Penetration Testing

Reconaissance

Scanning

- Nmap
- Netdiscover
- arp-scan
- Masscan
- Metasploit
- Nessus

Scanning & Enumeration

HTTP/HTTPS

- Nikto
- Dirbuster
- Dirb
- Gobuster
- Source Code
- Burp Suite
- Test Server upload
- Davtest

SMB

- Msfconsole - smb_version
- smbclient
- enum4linux (not working properly)

SSH

- Connection attempt

FTP

- anonymous access
- binary

Network

- ipconfig /all
- arp -a
- route print
- netstat -ano

Vulnerability Research

- Google
- Searchsploit
- Exploit Database
- Metasploit - search

Overview

Target Validation

- WHOIS
- nslookup
- dnsrecon

Finding Subdomains

- Google Fu
- dig
- Nmap
- Sublist3r
- Bluto
- crt.sh

Fingerprinting

- Nmap
- Wappalyzer
- WhatWeb
- BuiltWith
- Netcat

Data Breaches

- HaveIbeenPwned
- Breach-Parse
- WeLeakInfo
- scylla.sh
- leakedsource.ru

Email Address Gathering

- Hunter.io (Domain Search)

Identify Target

- bugcrowd.com

Breached Credentials

- Breach-Parse
- scylla.sh
  - email:*bbc.co.uk
  - email:username*

OSINT

- The Harvester

Subdomains

- Sublist3r
- crt.sh
- OWASP Amass
- Tonnomnon HTTPprobe

Identify Website Technologies

- BuiltWith
- Wappalizer
- whatweb

Information Gathering with Burp Suite

Google Fu

Social Medla

- LinkedIn
- Twitter

Exploitation

Initial Attack Vectors

LLMNR Poisoning

- Responder
  - LLMNR
  - NBT-NS
  - DNS/MONS
- Defences
  - Disable LLMNR and NBT-NS
  - Require Network Access Control
  - Require Strong User Passwords

Capturing NTLMv2 Hashes

- Responder

Password Cracking (Hashcat)

Host Discovery

- Nessus

SMB Signing Disabled

- Nmap script

SMB Relay Attacks

- Responder
  - HTTP Off
  - SMB Off
- ntlmrelayx
  - SAM Hashes Dump
    - Crack offline
    - Pass-the-Hash
  - Interactive shell -i
    - Netcat
  - Command execute -c
    - Reverse shell
      - Powershell
      - msf web_delivery
      - other
  - Execute .exe file -e
    - msfvenom
    - meterpreter
- Defences
  - Enable SMB signing on all devices
    - It will completely stop the attack
    - Performance issues with file copy
  - Disable NTLM Authentication
    - Stops the attack
    - If Kerberos stops working, back to NTLM
  - Account tiering
    - Admin only logging into their accounts / servers / domain controllers
    - Local Admin restriction
    - No local Admin
    - prevent lateral movement

Gain Shell Access

- msfconsole
  - exploit/windows/smb/psexec
  - exploit/windows/smb/psexec_psh
- psexec.py
  - AV noisy
- smbexec.py
  - Less noisy / Half-shell
- wmiexec.py
  - Less noisy / Half-shell

IPv6 Attacks

- LDAP Relay
  - mitm6
    - aclpwn restore
    - new user creation on DC
  - ntlmrelayx
    - info dump (loot folder)
    - delegate access
- Defenses
  - Disable IPv6
    - Possible unwanted side effects
    - Define Block Rules / instead of Allow Rules
  - Disable wpad if not in use
  - Enable LDAP signing and channel binding
    - usually not enabled
  - Put admin users into the protected users group
    - prevent impersonation or delegation

Other Attack Vectors and Strategies

- Day begins with
  - mitm6
    - Get loot back
    - Get account created on Domain Controller
      - Easy win
    - Early morning
    - Lunch time
  - Responder
    - See how the network responds
      - Are they giving us hashes ?
      - Are those hashes easy to crack ?
      - Easy win
      - If LMNR is disabled
        - might have had Pentest before
        - might know common attacks
    - Looking for hashes
    - Early morning
    - Lunch time
  - Nessus scan
  - Nmap scan
  - Look for SMB open / signing disbled
    - Morning
      - Pickup targets / hashes for SMB Relay attacks
    - Afternoon
      - Relay hashes
  - HTTP_Version (Metasploit)
    - Sweep entire network for websites
      - Look for printers
        - Loot at logins
          - Check for default creds
        - Check for Vulns
        - Scan-to-computer feature
        - Lot of people don't secure their printers
        - Is user domain admin on that printer ?
          - might get domain admin off
          - dump creds in clear text
            - get passwords for SMB user
        - using individual user accounts
      - Jenkins Instances
        - Often wide open
    - Use this if scans are taking too long
    - Less likely to be picked-up
  - Try all possible ways in
    - Search for low hanging fruits
    - Think outside the box
    - Enumerate as much as you can
    - Don't just focus on the exploit

Active Directory

Easy-win Strategy

- nmap --script=smb-enum-users.nse
- GetADUsers.py -dc-ip 10.10.10.161 htb.local/
- kerbrute userenum --dc 10.10.222.155 -d spookysec.local usernames.txt -t 100
- Attempt to list and get TGTs for those users that have the property "Do not require Kerberos preauthentication" set (UF_DONT_REQUIRE_PREAUTH)
  - GetNPUsers.py -dc-ip 10.10.10.161 htb.local/
- Users Enumeration
- Get TGT hash, for those users with such configuration
  - GetNPUsers.py -request -dc-ip 10.10.10.161 htb.local/
    - Hashcat
    - John the Ripper
    - Get a shell
      - Evil-winrm
      - psexec
- Brute force discovery of users, passwords and password spray
  - Kerbrute
  - Metasploit auxiliary/gather/kerberos_enumusers
- Abuse WriteDACL permissions
  - ntlmrelayx
  - PowerView
- Exploiting Kerberos
  - ASREPRoasting
    - GetNPUsers.py
      - Get Hashes
      - Crack the hashes
  - Shares Enum
    - smbclient
- Elevate Privileges
  - Secretsdump
    - NTDS.DIT
    - secrets dump
      - Pass-the-Hash
        - crackmapexec
          - check where you can authenticate
        - psexec
        - evil-winrm
        - Get system shell

Enumeration

- PowerView
- Bloodhound

Attack

- Dump the Hashes
  - secretsdump
    - SAM Dumping
    - LSA Secrets Dumping
    - DPAPI_SYSTEM KEY
  - Metasploit
    - psexec
    - meterpreter
    - hashdump
- Crack NTLM Hashes
  - Hashcat
- Pass-the-Hash
  - crackmapexec
    - Pwn3d! or green [+]
      - Try to authenticate with Psexec
        - get a shell
    - not Pwn3d!
      - no SMB access
  - Cannot pass NTLMv2
  - no cracking needed
- Pass-the-Password
  - crackmapexec
    - Pwn3d!
      - Try get a shell with Psexec
    - not Pwn3d!
      - no SMB access
    - Dump local SAM hashes
- Token Impersonation
  - Mimikatz
  - Meterpreter - Incognito
- Kerberoasting
  - Request TGT, provide NTLM hash
  - Receive TGT encrypted with krbtgt hash
  - Request TGS for Server (Presents TGT)
    - GetUserSPNs.py
  - Receive TGS encrypted with Server's account hash
  - Crack the hash
- GPP / cPassword
  - smbclient
    - prompt off
    - recurse on
    - mget *
  - Groups.xml
    - cpassword
      - gpp_decrypt
  - Invoke-GPP
  - smb_enum_gpp module in Metasploit
- Mimikatz
  - privilege::debug
  - Credential Dumping
    - sekurlsa::logonpasswords
      - NTLM
      - Logged in accounts
      - wdigest
    - SAM dump
      - lsadump::sam
      - lsadump::sam /patch
      - sam dump not working
        - shell with Metasploit
        - secretsdump.py
        - crackmapexec
      - just download the SAM
        - windows/system32/config/SAM
        - windows/system32/config/SECURITY
        - windows/system32/config/SYSTEM
        - crack with secretsdump.py
    - LSA dump
      - lsadump::lsa /patch
      - lsadump::lsa /inject /name:krbtgt
        - Pull down krbtgt account
          - SID
          - NTLM
          - Golden Ticket
            - Pass-the-Ticket
              - misc::cmd
                - opens cmd prompt
                - Access any computer
                  - dir \\THEPUNISHER\c$
                  - psexec.exe
                  - PsExec64.exe -accepteula \\THEPUNISHER cmd.exe
                  - shell
            - Persistence
          - Silver Ticket
            - Stealthier
    - ntds.dit
      - Usernames
      - Passwords
    - Why do we dump ?
      - Crack passwords offline
        - % we are able to crack
          - weak password policy
          - strong password policy
      - Golden Ticket attack
        - Kerberos Ticket Granting Ticket
- Features
  - Pass-the-Hash
  - Over-Pass-the-Hash
  - Pass-the-Ticket
  - Golden Ticket
  - Silver Ticket

Post-Compromise

- Mitigation
  - Limit account re-use
    - Avoid re-using local admin password
    - Disable Guest and Administrator accounts
    - Limit who is a local administrator
  - Pass Attack
    - Utilize strong passwords
      - The longer the better (>14 characters)
      - Avoid using common words
      - I like long sentences
    - Privilege Access Management (PAM)
      - Check out/in sensitive accounts when needed
      - Automatically rotate passwords on check out and check in
      - Limits pass attacks as hash/password is strong and costantly rotated
  - Token Impersonation
    - Limit user/group token creation permissions
    - Account tiering
    - Local admin restriction
  - Kerberoasting
    - Strong Passwords
    - Least privilege

Buffer Overflow

- Spiking
- Fuzzing
- Finding the Offset
- Overwriting the EIP
- Finding Bad Characters
- Finding the Right Module
- Generating Shellcode / Getting Root

Brute Force Attacks

- Metasploit
- Hydra
- Crdential Stuffing
- Password Spraying
- https://github.com/danielmiessler/SecLists
- https://github.com/initstring/passphrase-wordlist

Credentials

- Metasploit
  - Kiwi
    - Password dumping
    - Password dumping in memory
    - Hash dumping
    - Golden Tickets
  - Mimikats
    - Password dumping
    - Password dumping in memory
    - Hash dumping
    - Golden Tickets
- Default Creds
  - Common Bad Password List
- Word List Generator
  - CEWL

Eternal Blue MS17_010

- Metasploit smb_ms17_010
- AutoBlue alternative to metasploit
- smbclient

Hashes Dumping / Cracking

- SAM
  - SAM
  - SECURITY
  - SYSTEM
- secretsdump
- John
- Hashcat
- crackmapexec
  - Pass-The-Hash
- psexec
  - Pass-The-Hash

Privilege Escalation

- Tokens
  - Stealing & Manipulation
    - Metasploit
    - Incognito
- WEB
  - SQL Injection
  - XXS

Post-Exploitation

Maintaining Access

Persistence Scripts

- run persistence -h
- exploit/windows/local/persistence
- exploit/windows/local/registry_persistence

Scheduled Tasks

- run schedulene
- run schtaskabuse

Add a user

- net user hacker password123 /add

Pivoting

Metasploit

- route print
- connect to target
  - lpconfig
  - arp -a
  - psexec
- run autoroute -s 169.254.0.0/24
- run autoroute -p
- poc
  - use auxiliary/scanner/portscan/tcp

proxychains

SSH Pivoting

Covering Tracks

Make the System/Network as it was when you entered it

- Remove executables, scripts, and added files
- Remove malware, rootkits, and added user accounts
- Set settings back to original configurations

Legal Documents and Report Writing

Common Legal Documents

Sales

- Mutual Non-Disclosure Agreement (NDA)
- Master Service Agreement (MSA)
  - Performance Objectives
  - Outline the Responsabilities
  - Rapid7 MSA example
    - https://www.rapid7.com/legal/msa/
- Statement of Work (SOW)
  - Activities
  - Deliverables
  - Timelines
  - Quotation
- Others: Sample Report, Recommendation Letters etc..

Before you test

- Rules of Engagement (ROE)
  - Will cover specifics of you testing
  - What we can and can't do
  - What we can and can't attack (IP addresses)
  - Common 'don'ts'
    - Denial of Service
      - unless that's a specific thing the client wants to test
    - Social Engineering
      - often set aside as its own assessment
  - You can not start your penetration test until the Rules of Engagement document is signed

Findings Report

- After you test

Assessment Overview (high level)

- It's Snapshot in time
  - We are not responsible for anything happening after
  - We are under a time limited engagement
  - We are targeting what we can in that period of time
- Timeframe
- Guidelines
- Phases of Pentest
  - Planning
  - Discovery
  - Attacking
  - Reporting

Assessments Components

- What we are attacking
- What type of penetration test it is

Findings Severity Ratings

Scope

- IPs
- Scope Exclusions
  - No Denial of Service attacks
- Client Allowances
  - Did the client had to assist us in any way ?

Executive Summary

- Intended for people with no technical background
  - C-level executive
  - CISO
  - CEO
- Quick summary about vulnerabilities you found, and what they could lead to
- Attack Summary
  - What you managed to do
    - Actions
  - Recommendations
- Security Strengths
  - We were scanning they identified and blocked us
  - Give them kudos where they need it
- Security Weaknesses
  - Missing Multi-Factor Authentication
  - Weak Password Policy
  - Unrestricted Logon Attempts
- Vulnerabilities by Impact
  - Identify weaknesses at a high level
  - No-technical people will understand
  - Charts

Technical Summary

- Share technical details
- Intended for technical people
- Chained exploit of attacks
  - Exploitation Proof of Concept
  - References
- Remediation
  - Who
  - Vector
  - Action
- Additional Reports and Scans (Informational)

'How to' video on writing a pentest report

- https://www.youtube.com/watch?v=EOoBAq6z4Zk

Sample Pentest Report

- https://github.com/hmaverickadams/TCM-Security-Sample-Pentest-Report

Legal Documentation for Physical Security Testing

- https://github.com/trustedsec/physical-docs

Wi-Fi

WPA2 PSK

Guest Network

- No password
- Separation of networks
- How well is the network segmented
- Reduced funtionalities
- Access Employs' things / IPs / servers

Open network

Hidden networks

Walk around

- Evaluate what networks are around
- Rogue Devices

WPS

Hacking Process

- Place wireless card in monitor mode
- Discover info about network
  - Channel
    - Channel 1, 6 and 11 are the most used (no overlap)
  - BSSID
  - SSID
- Select network and capture data
- Perform Deauth attack
  - Speed-up the process
- Capture WPA handshake

Attempt to crack the handshake

- Strength evaluation
- Many companies use something familiar to them
  - Company Name
    - Substitute 1 with i. 0 with O
  - Phone numbers
  - Street address
  - Create a wordlist from thei website
    - CEWL
  - WPA2 PSK
- Weak Passwords
  - rockyou.txt

WPA2 Enterprise

Web Applications

Enumeration

- Finding Subdomains
  - ./run.sh tesla.com
    - Assetfinder
  - Amass
- Find Alive Domains
  - HTTProbe
- Screenshot Websites
  - GoWitness
- Subdomain takeover
  - Subjack
- Scraping Wayback data
  - Waybackurls

OWASP Top Ten

SQL Injection

- Parameterized Statements
- Sanitized Input
- Blind SQL Injection

Broken Authentication

- Credential Stuffing
- Brute Forcing or other automated attacks
- Weak or well-known Passwords
- Weak or Ineffective Credential Recovery
- Weak forgot-password processes
  - knowledge-based answers
- Missing or Ineffective two-factor authentication
- Session ID exposed in URL
- Session Fixation
  - Does not rotate Session ID after successful login
  - Dows not properly invalidate Session IDs during logout or inactivity
  - User Sessions or Authentication Tokens

Sensitive Data Exposure

- Find all directories
  - dirbuster
- Response tab
  - navigate all directories
    - BurpSuite
- Search for 'key' 'keys' 'password' 'passw'
- Response Headers
  - HTTP Strict Transport Security (HSTS)
- nmap --script=ssl-enum-ciphers -p 443 tesla.com
  - nmap
- https://securityheaders.com

XML External Entities (XXE)

- Attacking Systems that parse XML Input
- Abuse SYSTEM entity and get malitious
  - dos, local file disclosure, remote code execution, and more

Broken Access Control

- User gets access to somewhere they shouldn't
- Are you able to bypass access ?
- Can you access admin areas or even other user areas from an account ?
- unauthenticated, authenticated, admin
- IDOR - Insecure Direct Object Reference

Security Misconfiguration

- Disclosure of Sensitive Information
  - Default Credentials
- Application should not throw errors
  - Stack Traces - Error Handling
- Unnecessary features
  - Left behind applications
  - Left behind directories
  - Default features not in use
- Out-of-date Software
- Unnecessary ports open, activated accounts
- File upload
  - Deprecated Interface

Cross-Site Scripting (XSS)

- Client-side
  - Reflected XSS
  - DOM XSS
- Server-side
  - Stored XSS
- Preventing XSS
  - Encoding
  - Filtering
  - Validating
  - Sanitization

Insecure Deserialization

- Serialization
- Deserialization
- ysoserial

Using Components with Known Vulnerabilities

- Software is vulnerable, unsuported, or out of date
- No frequent scan for vulnerabilities
- No Patching, no fix, no update

Insufficient Logging & Monitoring

- Have Logs, Auditable Events
- Track anyone logging into the application
- Track failed login attempts
- Monitor if anyine is attacking your application
- Serialization