Threats and Testing

Azqa Nadeem
PhD candidate and lecturer
Cybersecurity group
Delft University of Technology

TU Delft

Today…

Part I

- Threat actors

Part II

- Types of cyber threats

Part III

- Penetration testing
- Incident response

TU Delft

This lecture: Prepare for the worst | Plan for failure

Black-hat (criminal) hacking discovers weaknesses in a computer software or computer network and exploits it for profit, protest, sabotage terrorism, or cyber war.

- Assume that you will get hacked at some point
- Have a plan for when (not if!) you get hacked
- Goal: Get visibility – Get situational awareness

Most hacks can be detected if organizations have sufficient situational awareness

TU Delft

Anatomy of a cyber attack

- Five main steps: the 5 P’s
- **P**robe
- **P**enetrate
- **P**ersist
- **P**ropagate
- **P**aralyze

TU Delft

Probe

Gather intelligence (Reconnaissance) about the target

- From network, socials, web services
- Goal: discover vulnerable services or people + identify deployed security mechanisms
- Scanning (ports, applications)
- Harvesting emails (bugs or links)

Exercise – OSINT

- Our target: TU Delft
- Who will you contact?
- What are you after?
- Who will you impersonate?
- What will be the content of the communication?

Penetrate

Get access to the identified vulnerable systems/people

- Brute-force authentication services (e.g., Metasploit, John the Ripper)
- Exploiting programming errors (e.g., buffer overflows)
- Exploiting application logic flaws (e.g., directory traversal)
- System configuration errors (exposing sensitive information)
- User input validation errors (e.g., SQLi, XSS)
- (Spear) Phishing (harvesting user credentials)
- Physical attacks (e.g., infected USB sticks)

Persist

Once a vulnerable host is exploited, it is time to establish a foot-hold

- Dump administrator passwords
- Establish communication channels with command and control (C&C) server
- Create backdoor accounts
- Create backdoor communication channels (persisting malware)
- Delete logs (covering tracks)

Propagate

Attempt to move laterally to other devices in the network

- Rerun of probing, penetrating and persisting

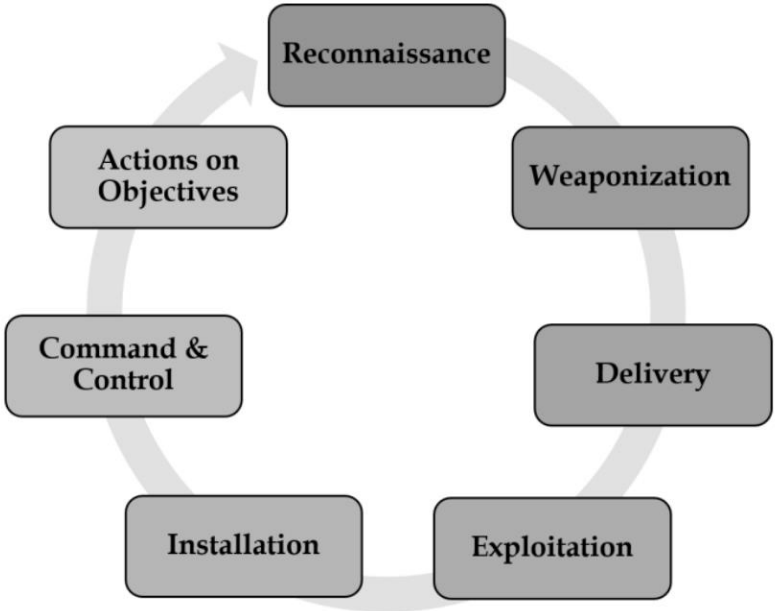
Paralyze

Complete the true objective of the attack

- Disclosure - removing files and information
- Disruption - stop or exhaust resources
- Distortion - encrypt valuable files
- Destruction - wiping logs or files
- Delivery - malware or backdoor

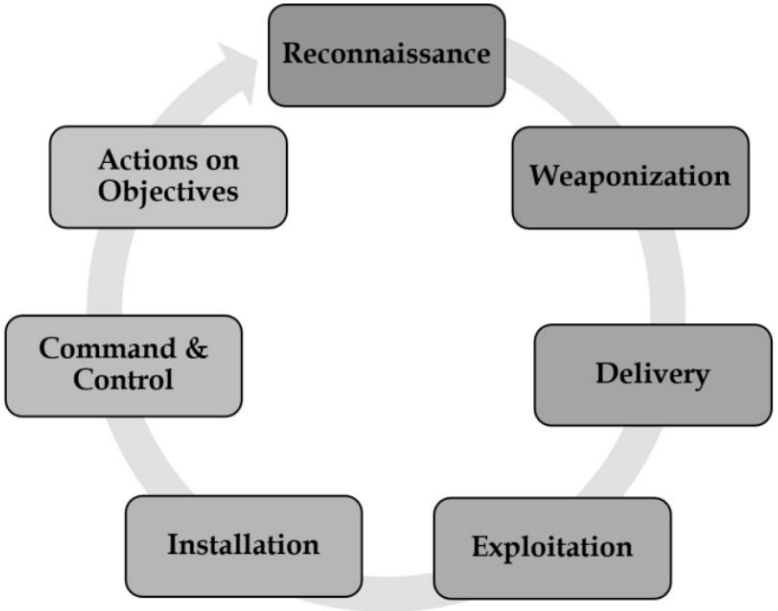
Exercise – The 5 P's and Kill Chain

- Probe
- Penetrate
- Persist
- Propagate
- Paralyze



Exercise – The 5 P's and Kill Chain

- Probe (Reconnaissance)
- Penetrate (Weaponization, Delivery, Exploitation)
- Persist (Exploitation, Installation)
- Propagate (Installation, Command & Control)
- Paralyze (Actions on Objectives)



Threat actors

- *A threat actor is defined as an actor who (intends to) adversely affect the Confidentiality, Integrity, and Availability of information and information systems*

- Threat actor dimensions
  - Capability, Opportunity, Intent (COI) model
  - Target, Expertise, Resources, Organization, Motivation

- Risk of an attack = Likelihood of an attack * Impact of the attack
- Likelihood = Opportunity, Intent, Informational value
- Impact = Cost of losses (Very difficult to estimate)

Threat actors

- Extortionists
  - Holding service or documents hostage in exchange for money
- Information brokers
  - Trading stolen sensitive documents
- Crime facilitators
  - Provide technical support to other attackers for renting botnets or exploit kits
- Digital robbers
  - Attacking financial institutions to steal money
- Scammers and fraudsters
  - Employing social engineering in their attacks, e.g., impersonation
- Crackers
  - Showing-off their capabilities to hack into digital services

Threat actors

- Insiders
  - Attackers that work inside an organization
- Hacktivists
  - Ideologically-driven hackers targeting critical infrastructure or enterprises
- Terrorists
  - Ideologically-driven hackers targeting and violently acting against critical infrastructure or enterprises
- State actors
  - Stealthy backdoor attacks used by government bodies to obtain strategic information
- State-sponsored networks
  - State-affiliated groups organized in networks

Threat actors

	Threat actor type	extortionists	information brokers	crime facilitators	digital robbers	scammers and fraudsters	crackers	insiders	terrorists	hacktivists	state actors	state-sponsored networks
Target	Citizens	■	■	■	■	■						
	Enterprises	■	■	■	■	■	■	■	■	■	■	■
	Public Sector	■	■	■		■	■	■	■	■	■	■
	Critical Infrastructure(s)						■		■	■	■	■
Expertise	Low	■				■	■			■		
	Medium	■	■	■	■	■	■	■		■	■	■
	High		■	■	■			■	■		■	■
Resources	Low	■	■			■	■	■		■		
	Medium	■	■	■	■	■			■	■	■	■
	High				■				■		■	■
Organization	Individual					■	■	■		■		
	Hierarchy	■	■						■		■	
	Market	■	■	■		■			■			
	Network	■	■	■	■	■	■			■		■
	Collective						■			■		
Motivation	Personal	■					■	■				
	Economic	■	■	■	■	■		■				
	Ideological							■	■	■		
	Geo-political										■	■

TU Delft

Exercise - Threat actor examples

- Extortionists
- Information brokers
- Crime facilitators
- Digital robbers
- Scammers and fraudsters
- Crackers
- Insiders
- Hacktivists
- Terrorists
- State actors
- State-sponsored networks

End of Part I
Questions?

TU Delft

Cyber attacks

Vector of Moving Forward GETTY

More Treachery And Risk Ahead As Attack Surface And Hacker Capabilities Grow

- Reported by Deloitte

- Nearly half of the executives expect attacks on accounting and financial services
- Open source code vulnerabilities in 84% code bases
- Microsoft, DocuSign, Google impersonated by attackers for phishing
- Fake CEO emails led to business email compromise in 78% cases
- Identity theft on the rise
- Extortion by ransomware
- Poor security of Internet connected devices (IoT , OT)

https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/

Malware

“Malicious software intentionally designed to cause disruption or destruction of a targeted network, services, hosts”

- Types based on objectives
  - Viruses – Software that replicates itself
  - Worms – Software that propagates to other systems
  - Trojan horses – Software that misleads users of its true intent
  - Ransomware – Software that encrypts user data and demands ransom
  - Wiper – Software that deletes user data
  - Keylogger – Software that logs keystrokes and shares with the attacker
  - Rogue security software – Software that misleads a user into installing an anti-virus which in turn installs malware

Malware (More terminology)

- Droppers – Trojans that deliver malware payload (stealthy and light payload)
- Drive-by-download – Access website that unintentionally (or intentionally) downloads a malicious payload
- Rootkit – Malware that enables admin-level access to a host while hiding from users
- Remote Access Trojan (RAT) – Rootkit that enables full admin privileges and remote access to a host
- Backdoor – Malware that enables unauthorized access to a host without the user knowing

Greyware

- Potentially unwanted applications (PUA)
  - E.g., applications that are bundled with wanted software
- Spyware – Software that gathers information about entities
- Adware – Software that shows advertisements to generate revenue for the software developer

Exercise – The TA505 hack

- Maastricht University had a ransomware attack on December 23, 2019
- Investigate:
  - What happened?
  - Which systems were compromised?
  - What was the impact of the attack? (Can you assign a monetary value?)
  - How would you mitigate this attack? (Reduce impact? Reduce costs?)

Botnets – Robot Networks

A web of hijacked computers used to distribute malware, conduct phishing, or stage a DDoS attack – usually an attack on availability

- Bot herder – Controller of a botnet
- Bots/Zombie – Individual (corrupted) devices in a botnet

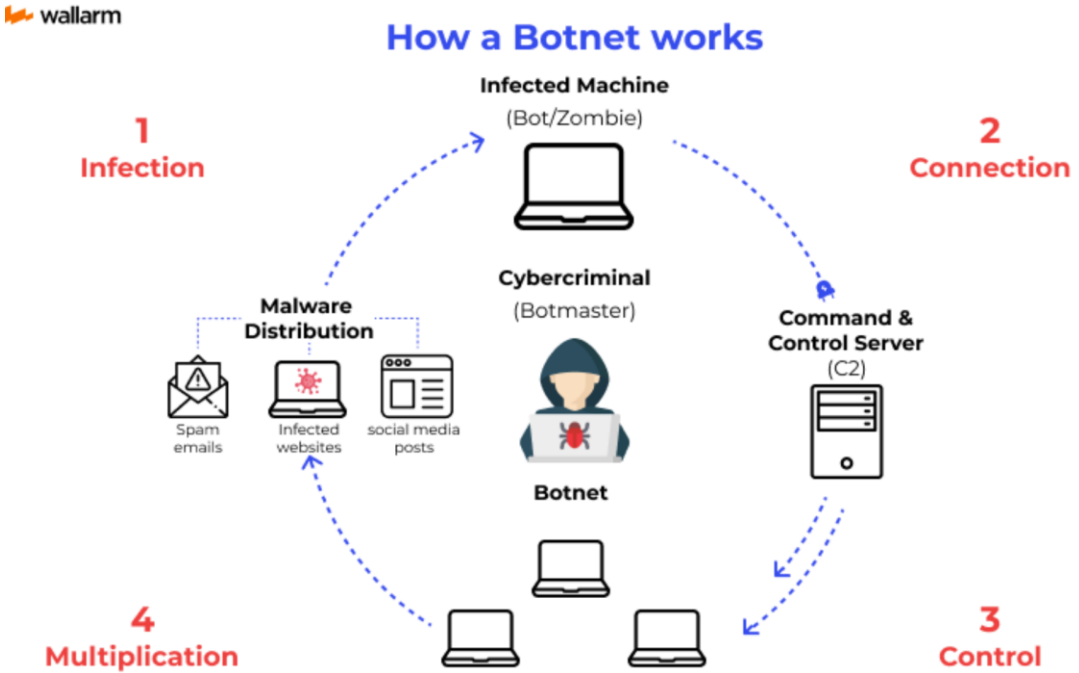
- Functional via remote commands from a Command and Control server (C&C) that guide the bots what to do

- Client-server
  - Robust communication with C&C, but easier to detect. Does not work if C&C is down
- Peer-to-peer infrastructure
  - All bots serve as C&C as well

Domain generation algorithms (DGA) generate lots of random domains, only one of which refers to the real C&C server

TU Delft

Botnets – Robot Networks



- Distributed Denial of Service (DDoS)
- Phishing
- Brute force attacks
- Crypto jacking

https://www.wallarm.com/what/what-is-a-botnet

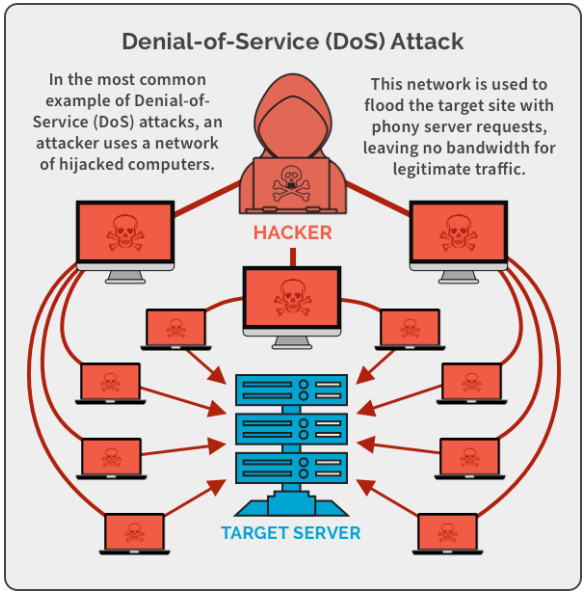
Botnets – Detection

- Sudden spike in bandwidth?
- Unidentified services keep booting up?
- Cannot close/stop a service?
- Changes made to file system?

(Distributed) Denial of Service

Flood the target system with arbitrary requests to the point of exhausting its resources

- DoS vs. DDoS: Single vs. multiple origin of attacks
  - Costs for the attacker?
  - Speed and traffic volume of the attacks?
  - Difficulty of detection?
- Volume-based attacks vs. Protocol-based attacks
- UDP/ICMP flooding, SYN flooding, Slowloris, Ping of death



Exercise – The Mirai botnet

FEATURE

The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet

Mira
It sc
atter
a bot

Who's responsibility was the attack? Mirai's code developers, vulnerable IoT device owners, Internet Service Providers?

This

including AirBnB, Amazon, Github, HBO, Netflix, Paypal, Reddit, and Twitter, by disturbing the DYN name-resolution service.

https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html/;
https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/

Cybercrime as a Service (CaaS)

A new(?) market created by "black-hat hackers for hire"

- No longer need coding skills to conduct cyberattacks

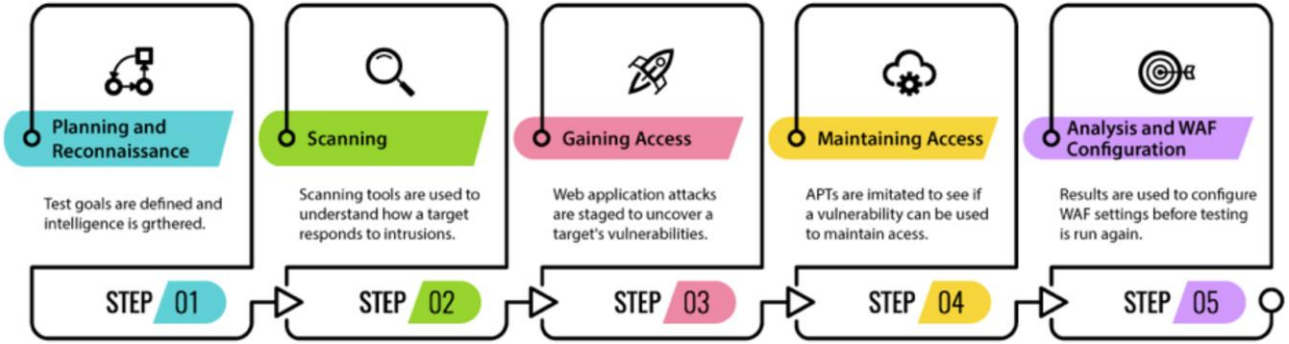
- Fraud-as-a-service
- Social account take-over
- Malware and phishing kits (e.g., Pegasus spyware)
- Eavesdrop in digital devices
- Wipe-out identity of a target – digital assassins

End of Part II
Questions?

TU Delft

Penetration testing

Simulated cyberattack on internal resources to discover exploitable vulnerabilities



- Two most important phases
  - Planning the scope and objectives
  - Reporting and patching the discovered vulnerabilities

- Access levels: External | Internal | Blind | Double-blind

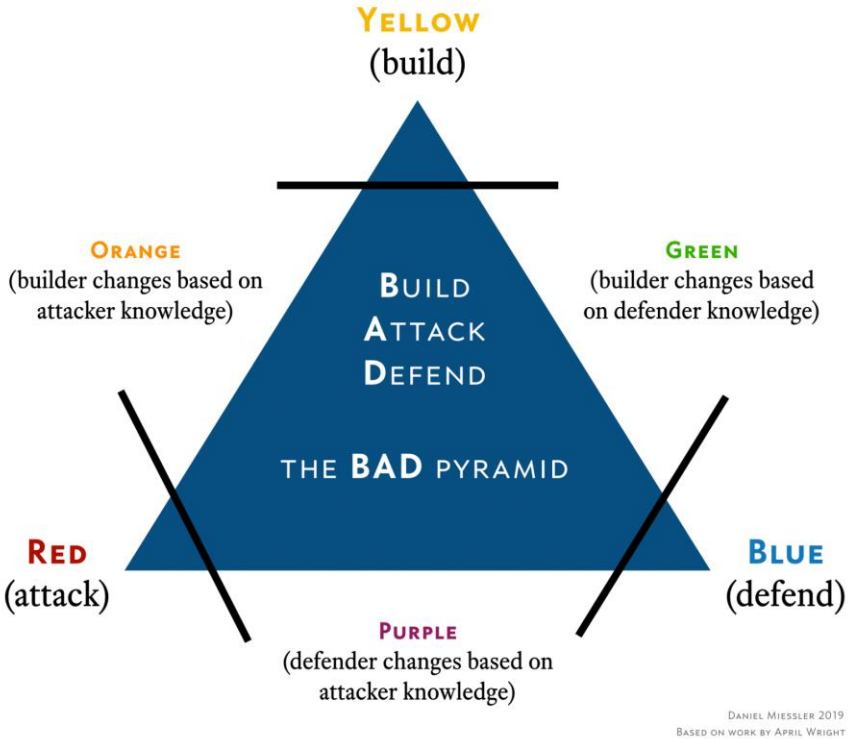
https://www.roguelogics.com/penetration-testing-what-do-you-need-to-know/

Red/blue/purple teaming

Red/blue team exercises run for extended time periods where red teams emulate the TTPs of (potentially) real adversaries and blue teams defend against (potentially) real attack campaigns.

- Red teams act like real adversaries
  - What is the difference from penetration testing?
- Blue teams are proactive defenders
  - Are all defenders blue teamers?

- Purple teaming refers to the communication between the red/blue teams



https://danielmiessler.com/study/red-blue-purple-teams/

Exercise – Incident response case study

Schwitter has an in-house incident response team. The analysts arrive in the morning to an alert that was raised last night at 2 am: a log-in attempt from an unrecognized device with an IP address located in India attempted to log in to the database containing customer information.

- What do you do?

The team gets a call that a database allegedly containing user credentials from Schwitter was found on sale on the dark-web.

- How do you verify this?

After investigating the attack, present a case to the company stakeholders.

TU Delft

Incident response and escalation

- Collect Indicators of Compromise (IoCs)
- Correlate different IoC sources to understand what is going on
  - Better yet, use a Security Information and Event Management (SIEM) to automate it
- Goal: Detect and stop the attack ASAP
  - Reduce cost/damages
- What are IoC sources?

Firewall logging

Network traffic

Intrusion detection system logs

VPN (remote access) logging

Anti-virus logging

Mail (spam) logging

Authentication logs

DNS logging

Incident response and escalation

- Analyze and correlate IP-addresses used by attackers (black listing)
- Investigate whether suspicious IP-addresses are linked to malicious activities
- Analyze the output of probes to identify what the attacker knows
  - Investigate logs
  - Run the software/tools yourself
- Analyze malware or suspicious software found on client machines
- Investigate the cause of unexpected crashes

TU Delft

Incident response and escalation

- Set up a separate logging mechanism on a secured server
- Forensic analysis on compromised machines
- Reset all passwords/ fresh OS installation
- Delete unknown user accounts
- Test early warning signs already in **P**robing and **P**enetration phases

Incident response and escalation

- Audit response mechanisms when a hack is detected
  - Make sure everything works correctly and nothing has been modified
- Agreements in place when a service provider is hacked or data is breached
- Disclose the breach/hack and its impact to the relevant parties

End of Part III
Questions?

Recap

Let’s fill it out together

- ??