

module-5

Penetration Testing, Incident Response and Forensics

21/09/2022

(W1)

⇒ Penetration testing is security testing in which **attackers** mimic real-world attacks to identify methods for circumventing the security features of an application, system or network.

- important to take vulnerability scans (overcome an obstacle)
- to ensure cyber controls are working

↳ Approaches

- Internal vs External (hacking)
- web and mobile app assessments
- Social Engineering //
- Wireless Network, Embedded & IoT
- ICS penetration

↳ Industry control systems: outdated passwords, OS, etc.
soc eng. etc (oil, gas, electric industries)

↳ General methodology

planning > Discovery > Attack > Report

↳ Planning

- set Objectives
- Establish boundaries
- Informing need-to-know employees

↳ Discovery

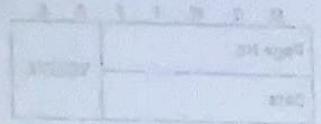
- Vulnerability Analysis (Identify OS & major software apps and match them with info or known vulnerabilities in vulnerability databases)

↳ Dorks : google dorks

- admin login pages
- usernames and names
- vulnerable entities
- sensitive documents
- Govt/military data
- Email list
- Bank account details and more

↳ passive vs active

- monitoring employees
- listening to network traffic
- Network mapping
- port mapping
- password cracking



M	T	W	T	F	S	S
Page No.:	YOUVA					
Date:						

↳ Scanning tools

- network mapper (en: NMAP)
- network Analyzer & profiler (en: Wireshark)
- password crackers (en: John the Ripper)
- Hacking tools (en: Metasploit)

↳ Passive - Online

- Wire Sniffing (data packet capture across network)
- Man in the Middle. (hijacking session)
- Replay Attack (data retransmission or delay)

↳ Active - Online

- password Guessing (Brute force) Attack
- Trojan/Spyware/Keyloggers (collucts data from session)
- Hash Injection (Authenticate to a remote server or service by using underlying NTLM or LANMan hash of a user's password)

[getting password file from server and decode it]

older version
of NTLM

(New Technology)
LAN Manager -
Suite of Microsoft -
provides authentication,
integrity and confidentiality
to users)

- phishing (malicious link)

↳ Offline Attacks

- pre-computed Hashes
- Distributed Network Attack (DNA)
- Rainbow Attack.

↳ Technique Discovery

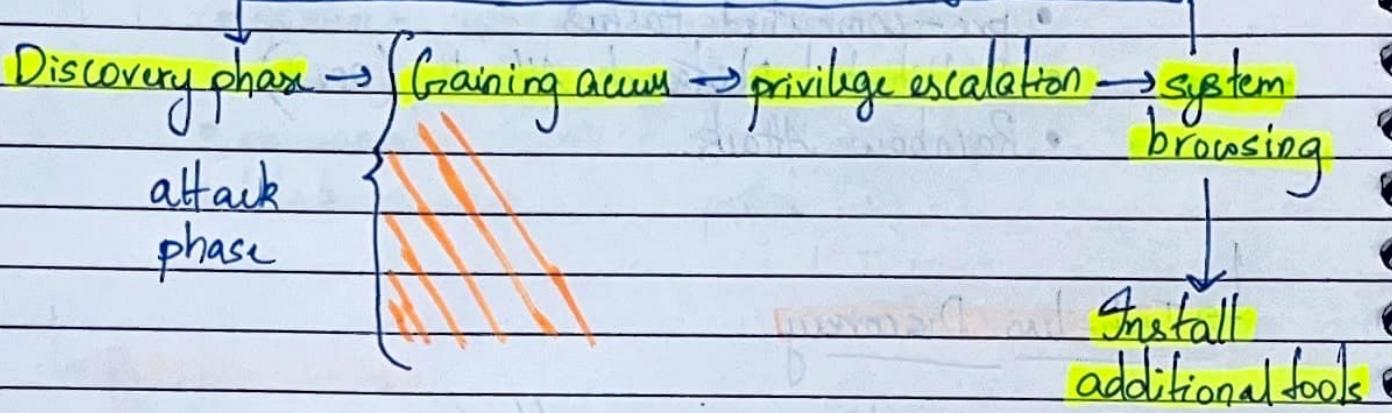
- Social Engineering !!
- Shoulder surfing (use someone to physically see if the employee is inputting their password)
- Dumpster diving (not illegal to check trash of a company)

⇒ Notable website: securitytrails.com/blog/google-hacking-techniques
 - for google docks and more

: subscription.packthub.com/search-library

Attack phase

Additional discovery



Exploited vulnerabilities

- Misconfiguration
- Kernel flaws
- Insufficient Input Validations
- Symbolic links (file point to another file)
- File descriptor attacks (numbers used to keep track of file streams)
- Race conditions

program or process entered privilege mode

- Buffer overflows (not checking input for appropriate length)
- Incorrect file or directory permissions

Resources

Penetration testing executing standard

- ibm.biz/PTES-exploit
- ibm.biz/owasp-pentest

Reporting

- Executive Summary (who, what, when, where of testing)

- Background
- Overall posture
- Risk Ranking
- General findings
- Recommendations
- Roadmap

high level detail

↳ Technical Review (Why and how of testing)

- Introduction (person involved, contact info, clients involved, etc.)
- Scope
- Vulnerability Assessment
- Vulnerability Confirmation
- Post Exploitation
- Risk/Exposure

penetration Tools for pentesting

- Kali Linux
- ~~www~~ nmap.org !! (for CEH)
- JT Ripper
- ~~jtr~~: metasploit
- wireshark

- HTB (practice) - lannwalkthrough

} @ ibm.biz / <tool-name>

(W2)

⇒ Incident Response

Event: something not with respect to normal behaviour of system or change to normal behaviour

Incident: Event that has a negative impact on the IT system or organization

↳ IR Team models

- Central (Single response team)
- Distributed (per site or per office)
- Coordinating

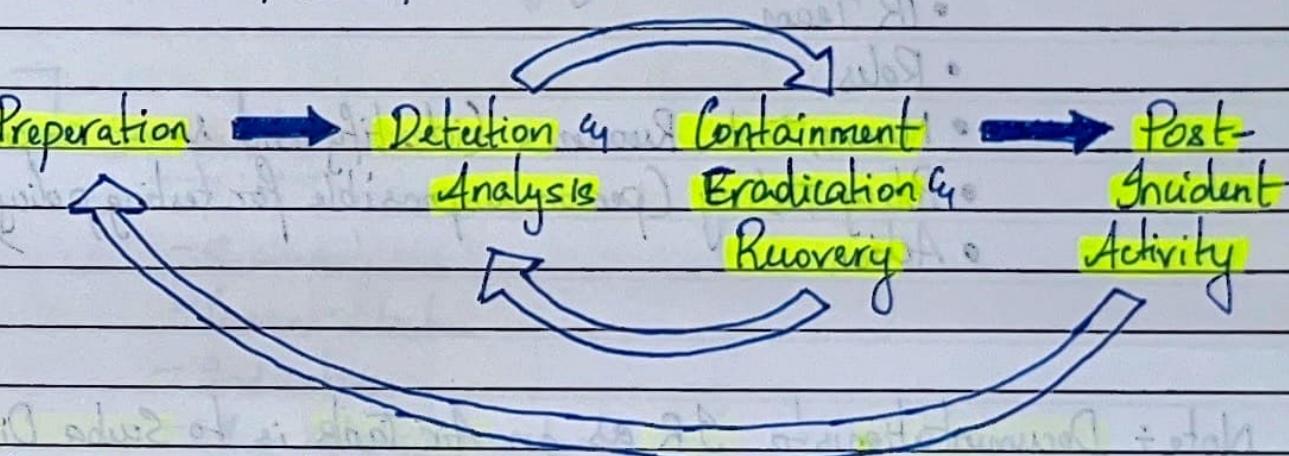
→ relationship with other teams (areas to look for)

- management
- Information Assurance
- IT Support
- Legal
- Public Affairs and media Relations
- Human Resources
- Business Continuity planning
- Physical Security and facilities management.

↳ Common Attack Vectors

- External/Removable media
- Attrition (sustained or persistent attack to weaken defense)
- Web
- Email
- Impersonation
- Loss or theft of equipment

↳ Incident Response phases (NIST framework)



Note: Sans Equivalent

- preparation
- identification
- Containment
- Eradication
- Recovery
- Lessons learned.



→ the best offence

- Risk Assessment
- Host Security
- Network Security
- Malware Prevention
- User awareness and training

} part of prep

→ Preparation

- Incident Response Policy

- IR Team
- Roles
- Means, Tools, Resources (identify and recover compromised data)
- Policy Testing (person responsible for testing policy)
- Action

Note: Documentation is to GR as an Air Tank is to Suba Diving

→ Detection and Analysis

- Precursor: sign that an incident may occur in the future. (web server log entries showing usage of vuln scanner)

- Indicator: sign that an incident may have occurred or maybe occurring now.

(Antivirus software alerts
malware infection)

↳ Monitoring systems

- IDS vs IPS

- DLP

- Data loss prevention - insures that sensitive data isn't lost, misused or accessed by unauthorized users.

- SIEM

- analysis of event and log data in real time with Security Information Management (SIM)

↳ Documentation

- Summary

- Current status

- Indicators

- Other related incidents

- Actions taken by incident handlers

- Chain of custody

- Impact assessment

- Contact info

- Evidence gathered

- Next steps to be taken

↳ Types of impact (functional)

- none - no effect to org's service to users
- low - minimal effect; lost efficiency
- Medium - lost ability to provide a critical service to a subset of system users
- high - no longer able to provide critical service to users

(Information)

- none - no info was infiltrated, changed or deleted
- primary Breach - sensitive PII of users caused or infiltrated
- proprietary Breach - undclassified proprietary information, such as protected critical infrastructure information (PCII) was caused or infiltrated.
- Integrity loss - Sensitive or proprietary info was changed or deleted.

(Recoverability effort)

- Regular - Time to recovery is predictable with existing resources
- Supplemented - "with additional resources"
- Extended - Time to recovery is unpredictable; additional resources and outside help are needed.
- Not Recoverable - Recovery from incident isn't possible.

(sensitive data exfiltrated and posted publicly);
Launch investigation.

↳ Containment, Eradication and Recovery

- ↳ ①
 - potential damage to theft and resources
 - Need for evidence preservation
 - Service Availability
 - Time and resources needed to implement strategy
 - Duration of Solution

- forensics in IR

- capture backup image of system as-is
- gather evidence
- follow chain of custody protocol

- ↳ ②
 - deleting malware
 - disabling breached user account
 - identifying and mitigating all vulnerabilities exploited

- ↳ ③
 - Recovery using clean backups
 - replacing compromised files with clean versions
 - installing patches
 - changing passwords
 - tightening network parameter (firewall rulesets, router ACLs)

- high level testing, monitoring deployed.

↳ Post incident

- lessons learned

- Utilizing data collected (reviewing response times, system impacted)
- Evidence Retention
- Documentation

⇒ Incident Response Demo

↳ Common threats

- Software Attacks
- Data theft
- Information Sabotage
- Theft of equipment

↳ Attack Vectors

→ website using hosting malicious content.

• Gradar (collects system event info from drivers or apps on our network including log info from OS)

Counter mechanism

- McAfee endpoint Orchestrator
- Next generation firewall

↳ IR process

- preparation (contact shareholders, teams involved)
- Detection & analysis
- Containment, eradication & Recovery
- Post-Incident Activity

↳ Using Radar we see multiple information like

- Description

- Log ID

- Offense type

- Offense Source

- Magnitude

- Source IPs

- Destination IPs

- Users

- Log Source

- Events

- flows

- Clicking on any of the offenses, brings us to the summary page giving us different details, including Top 5 Source IPs, dest IPs, log sources.

- Main thing to notice is top 5 Annotations.

- Going through the events to get more details (DNS queries, risk meter, threat, etc.)

- To check it out, go to events, click on Event/flow count.

- Then we note down our information to proceed to step 2 of Incident Response.

- In an Incident Response form, we have :

- Type of ~~Tempalte~~ Incident : DNS query known
- Detection Source : CRadar
- Environment : LAB
- Hostname : LABPC02
- IP Address : 192.168.6.12 (affected one)
- Webserver : No. (system is a workstation)
- Public IP: 8.8.8.8 (google's DNS server)

#

- start recording what time we found the information

- timestamps
- 1302 - webdut.co (malicious DNS query discovered)
 - 1303 - workstation 192.168.4.6 LABPC02 (found out that DNS query came from our workstation)
 - 1307 - Submit ticket to network team to disable switch port.
 - 1309 - Kick off McAfee ENS full scan
 - 1313 - Reviewed McAfee ENS full scan results, 0 files were detected
 - 1314 - Recommend system to be reimaged
 - 1500 - Submit ticket to have system reimaged

- After doing all that, we can send the information up and allow them to process it and archive it.
- Now that the investigation is done, we close the incident
- Reason for closing - closed; testing
- Note - copy paste the incident response form.
- If we see any false positives, even a local to local DNS attack, it might just be an user working with server to develop application using an API.
- So multiple 443 is expected (session open, closes) for that system from workstation
- So we close the offense, stating reason: Non-issue
- Note: The rule threshold has been increased.
- Reduces the amount of false positives.

↳ So to summarize IR process

- Step 1 was preparation
 - know what to look for
 - know what assets we're monitoring
 - Events to trigger on
 - people to contact in case of incident

• Step 2 was Detection and Analysis

- gather information
- Research events that triggered alert
- determine if event is real

• Step 3 was Containment, Eradication and recovery

- disconnect from network
- contact team for those network connections
- look for other threats
- look for areas that it might have spread to
- get system back in state
- give direction to Seimage system
- logs

• Step 4 was post incident Activity

- after action report to be made
- include mistakes committed
- anything that could have been done better
- anything to increase efficiency.

⇒ free and open source IR tools

- Cynet 360
- GRR Rapid Response
- Alien Vault
- Cyphon
- Volatility
- Sans Investigative forensics Toolkit (SIFT) Workstation
- TheHive Project

↳ SOAR → combining IR, automation and threat intelligence.

- Security Orchestration Automation and Response
- capabilities include:

- **Orchestration**: ability to connect to and integrate various tools
- **Automation**: ability to collect data automatically and enrich events.
- **Response**: ability to allow analysts to manage, collaborate, and share data regarding incidents for better outcomes

⇒ QRadar lab Using IBM QRadar SIEM (Check files for instruction manual)

→ Incident Response team:

- Incident Handler Communication and facilities
- Incident Analysis Resources (portlist, Docs, Crypto hashes)
- Incident Analysis Hardware and Software

⇒ Forensics

(N3)

22/09/2022

↳ Digital forensics is application of science to the collection, identification, examination and analysis of data while preserving integrity of data and maintaining direct chain of custody.

↳ Types of data

- desktop Computers (CDs, DVDs)
- Servers (internal, external drives, application usage)
- Network Storage devices (network Activity)
- devices laptop (portable digital devices)

↳ need

- Incident handling
- log monitoring
- Data recovery
- Data acquisition
- operational troubleshooting
- Regulatory Compliance/ due diligence

↳ Forensic Process

- Collection ①
- Examination ②
- Analysis ③
- Reporting ④

↳ ①

- more Types of data

- Externally owned property
- Computer at home office
- Alternate Sources of data
- logs
- Keystroke monitoring.

- Steps to collect data

- Develop a plan to acquire the data
- Acquire data
- Verify integrity of data

- Observe Chain of Custody

- Keep log of every person who handled evidence.
- Store evidence in secure location.

- copy of evidence to be made
- verify integrity of copy vs original.

L → ②

- Bypassing Controls (OS and apps may have data compression, encryption, etc)
 - Sea of data
 - Tools
- Basically examining data

L → ③

- include identifying people, places items and events
- Putting pieces of data
- coordination between multiple sources of data is crucial

L → ④

- report needs to detail basis of your conclusions
- Detail every test conducted, methods and tools used and result

Report Composition

- Overview/Care Summary
- Forensic Acquisition & Examination Preparation
- Findings & Report (Analysis)
- Conclusions

- Sans Institute best practice (Findings & Analysis)

- Take ss
- Bookmark evidence via forensic application of choice
- Use built in logging/reporting options within forensic tool
- highlight and exporting data items into .csv or .txt files
- Use digital audio recorder vs handwritten notes when necessary.

↳ Data files

- Windows

- FAT

(Circular)
• 12

• 16

• 32

• NTFS

• ReFS

- Unix

- EXT - 2, 3, 4

• ReiserFS

• XFS

• JFS

• Btrfs

- macOS

- HFS +

• APFS

- What not there

- **Deleted files** : not really deleted, info pointing to file location is deleted
- **Slack Space** : entire file allocation unit size reserved for file even if it doesn't need that much space
- **Free space** : media ie not allocated

- MAC Data

- Modification Time
- Access Time
- Created Time

- Collecting Backup

- Logical Backup : copies files and directories of logical volume ; doesn't capture other data present on media (deleted files or residual data)
 - : Resource Intensive : can be used on live system
- Imaging : Generates bit-for-bit copy of original media (including free and slack space)
 - : if evidence or analysis is needed, it should be worked on this duplicate.
 - : can't be used on live system

- Tools for Techniques

- File viewers
- Uncompressing files
- GUI for Data Structures
- Identifying known files
- String Searches and pattern matches
- Metadata

→ OS data exists in volatile and non-volatile state

data lost after
system powered
down. enⁿ network
connections.

- slack space
- open files
- running processes
- login sessions
- OS Time
- memory contents
- network configurations

exists even after system is
powered down

- Config files
- logs
- Application files
- Data files
- Swap files
- Dump files
- Hibernation files
- Temporary files

Collecting non
volatile data

- consider
power-down
options

→ Logs

- In case of network hack:

- collect logs of all network devices lying in
the route of hacked device and perimeter
router (ISP Router)

- In case of an unauthorized access:

- Save web server logs, application server logs, application logs, router or switch logs, firewall logs, database logs, IDS logs, etc.

- In case of a Trojan / Virus / Worm Attack

- Save antivirus logs apart from event logs.

↳ Windows

- Analyzing locations like

- Recycle bin
- Registry
- Thumbs.db (Folder representing thumbnails of files)
- browser History
- print spoofing

↳ Mac OS

- Unix based OS containing Mach 3 micro kernel and FreeBSD based subsystem.

- Put the Mac into target disk mode to create a forensic duplicate of hard disk. with firewall cable between 2 pc's

↳ Linux

- Analyze Location like:

• /etc [% SystemRoot %] /System32/config]

- contains system config directory holding separate config files for each application

• /var/log

- contains application and security logs.
- kept for 4-5 weeks

• /home/\$USER

- user data and configuration info

• /etc/passwd

- contains user account information.

↳ Application data

- config settings
- Authentication
- logs
- data
- supporting files (Docs, links, graphics)
- App Architecture (local, client/server, peer-to-peer)

↳ Types of applications

- Email
- Web Usage (host-cookies, history, fav websites; server-TS, IPs, ...)
- Interactive Communications (group chat, etc) (Type of request)
- Data Concealment tools
- Security Applications
- Document Usage
- file sharing.

protocol : IRC → Internet Relay Chat

→ Network Data

→ TCP/IP

- Application layer : sends and receives data for particular apps, such as DNS, HTTP, SMTP

(packet)

- Transport layer : provides connection-oriented or connection-less services for transporting application layer services between networks.

-TCP/UDP

(datagram)

- Network layer (IP layer) : Routes packets across networks.

IP - fundamental network protocol for TCP/IP.
other protocols - ICMP, IGMP.

(frame)

- Hardware layer (Data link layer) : handles communications on physical network components.
en : Ethernet protocol.

↳ Sources of network data

- firewalls and Routers (may log every packet)
- packet Sniffers & protocol Analyzers
- Intrusion detection system
- Remote Access

- Network forensic Analysis Tools
- Security events management Software

↳ Data Value

- IDS Software
- SEM Software
- NFAT Software (network forensic Analysis tool)
- Firewalls, routers, proxy servers, & RAS
- DHCP Servers (log each IP address assignment to associated MAC address)
- packet sniffers !!
- Network Monitoring
- ISP Records

↳ Attacker Identification

- Contact IP address owner
- Send network traffic (ping IP) (not recommended for org)
- Application Content (Data packet could contain attacker identity info)
- ask ISP Assistance
- History of IP address (trends of suspicious activity)

(W4)

⇒ Introduction to Scripting

23/09/2022

↳ IBM's Job Control language (JCL) → first scripting language

↳ Script Usage

- automation
- Image rollbacks
- Validation
- Backup
- Testing

↳ Python

- open source
- portable
- high level

↳ Data Structures

• Tuple → immutable sequence of objects → (), (1, 2, 3), ('python', 3)

• List → mutable sequence of objects → [], [1, 2, 3], ['hello', 'world']

• set → set/frozenset → unordered set of unique items

→ {1, 2, 3}, {"world", 'hello'}

→ frozenset → immutable ; set → mutable

• Dictionary → items composed of key value pair → {}, {'name': 'Egio', 'surname': 'Meclootti'}

↳ Digital forensics using python programming

- web server fingerprinting
- simulation of Attacks
- Port Scanning
- Website Cloning
- load generation and testing of website.
- Creating IDS and IPS
- Wireless network Scanning
- Transmission of traffic in network
- Accessing mail Servers, etc

• website : <https://opensourcetech.com/2016/11/python-programming-digital-forensics-security-analysis/>

↳ Graphic and Visualization functions in python

- Seaborn
- Matplotlib

↳ Scientific Computing functions

- Numpy
- Pandas

cochlear

卷之三

front has black bands with orange highlights on the sides. The back has
orange or yellowish-green streaks with black spots.

(cont'd) discussed behaviour research based on the
behaviour of the old people in the community.
Community
Involvement in local clubs and other social groups
is known and makes better communication easier.
Community participation is
also helpful in maintaining their independence.
It is also helpful in maintaining their independence.

• golM upskirt2 unparallel straight
• BL — — — — —
around front back, front back, front back - (stab elongate) stitch
dark shading breaking away
major hollowed seam - (the bar or stab sing) wing
minor hollowed seam - (small bar stitching bar) rope
minor hollowed seam - (small bar stitching bar) rope