Digital Forensics in Computer Crime Investigation

Practical guidance for investigators navigating the complex landscape of cybercrime

Course Objectives

01

Identify Common Computer Crimes

Recognize patterns and characteristics of major cybercrime categories

02

Understand Forensic Approaches

Learn how different crimes require tailored investigative strategies

03

Apply Appropriate Strategies

Match forensic techniques to specific criminal activities

Computer Crime's Impact on Forensics

Three Roles of Computers in Crime

Target

System being attacked

Example: Hacking attempt

Instrument

Tool used to commit crime

Example: Breaking into another system

Evidence Repository

Storage of crime-related data

Example: Deleted files, logs

Modern Investigation Challenges

Data Volume Crisis

- Massive storage capacities
- Manual searches impractical
- Need automated tools

Law enforcement requires **quick information retrieval** for effective investigations

Computer Crime Categories

White-Collar Crimes

Fraud, identity theft, financial crimes

Violent Crimes

Cyberstalking, harassment, threats

National Security

Terrorism, espionage, counterintelligence

Key Forensic Principle

Crime type determines evidence type

Identity theft → Email evidence

Hacking → Firewall logs

Fraud → Financial records

Identity Theft

Identity Theft Defined

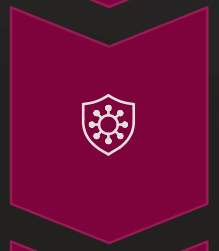
Wrongful obtaining and using another person's personal data through **fraud or deception**

Usually for financial gain or obtaining official documents

Common Methods

Phishing

Deceptive emails from "trusted" sources



Spyware

Software monitoring computer activity

Discarded Information

Dumpster diving for personal documents

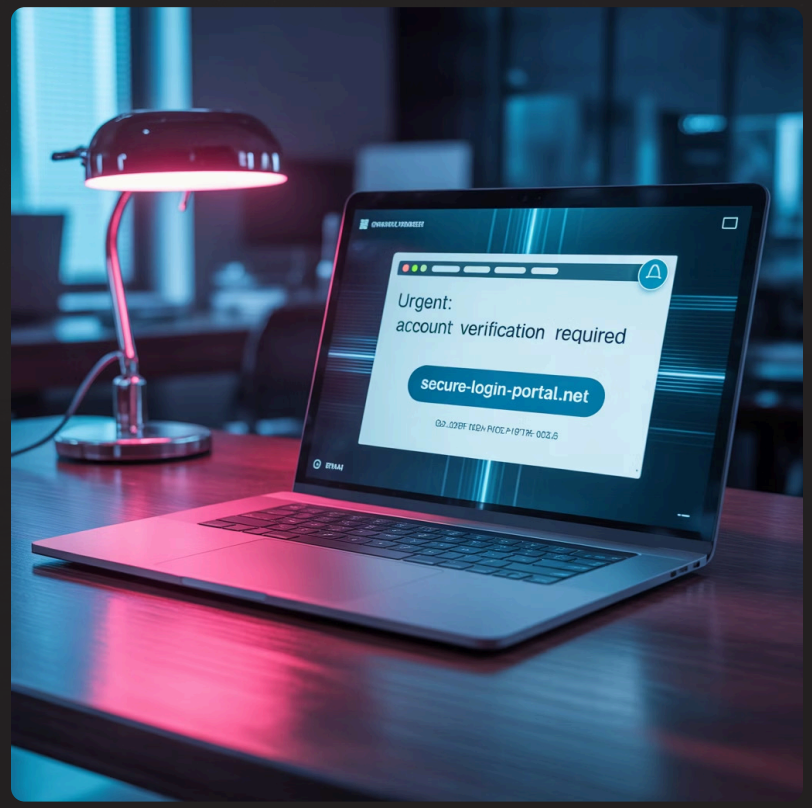
Phishing Attacks

Standard Phishing

- Mass emails to random targets
- Generic "bank" or "IRS" messages
- Malicious links to fake sites

Spear Phishing

- Highly targeted attacks
- Extensive victim research
- Personalized, believable content



Spyware: Legal vs. Criminal Use

Legal Uses

- Parents monitoring children
- Employers on company systems
- Law enforcement with warrants

Criminal Uses

- Trojan horse delivery
- Deceptive email attachments
- Unauthorized monitoring

⚠ **80%** of internet-connected computers believed infected with spyware

Identity Theft Forensics

01

Check for Spyware

Primary investigative step on victim's computer

02

Trace Communications

Email attachments, server connections leave forensic traces

03

Examine Digital History

Email records, web browsing, suspicious websites

Hacking

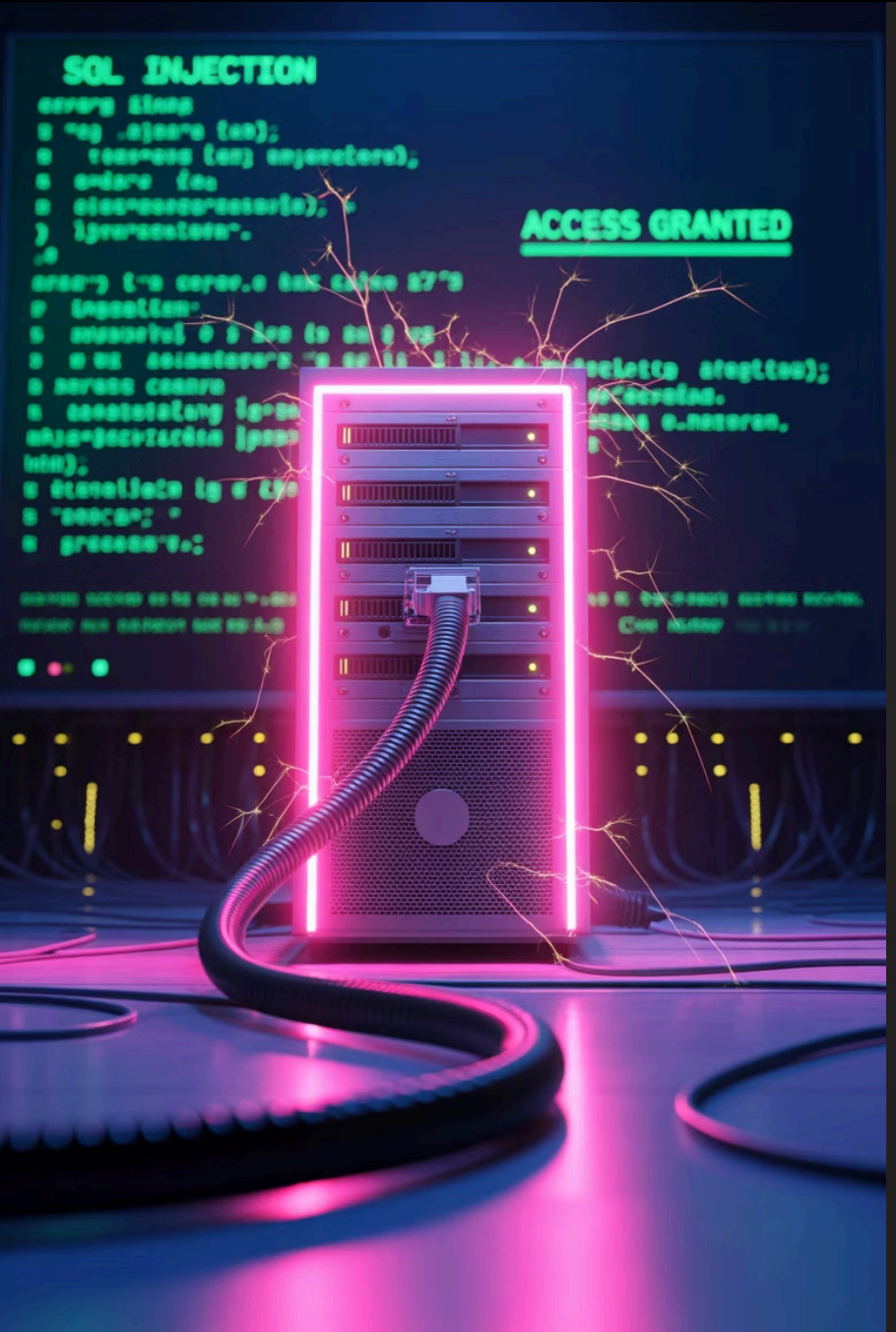
Hacking Defined

Hacking Community

Experimenting with systems to understand rules and fix flaws

Law Enforcement Context

Circumventing system security



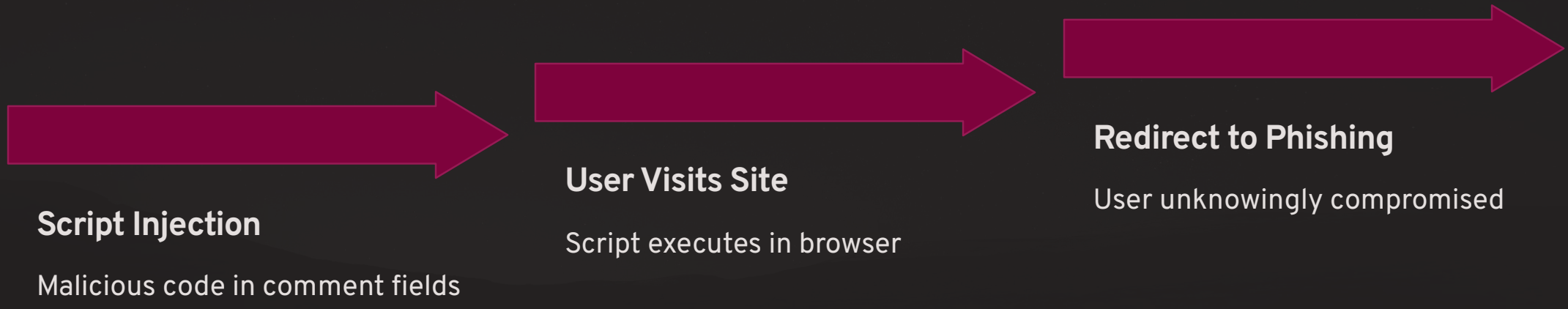
SQL Injection Attacks

Exploiting web application vulnerabilities through malicious database queries

```
Normal: SELECT * FROM Users WHERE name='john'
Attack: SELECT * FROM Users WHERE name='' OR 1=1 --'
```

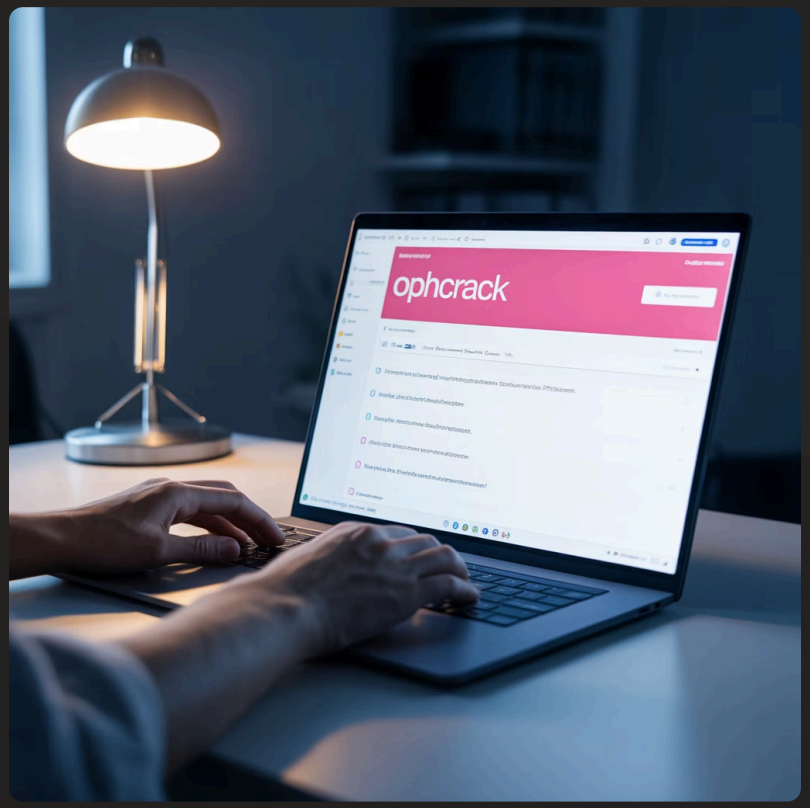
Result: **Bypasses authentication** - gains unauthorized database access

Cross-Site Scripting (XSS)



Investigate by searching server logs for HTTP 300-range redirects

Ophcrack: Physical Access Threat



Requirements

- 10 minutes physical access
- Boot from CD/USB
- Access to BIOS settings

Method

Uses rainbow tables to match password hashes from Windows SAM file

Ophcrack Forensic Detection

Unexpected Reboot

System restart followed by unusual account login

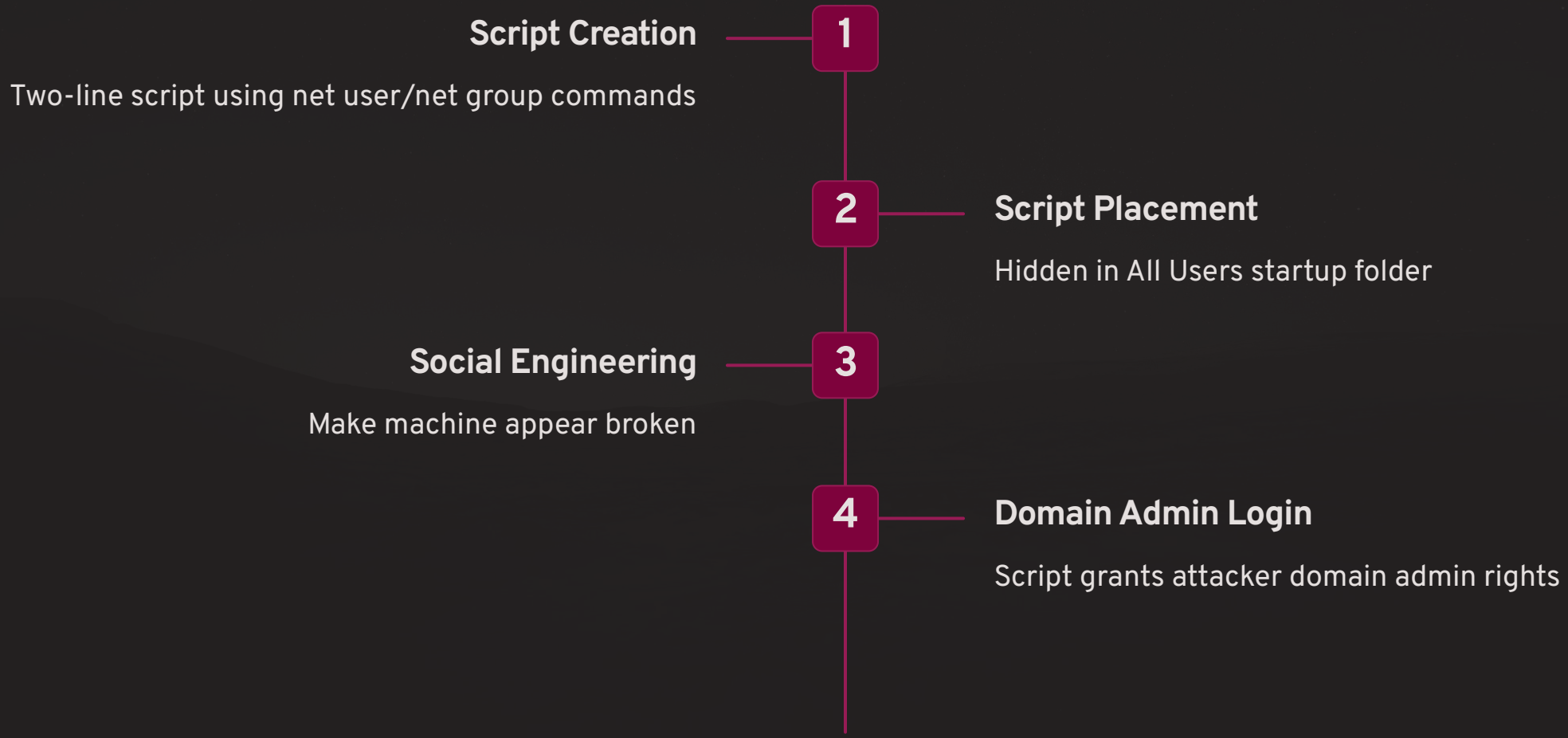
Physical Evidence

Security cameras, fingerprints crucial

Account Anomalies

Administrator login when user not present

Advanced Attack: Tricking Tech Support



Cyberstalking

Cyberstalking Defined

> Using electronic communications to stalk another person through **repeated harassing or threatening behavior**

Often includes credible threats against victim or family

Three Key Assessment Criteria

Is it possible?

Threat credibility assessment

Anonymous vs. specific details

How frequent?

Pattern of repeated behavior

Not isolated angry remarks

How serious?

Specific vs. vague threats

Shows premeditation

Notable Cyberstalking Cases

1

Cody Henson (2019)

NC State Rep threatened ex-wife and family

2

Joseph Medico (2010)

70-year-old stalked 16-year-old girl

3

California First (1999)

Security guard terrorized woman via internet impersonation

More Complex Cases

Samuel Hughes (2020)

Threatened 10+ people with rape/murder

San Diego Graduate (2019)

Hundreds of violent emails to 5 students over one year

Cyberstalking Forensics

Computer as **tool** targeting victims

→ **Start with Communications**

Trace emails and text messages

→ **Examine Suspect Devices**

Obsessive behavior = retained evidence

→ **Low Tech Skills**

Most stalkers not tech-savvy

Internet Fraud

Fraud Categories

Investment Offers	Data Piracy
Pump & dump schemes	Illegal IP distribution
Nigerian prince scams	Warez sites

Pump & Dump Schemes

Spread False Rumors

Via fake blogs, emails

Stock Price Inflates

Artificial demand created

Sell at Peak

Fraudster profits

Investors Lose

Devalued stock remains

Fraud Investigation Strategy

Investment Fraud

- Trace email communications
- Investigate domain registration
- Follow money trail

Data Piracy

- WHOIS domain searches
- Trace website ownership
- Track distribution networks

Non-Access Crimes

Denial of Service (DoS)

Preventing legitimate users from accessing computer resources

> **Cyber vandalism** - making systems unusable rather than breaking in

Common DoS Attack Types

SYN Flood

Exploits TCP handshake process

Smurf Attack

ICMP flood via IP spoofing

DHCP Starvation

Exhausts IP address pool

Virus Categories & Examples

Recent Notable Viruses

- **WannaCry (2017):** Ransomware exploiting unpatched systems
- **Emotnet (2019):** Fake document botnet
- **Ryuk (2019+):** Government-targeting ransomware

Investigation tip: Document behavior, find commonalities among infected systems

Key Takeaways

Crime-Specific Evidence

Each crime type yields different forensic traces

Tailored Approaches

Investigation methods must match crime characteristics

Technical Knowledge

Understanding attack methods enables effective forensics

Successful digital forensics requires matching investigative techniques to specific criminal activities