RING 1 – ENTER THE WANG

"OPEN SESAME" – PHYSICAL ABUSE

TASK: PICK THE CABIN LOCKS
GAIN PHYSICAL ACCESS TO DEVICES
TASK: GAIN NETWORK SWITCH CONSOLE ACCESS
PHYSICALLY ACCESS THE NETWORK SWITCH VIA CONSOLE PORT TO CONFIGURE SETTINGS.
TASK: CONFIGURE MITM PORT ON NETWORK SWITCH
SET UP A MAN-IN-THE-MIDDLE (MITM) PORT TO INTERCEPT NETWORK TRAFFIC.
TASK: SUCCESSFUL USE OF TOOLS OF THE TRADE
FLIPPER ZERO USAGE: USE FZ AS A MALICIOUS USB DEVICE.
TASK: BIOMETRIC SPOOFING
SPOOF BIOMETRIC SYSTEMS SUCH AS FINGERPRINT OR FACIAL SCANNERS.
TASK: USB DEVICE ATTACK
USE MALICIOUS USB DEVICES TO COMPROMISE SYSTEMS.
USE MALICIOUS USB DEVICES FOR SUCCESSFUL CALLBACK TO ATTACKER STATION

"CLEANING HOUSE" – A VACUUM IN SPACE

TASK: GAIN PHYSICAL ACCESS TO NEXTGEN ROBOTICS VACUUM CLEANER PRINTBOARD(S)
LOCATE AND SUCCESSFULLY CONNECT TO USB PORT OF ROBOT.
IDENTIFY OPERATING SYSTEM OF ROBOT.
LOGIN TO SYSTEMBOARD OF ROBOT.
GAIN ACCESS SENSORS OF ROBOT.
MANIPULATE SENSORS OF ROBOT.
TASK: INTERCEPT WIRELESS TRAFFIC NEXTGEN ROBOTICS VACUUM CLEANER
MITM WIRELESS TRAFFIC ROBOT.
LOCATE CLOUDMANAGEMENT PORTAL NEXTGEN ROBOTICS.
LOGIN CLOUDMANAGEMENT PORTAL NEXTGEN ROBOTICS.

"THE ENDLESS RIVER" – NETWORKING ABUSE

TASK: CONFIGURE MITM PORT ON NETWORK SWITCH
SET UP A MAN-IN-THE-MIDDLE (MITM) PORT TO INTERCEPT NETWORK TRAFFIC.
TASK: MITM WIRED NETWORK TRAFFIC
IDENTIFY AND ABUSE VLAN STRUCTURE (VLAN HOPPING)
INTERCEPT AND ANALYZE DATA TRANSMITTED OVER WIRED NETWORKS.
IDENTIFY ACTIVE DEVICES AND SERVICES WITHIN THE NETWORK.
SET UP AN SSL PROXY AND SUCCESSFULLY INTERCEPT WIRED SSL TRAFFIC.
TASK: MITM WIRELESS NETWORK TRAFFIC
CAPTURE AND ANALYZE WIRELESS NETWORK TRAFFIC.
IDENTIFY ACTIVE DEVICES AND SERVICES WITHIN THE NETWORK.
CREATE A FAKE WI-FI NETWORK THAT MIMICS A LEGITIMATE ONE TO INTERCEPT NETWORK TRAFFIC.
SET UP AN UNAUTHORIZED ACCESS POINT TO INTERCEPT AND MANIPULATE NETWORK TRAFFIC.
SET UP AN SSL PROXY AND SUCCESSFULLY INTERCEPT WIRELESS SSL TRAFFIC.
TASK: MITM BLUETOOTH NETWORK TRAFFIC
INTERCEPT AND EXPLOIT BLUETOOTH COMMUNICATIONS.
TASK: CAPTURE PLAINTEXT NETWORK TRAFFIC
IDENTIFY AND EXTRACT UNENCRYPTED INFORMATION FROM NETWORK TRAFFIC.
TASK: EXTRACT SENSITIVE INFORMATION
RETRIEVE CONFIDENTIAL DATA SUCH AS PASSWORDS, EMAILS, AND PERSONAL INFORMATION.
TASK: ABUSE BLUETOOTH DEVICES
RFID BLUETOOTH CLONING.
EXPLOIT VULNERABILITIES IN BLUETOOTH DEVICES TO GAIN UNAUTHORIZED ACCESS.
EXTRACT DATA FROM BLUETOOTH DEVICES.

RING 1 – ENTER THE WANG

PART DEUX

"ZAPPATITE" – ENDPOINT ABUSE

TASK: SCAN AND FIND VULNERABILITIES (WINDOWS & LINUX)
USE TOOLS TO (REMOTELY) SCAN SYSTEMS FOR KNOWN VULNERABILITIES.
TASK: EXPLOIT VULNERABILITIES (WINDOWS & LINUX)
LEVERAGE DISCOVERED VULNERABILITIES TO GAIN UNAUTHORIZED ACCESS.
ACCESS AND EXPLOIT SECURE SHELL (SSH) SERVICES ON LOCAL SYSTEMS. (LINUX)
EXECUTE ARBITRARY CODE ON LOCAL SYSTEMS BY EXPLOITING VULNERABILITIES.
EXECUTE MALICIOUS CODE TO GAIN CONTROL OF A TARGET SYSTEM.
TASK: ENUMERATE SERVICES (WINDOWS & LINUX)
ENUMERATE AVAILABLE SERVICES ON LOCAL DEVICES TO IDENTIFY POTENTIAL TARGETS.
TASK: ENUMERATE LOCAL ACCOUNTS (WINDOWS & LINUX)
IDENTIFY AND LIST ALL LOCAL USER ACCOUNTS ON A TARGET SYSTEM.
TASK: GAIN REMOTE ACCESS (WINDOWS)
GAIN REMOTE CONTROL OF A WINDOWS MACHINE USING RDP.
USE WMI TO EXECUTE COMMANDS ON REMOTE WINDOWS MACHINES.
TASK: GAIN REMOTE ACCESS (LINUX)
GAIN REMOTE CONTROL OF A LINUX MACHINE USING SSH.
USE RDP TO CONTROL A LINUX MACHINE, TYPICALLY THROUGH XRDP OR SIMILAR TOOLS.
TASK: ABUSING BUILT-IN WINDOWS FEATURES
EXECUTE COMMANDS ON REMOTE SYSTEMS USING POWERSHELL.
CREATE OR MODIFY SCHEDULED TASKS TO EXECUTE MALICIOUS ACTIONS.
USE WINRM FOR REMOTE MANAGEMENT AND COMMAND EXECUTION.
TASK: ABUSING BUILT-IN LINUX FEATURES
CREATE OR MODIFY CRON JOBS TO EXECUTE MALICIOUS ACTIONS.
EXPLOIT THE SSH AGENT TO USE LOADED KEYS WITHOUT NEEDING PASSWORDS.
EXPLOIT SUDO PRIVILEGES TO EXECUTE COMMANDS AS THE SUPERUSER.
TASK: CREDENTIAL HARVESTING (LINUX)
STEAL SSH KEYS TO GAIN UNAUTHORIZED ACCESS TO REMOTE SYSTEMS.
EXTRACT PASSWORD HASHES OR PLAINTEXT PASSWORDS FROM THE SYSTEM.
TASK: CREDENTIAL HARVESTING (WINDOWS)
PASSWORD DUMPING: EXTRACT PASSWORD HASHES OR PLAINTEXT PASSWORDS FROM MEMORY.
PASS THE HASH: USE CAPTURED PASSWORD HASHES TO AUTHENTICATE WITHOUT KNOWING THE ACTUAL PASSWORD.
PASS THE TICKET: USE STOLEN KERBEROS TICKETS TO IMPERSONATE USERS.
TASK: ESTABLISH SUCCESSFUL CALLBACK TO ATTACKER STATION
SET UP A REVERSE CONNECTION FROM THE TARGET SYSTEM TO THE ATTACKER'S CONTROL SYSTEM.
ESTABLISH PERSISTENCE WHICH SURVIVES REBOOTS.
TASK: GAIN LOCAL ADMINISTRATOR/ROOT RIGHTS
ELEVATE PRIVILEGES TO OBTAIN ADMINISTRATIVE ACCESS TO A LOCAL SYSTEM.
TASK: ENUMERATE DOMAIN ACCOUNTS
IDENTIFY AND LIST DOMAIN USER ACCOUNTS ON THE LOCAL SYSTEM.
TASK: BYPASSING SECURITY SYSTEMS
AVOID DETECTION BY DIGITAL SYSTEMS.

NYMACON

THE DOJO EDITION '24

Nijmegen · HUNT & HACKETT · TeleMANN · Radboud University

RING 2 – TINY GRASSHOPPER

"REMEMBER THE CANT" – LATERAL MOVEMENT

TASK: SCAN AND MAP THE NETWORK
IDENTIFY AND DOCUMENT ALL DEVICES AND NETWORK TOPOLOGY.
TASK: ENUMERATE (REMOTE) SERVICES
ENUMERATE AVAILABLE SERVICES ON NETWORKED DEVICES TO IDENTIFY POTENTIAL TARGETS.
TASK: REMOTE CODE EXECUTION
EXECUTE ARBITRARY CODE ON REMOTE SYSTEMS BY EXPLOITING VULNERABILITIES.
TASK: BREAKOUT FROM LOCAL ENDPOINT
MOVE FROM AN INITIALLY COMPROMISED ENDPOINT TO OTHER DEVICES IN THE NETWORK.
ROUTE TRAFFIC THROUGH MULTIPLE INTERMEDIATE SYSTEMS TO OBFUSCATE THE ATTACK SOURCE.
USE A COMPROMISED SYSTEM AS A VPN ENDPOINT TO ACCESS INTERNAL NETWORKS.
TASK: DYNAMIC DNS
USE DYNAMIC DNS SERVICES TO MAINTAIN CONTROL OVER COMPROMISED SYSTEMS WITH CHANGING IP ADDRESSES.
TASK: BYPASSING SECURITY SYSTEMS
AVOID DETECTION BY DIGITAL SYSTEMS WHILE MOVING LATERALLY

RING 3 – COWABUNGA

"WAKANDA FOREVER!" – IDENTITY PROVIDER ABUSE

TASK: ENUMERATE DOMAIN USERS
USE A TOOL LIKE LDAPSEARCH OR NET USER TO ENUMERATE ALL USERS
TASK: ENUMERATE DOMAIN GROUPS
LIST ALL GROUPS WITHIN THE ACTIVE DIRECTORY DOMAIN.
TASK: ENUMERATE DOMAIN ADMINS
IDENTIFY USERS WITH DOMAIN ADMIN PRIVILEGES.
TASK: EXTRACT KERBEROS TICKETS
USE MIMIKATZ TO EXTRACT KERBEROS TICKETS FROM MEMORY.
TASK: PASS-THE-HASH ATTACK
USE CAPTURED NTLM HASHES TO AUTHENTICATE WITHOUT KNOWING THE ACTUAL PASSWORD.
TASK: DUMP ACTIVE DIRECTORY DATABASE
DUMP THE NTDS.DIT FILE FROM THE DOMAIN CONTROLLER.
TASK: PRIVILEGE ESCALATION VIA SERVICE MISCONFIGURATION
EXPLOIT A SERVICE RUNNING WITH SYSTEM PRIVILEGES DUE TO MISCONFIGURATION.
TASK: KERBEROASTING ATTACK
REQUEST SERVICE TICKETS FOR SPNS AND CRACK THE HASHES OFFLINE.
TASK: ABUSE UNCONSTRAINED DELEGATION
EXPLOIT A SYSTEM CONFIGURED WITH UNCONSTRAINED DELEGATION TO EXTRACT TGTS.
TASK: DCSHADOW ATTACK
USE DCSHADOW TO INJECT MALICIOUS CHANGES INTO ACTIVE DIRECTORY.

RING BONUS (1)

"NO SURPRISES" – NEVER A DULL MOMENT

TASK: DOCUMENTING ACCESS TECHNIQUES
RECORD DETAILED STEPS TAKEN TO BYPASS SECURITY MEASURES.
TASK: CREATING PROOF OF CONCEPT (POC) FOR ATTACKS
DEVELOP POC VIDEOS OR PRESENTATIONS TO DEMONSTRATE SUCCESSFUL ATTACKS.
TASK: REPORTING VULNERABILITIES
COMPILE AND SUBMIT COMPREHENSIVE REPORTS ON DISCOVERED VULNERABILITIES AND THEIR POTENTIAL IMPACT.

RING BONUS (2)

"BURNING DOWN THE HOUSE" – ZAP THE WEB

TASK: SCANNING, ENUMERATION
SCAN AND ENUMERATE THE ENVIRONMENT WHILE REMAINING UNDETECTED.
IDENTIFY THE TECHNOLOGIES USED BY THE APPLICATION.
TASK: THE ULTIMATE DORKMASTER
USE GOOGLE DORKS TO FIND INDEXED PAGES OR FILES THAT SHOULDN'T BE PUBLIC.
USE AI TO FURTHER DEEPEN OUT YOUR DORKS.
TASK: FIND RELATIVE ENVIRONMENTS
DISCOVER RELATIVE SUB-DOMAINS.
DISCOVER HIDDEN DIRECTORY OR FILES.
TASK: FIND AND EXPLOIT A MISCONFIGURATION
LOGIN THE WEBFORM.
EXPLOIT PDF GENERATION WITH MALICIOUS DATA.
EXPLOIT POST PARAMETER POLLUTION BY INJECTING DUPLICATE OR UNEXPECTED PARAMETERS CAUSING THE SERVICE TO BEHAVE IN AN UNINTENDED WAY.

NYMACON

THE DOJO EDITION '24

Nijmegen · HUNT & HACKETT · TeleMANN · Radboud University