Successful **Deception Tactics**

The Deception layer recommendations below are easily deployed using the automatic nature of the Fidelis Deception® solution.

TACTICS AND TECHNIQUES*

DECEPTION LAYER

INITIAL ACCESS

Exploiting Public-Facing Application

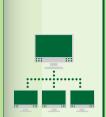


- Deploy decoys running the organization's public facing applications. It can include FTP server, SSH server, web-based applications (HTTP/S) and more. Sanitize the triggered alerts when valid
 - credentials are used or find campaigns against the organization.

CREDENTIAL ACCESS

CREDENTIAL ACCESS

Brute Force



- Deploy decoys with different operating systems running applications like databases and servers. Deploy breadcrumbs on assets directing towards
- the deployed decoys. Attackers can reach out to the decoys based on
- random scanning or using the breadcrumbs and then try to brute force the login mechanism.

CREDENTIAL ACCESS

Poisoning and Relay

LLMNR/NBT-NS



LLMNR, ARP, WPAD and more.

Deploy Decoys running protocols for luring the

attackers to communicate with the decoys like

CREDENTIAL ACCESS

Sniffing

Network



Deploy decoys that are active on the network to be detected by the attackers. Decoys activities on the network includes MITM

different broadcasts packets, etc.

luring protocols, ARP requests, HTTP requests,

DISCOVERY

DISCOVERY

Discovery

Account



requests to acquire information about users and groups. Define faked users in Active Directory binded to

decoys that are communicating with the Active

Deploy decoys that are responding to network

Directory to be revealed when the attackers query the Active Directory.

DISCOVERY

Bookmark Discovery

Cookie and



web server applications and web services.

Deploy decoys with shared folders and files

Deploy decoys with applications like web server

bookmarks luring the attackers to access the

and web services; deploy the relevant browser

DISCOVERY

Directory Discovery

File and



to access the decoys.

breadcrumbs to lure the attackers to access the

shared folders and/or use the content in the files

DISCOVERY

Scanning

Network

Service



services. Decoys triggers on accesses even if services are not deployed on specific ports.

Deploy decoys with multiple services responding

to attackers scanning the network for available

DISCOVERY

Discovery

Network Share



 Deploy breadcrumbs files/emails/etc. leading to these shared folders.

shared folders.

Deploy decoys with shared folders and relevant

breadcrumbs to lure the attackers to access the

Deploy decoys with multiple services like SMB,

FTP, SSH, RDP, HTTP, responding to attackers

scanning the network and queries for available

DISCOVERY

Remote System

Discovery

System

Network

Connection

Discovery



services.

DISCOVERY

System

Service

Discovery



services.

connections to the decoys.

Deploy decoys with multiple services responding

to attackers scanning the network for available

Deploy decoys running multiple services

luring the attackers to find the active

like SMB, FTP, SSH, RDP, HTTP and relevant

active breadcrumbs accessing the decoys

LATERAL MOVEMENT

DISCOVERY

LATERAL MOVEMENT

Exploitation

of Remote

Service



Deploy decoys running multiple services like

relevant breadcrumbs to lure the attackers

SMB, FTP, SSH, RDP, HTTP, database and

to access the decoys.

access these RDP decoys.

LATERAL MOVEMENT

ENT

Remote **Desktop**

Protocol



Deploy decoys running RDP server and breadcrumbs luring the attackers to

LATERAL MOVEN LATERAL MOVEMENT

Windows

Administrator

Share

Remote

Services



Deploy decoys running administrator share

luring the attackers to access these shares.

Deploy services like Telnet, SSH and FTP along

attackers to access these services.

with breadcrumbs to these services to lure the

LATERAL MOVEMENT

Remote

File Copy



databases to allow the attackers to retrieve files from the decoys.

Deploy decoys with shared folders, files, and

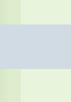
COLLECTION

Data from



COLLECTION

Information Repositories



Deploy decoys with shared folders, data bases

and huge amount of data to lure attackers to

investigate the data and find valuable information.

COLLECTION

Local Systems

Data from



the systems.

Deploy decoys with shared folders including data

files to allow the attackers to retrieve files from

COLLECTION

Data from

Network

Shared Drive



 Deploy decoys with shared folders including data files to allow the attackers to retrieve files from

*MITRE ATT&CK®



the systems.