

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

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

LLMNR/NBT-NS Poisoning and Relay



- Deploy Decoys running protocols for luring the attackers to communicate with the decoys like LLMNR, ARP, WPAD and more.

CREDENTIAL ACCESS

Network Sniffing



- Deploy decoys that are active on the network to be detected by the attackers.
- Decoys activities on the network includes MITM luring protocols, ARP requests, HTTP requests, different broadcasts packets, etc.

DISCOVERY

DISCOVERY

Account Discovery



- Deploy decoys that are responding to network requests to acquire information about users and groups.
- Define faked users in Active Directory binded to decoys that are communicating with the Active Directory to be revealed when the attackers query the Active Directory.

DISCOVERY

Cookie and Bookmark Discovery



- Deploy decoys with applications like web server and web services; deploy the relevant browser bookmarks luring the attackers to access the web server applications and web services.

DISCOVERY

File and Directory Discovery



- Deploy decoys with shared folders and files breadcrumbs to lure the attackers to access the shared folders and/or use the content in the files to access the decoys.

DISCOVERY

Network Service Scanning



- Deploy decoys with multiple services responding to attackers scanning the network for available services.
- Decoys triggers on accesses even if services are not deployed on specific ports.

DISCOVERY

Network Share Discovery



- Deploy decoys with shared folders and relevant breadcrumbs to lure the attackers to access the shared folders.
- Deploy breadcrumbs files/emails/etc. leading to these shared folders.

DISCOVERY

Remote System Discovery



- Deploy decoys with multiple services like SMB, FTP, SSH, RDP, HTTP, responding to attackers scanning the network and queries for available services.

DISCOVERY

System Network Connection Discovery



- Deploy decoys running multiple services like SMB, FTP, SSH, RDP, HTTP and relevant active breadcrumbs accessing the decoys luring the attackers to find the active connections to the decoys.

DISCOVERY

System Service Discovery



- Deploy decoys with multiple services responding to attackers scanning the network for available services.

LATERAL MOVEMENT

LATERAL MOVEMENT

Exploitation of Remote Service



- Deploy decoys running multiple services like SMB, FTP, SSH, RDP, HTTP, database and relevant breadcrumbs to lure the attackers to access the decoys.

LATERAL MOVEMENT

Remote Desktop Protocol



- Deploy decoys luring RDP server and breadcrumbs luring the attackers to access these RDP decoys.

LATERAL MOVEMENT

Remote Services



- Deploy services like Telnet, SSH and FTP along with breadcrumbs to these services to lure the attackers to access these services.

LATERAL MOVEMENT

Windows Administrator Share



- Deploy decoys running administrator share luring the attackers to access these shares.

LATERAL MOVEMENT

Remote File Copy



- Deploy decoys with shared folders, files, and databases to allow the attackers to retrieve files from the decoys.

COLLECTION

COLLECTION

Data from 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

Data from Local Systems



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

COLLECTION

Data from Network Shared Drive



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

*MITRE ATT&CK®