CCTC Security

OPERATION Dry Run



Tasking

All actions must be in accordance with mission brief, scope, and RoE.

Complete the taskings on each referenced target below.

Each heading is the hostname of a target. The first listed target’s hostname is “PublicFacingWebsite”.

#

# PublicFacingWebsite

## Perform Reconnaissance

1. Find all information about, and contained within, the target system to include potential phishing targets, website directory structure, and hidden pages.
2. Actively scan and interact with target to find potential attack vectors.

## Attempt Exploitation || Gain Initial Access

1. Use information gained from reconnaissance to gain access to the system.
2. There are multiple ways to gain access, try to find all.

## Find Additional Targets

1. Perform post-exploitation tasks (situational awareness, localhost enumeration, privilege escalation, etc).
2. Discover additional targets through analysis of information from post-exploitation tasks.
3. Discover potential vulnerable binary to attempt exploitation and read sensitive file at *“/root/secret\_msg.txt”*

## Pivot to Found Targets

1. Pivot through network to other targets as you find them.

# NOTES

#

# BestWebApp

## Perform Reconnaissance

1. Find all information about, and contained within, the target system to include potential phishing targets, website directory structure, and hidden pages.
2. Actively scan and interact with target to find potential attack vectors.

## Attempt Exploitation

1. Attempt to retrieve privileged information from the target by using information found in reconnaissance. Reconnaissance from other targets within the network may have information relevant to any target.

# NOTES

#

# RoundSensor

## Perform Reconnaissance

1. Actively scan and interact with target to find potential attack vectors.

## Attempt Exploitation || Gain Initial Access

1. Use information gained from reconnaissance to gain access to the system. Reconnaissance from other targets within the network may have information relevant to any target.

## Find Additional Targets

1. Perform post-exploitation tasks (situational awareness, localhost enumeration, privilege escalation, etc).
2. Discover additional targets through analysis of information from post-exploitation tasks.

## Pivot to Found Targets

1. Pivot through network to other targets as you find them.

# NOTES

#

# Windows-Workstation

## Perform Reconnaissance

1. Actively scan and interact with target to find potential attack vectors.

## Attempt Exploitation || Gain Initial Access

1. Use information gained from reconnaissance to gain access to the system. Reconnaissance from other targets within the network may have information relevant to any target.

## Find Additional Targets

1. Perform post-exploitation tasks (situational awareness, localhost enumeration, privilege escalation, etc).
2. Discover additional targets through analysis of information from post-exploitation tasks.

## Pivot to Found Targets

1. Pivot through network to other targets as you find them.

# NOTES