Script
Win_CleanUp
IIS_Web_Application
MSSQL_Server
flag
ATTCK_T1003_1
ATTCK_T1187_1
ATTCK_T1552_2_1
ATTCK_T1574_9_1
Linux_User
Linux_Authorized_Keys
Linux_Directory
Linux_Simple_File
Linux_Dirtree_Copy
Linux_Apt_Package_Install
Linux_Apt_Package_Upgrade
Linux_Nginx_Website
Linux_Shell_Script
Linux_EARLY_Shell_Script

Copyright © 2022 Accenture. All rights reserved.

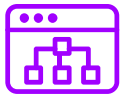
Time for a new release

Copyright © 2022 Accenture. All rights reserved.

Dynamic Labs - version 1.2

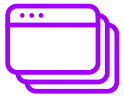
Available on GitHub

Simplified usage and template syntax



Improved documentation

Added new system features and extended the supported OS versions



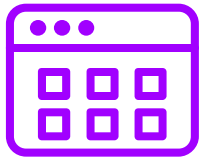
New and improved lab templates

Copyright © 2022 Accenture. All rights reserved.

Contributing

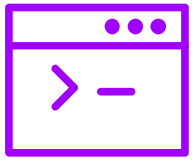
Copyright © 2022 Accenture. All rights reserved.

Contributing to Dynamic Labs



Templates

- Create new template
  - Description
  - Walkthrough
- We'll add them to the community version



Core Code

- Implement new system features
- Add support for a new cloud providers

Copyright © 2022 Accenture. All rights reserved.

04

Conclusion

Copyright © 2022 Accenture. All rights reserved.

Takeaways

Dynamic Labs is a tool that provides a **modern approach to lab environments** for red teamers and pentesters.

Open Source

Tool publicly available at https://github.com/ctxis/DynamicLabs

Lab templates

Lightweight and easy to create, modify and distribute

Open to community contributions

Create lab templates and share them with the community

Copyright © 2022 Accenture. All rights reserved.

Credits

Rohan Durve (@Decode141)

Copyright © 2022 Accenture. All rights reserved.

Thank you

David Turco

@endle_ _

https://github.com/ctxis/DynamicLabs

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Song, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 710,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

Disclaimer: Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this presentation and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

Copyright © 2022 Accenture. All rights reserved.