ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

CDS201: Έλεγχος Εισβολών Δικτύων και Συστημάτων (Penetration Testing)

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Whoami

- Vasileios Chantzaras (vchantzaras@unipi.gr)
  - Computer Science (BSc)
  - Information Systems Security (MSc)
  - Hellenic National Defense / Cyber Defense
    - Offensive Security Engineering
    - Penetration Testing
    - Red Teaming
    - Cyber Defense Exercises
    - Incident Response

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Familiarization

- Operating Systems:
  Windows – Linux – Mac
- Windows/Linux Administration?
  Active Directory/Domain?
  Bash/sh, Powershell or others?

- Programming?
  Scripting Languages: Python, Perl, Ruby, Javascript?
  Low Level Windows Native: C/C++, (or Go, Rust)
  Others?

- Command and Control Frameworks(C2s)?
  Metasploit? CobaltStrike (or others)?

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Presentation Outline

- Penetration Testing Overview
  - Methods, Types, Environments
- Red Teaming vs Penetration Testing
- OPSEC
- Attack Lifecycle – Kill Chain

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Penetration Testing Overview

- often referred to as a “pentest”
- an organized, targeted, and authorized attack attempt
- test IT infrastructure and its defenders to determine their susceptibility to IT security vulnerabilities
- uses methods and techniques that real attackers use
- various techniques and analyses are applied to measure the impact that a vulnerability (or chain of vulnerabilities) may have on the confidentiality, integrity, and availability of an organization's IT systems and data.

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Penetration Testing Overview

- A pentest aims to uncover and identify ALL(?) vulnerabilities and improve the security for the tested systems

Penetration Testing Overview
Risk Management Process

Step	Details
Identifying the Risk	…risks the business is exposed to (legal, environmental, market, regulatory,….)
Analyze the Risk	determine their impact and probability. Should be mapped to the organization's policies, procedures, and processes.
Evaluate the Risk	Evaluate, rank, and prioritize risks. The organization must decide to accept (unavoidable), avoid (change plans), control (mitigate), or transfer risk (insure).
Dealing with Risk	Eliminate or contain the risks as best as possible. Communicate with the stakeholders for the system or process that the risk is associated with.
Monitoring Risk	Constantly monitor risks for any situational changes that could change their impact score, i.e., low to medium or high impact.

Penetration Testing Overview
Risk Management

- Pentesting is part of Risk Management Process of an organization
- identify, evaluate, and mitigate any potential risks that could damage the confidentiality, integrity, and availability of an organization's information systems and data
- reduce the overall risk to an acceptable level (?)
- identifying potential threats,

Penetration Testing Overview
Risk Management

Reduce the overall risk to an acceptable level (?) by:

- identifying potential threats
- evaluating their risks
- taking the necessary actions to reduce or eliminate them by
  - implementing the appropriate security controls and policies (access control, encryption, …)
- ensure that the data is kept safe and secure

Penetration Testing Overview
Risk Management

- We **cannot** eliminate every risk
  - even when the organization has taken all reasonable steps to manage the risk the risk of a security breach is present
- Organizations can use different ways to Accept, Transfer, Avoid, and Mitigate the risks
  - Purchase insurance to cover certain risks (natural disasters, accidents) or transfer the risk to third party providers
  - Implement preventive measures (to reduce the likelihood of certain risks
  - Put procedures in place to minimize the impact of risks being occurred
  - Financially reduce the economic consequences of specific risks

Penetration Testing Overview
Risk Management

Our role as a trusted advisor (pentester) is to prepare detailed documentation on the tasks and steps taken and the related results:

- Report vulnerabilities
- Detailed reproduction steps
- Appropriate remediation recommendations

We **do not**:

- Apply patches
- Make code changes

A pentest is a snapshot of the security level at the current time

Penetration Testing Overview Vulnerability Assessments

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

- Vulnerability or security assessments (VAs) are conducted using automated tools
- Systems are checked for known issues and vulnerabilities by scanning with tools like
  - Nessus
  - Qyalys
  - OpenVAS
- Automated scans cannot adapt to the configurations of the assessed systems so **manual testing by experienced testers is essential**

Penetration Testing Overview Vulnerability Assessments

A pentest

- is a mix of automated and manual testing (validation)
- Is conducted after extensive manual information gathering
- Adjusted to the systems being tested
- Planning and Execution are much more complex
- VAs may only be carried out under a mutual agreement between the employing company of the tester and the assessed organization
- An explicit written authorization is mandatory to conduct any assessment activities
- The assessed organization may only request testing against its' own assests
  - Written approvals from third party entities
  - Confirm asset ownership with the organization during scoping phase (AWS policy doesn't require one for example when pentesting Amazon assets of a company)

Penetration Testing Overview

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

A successful pentest requires:

- Considerable preparation and organization
- A clear process model
- Adoption to the organization’s needs
- The organization must have a clear understanding of the process and the activities planned
- Accurate scoping of the assessment

Penetration Testing Overview

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

- Typically Employees are not informed about a pentest taking place
- They however may be informed due to privacy concerns from the organizations
- Personal data found during a pentest must be kept private according to regulations from Data Protection Authorities
- If personal/sensitive data are found during and assessment (e.x. in Databases) then acts are recommended (encryption, changing passwords …) accordingly

Penetration Testing Overview
Testing Methods

Based on where we start our tests:

- **External**
  - As an anonymous user on the internet
  - the goal is to ensure protection against attacks on the external network perimeter (as possible)
  - Can be conducted from our own host (with a VPN connection to avoid ISP blockings) or from a VPS.
  - My be conducted in a stealthy approach (trying to avoid IPS/IDS triggering alarms) or

    In hybrid mode - where we gradually become “noisier” to test the detection effectivness

  Goal: Access public-facing hosts, obtain sensitive data, or gain access to the internal network

Penetration Testing Overview
Testing Methods

Based on where we start our tests:

- **Internal**
  - Perform testing from within the corporate network/environment
  - Can follow up a successful external penetration test
  - Or conducted in an assumed breach scenario
  - Isolated systems may also be assessed with a physical presence

Penetration Testing Overview Types

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Based on how much information is available to us:

Type	Information available
Blackbox	Only essential information (Ips, domains)
Greybox	Additional information provided (Urls, hostnames, subnets ..)
Whitebox	Everything is disclosed. The entire infra. Even detailed confs, admin creds, web app source code, …
Red- Teaming	Extra tasks such as social engineering assessments, physical testings. Can be conbined with (Black | Grey | White) box
Purple - Teaming	As Red Teaming but in cooperation with the defense team (Blue)

Penetration Testing Overview Types

Complexity and time of a pentest depends on information provided.

Blackbox type:

We must first map the organizational infra based on scope, servers, hosts, services present which requires considerable amount of time (especially if a stealthy approach is requested)

Penetration Testing Overview
Testing Environments

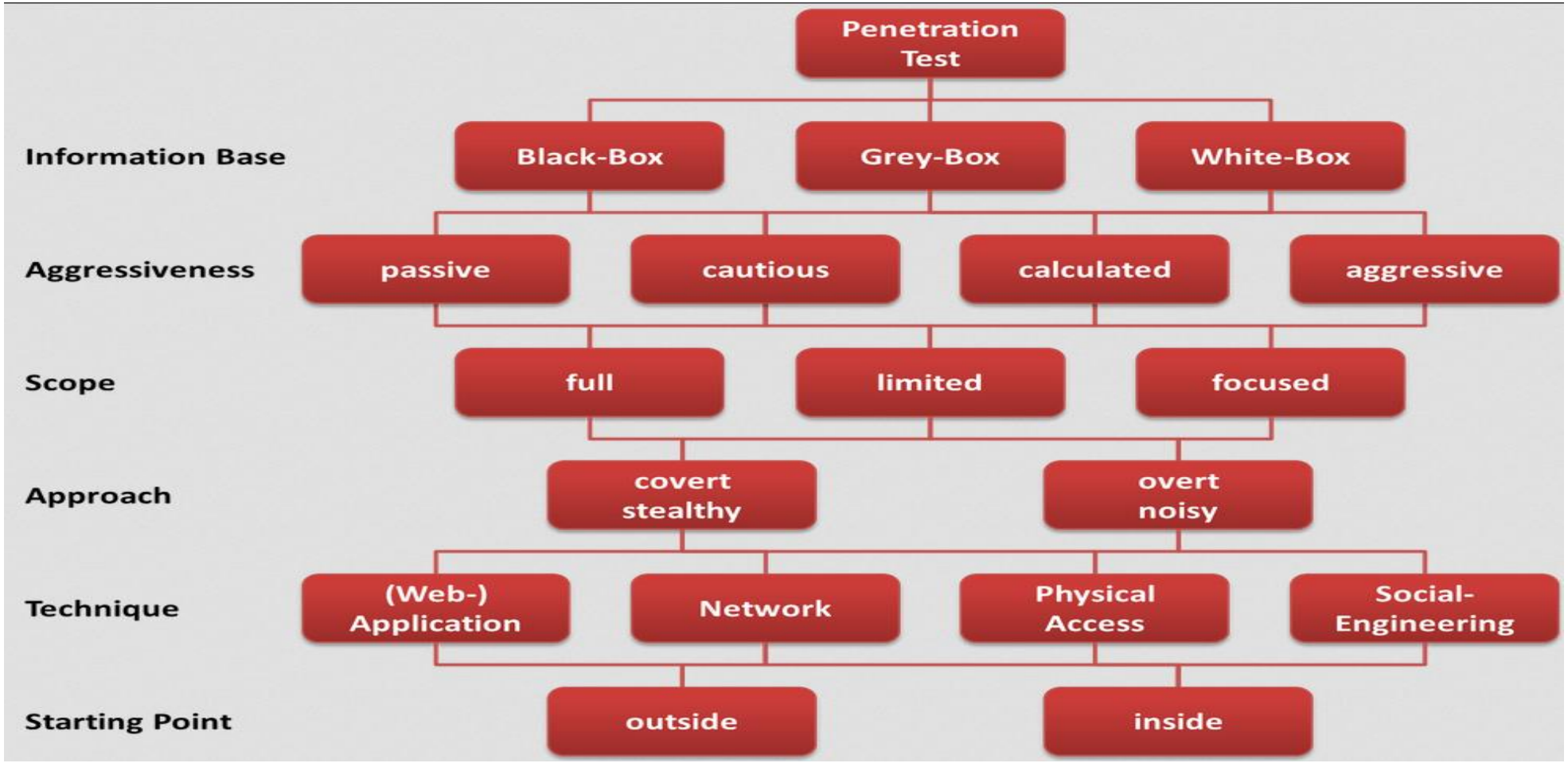
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

What to be tested. Some of the categories of the environments can contain:

- Network
- WebApp
- API
- Cloud
- Security Policies
- Employees
- …..

All categories may be included in any different type of a pentest

Penetration Testing Overview
Testing Matrix



Ethical and Legal Considerations

- Each country has its federal laws and regulations for computer-related activities and other.
- During a pentest we must follow these laws to protect individuals from unauthorized actions performed that can lead to exploitation and ensure their privacy.

Ethical and Legal Considerations

- perform actions against a company that would be against the law under other circumstances
- there is a line between legal and illegal actions that can easily be crossed if we try to practice our skills outside of these controlled environments
- performing ANY activities that interact with ANY of an organization's systems without explicit written consent (detailed scope of testing, contract, rules of engagement) is against the law and **could lead to legal and even criminal action being taken against us**

Ethical and Legal Considerations
“primum non nocere” = "first, do no harm"

- Nice to follow the Hippcratic Oath - doctors should not risk doing more harm than good to their patients
- As security professionals we don't want to harm or weaken the security of our clients
- …but some harm is worth enduring for the potential benefit.

Ethical and Legal Considerations Some precautionary measures

- Obtain written consent from the owner or authorized representative of the network or assets being tested
- Test strictly in scope of the consent obtained - respect any limitations specified
- Prevent causing damage to the systems or networks being tested
- Do not access, use or disclose personal data or any other information obtained during the testing without permission
- Do not intercept electronic communications without the consent of one of the parties to the communication

Penetration Testing Process

- A deterministic process (events are dependent on others)
- Specific sequence of operations (flexible processes)
- All the steps performed in order to fulfil our objectives
- Stages in a circular process

Penetration Testing Process
Pre-engagement

During this phase everything is arranged about the testing:

- NDAs (Non – Disclosure Aggreement)
- Scope and Goals to be achieved
- Time of testings
- Rules of Engagement

Penetration Testing Process Information Gathering

- Gather information about the target, which may include domain names, IP addresses, network architecture, and any publicly available data.
- Use passive reconnaissance techniques like OSINT (Open Source Intelligence) to collect information about the organization and its assets.
- We gather anything (Passively) that could be used to gain a foothold

Penetration Testing Process
Footprinting and Enumeration

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

- Perform active reconnaissance to discover open ports, services, and vulnerabilities.
- Utilize tools like Nmap to scan for live hosts and services (Actively Scanning).
- Enumerate services and collect detailed information about the target systems.

Penetration Testing Process
Vulnerability Analysis

- Analyze the results from information gathering phase to find known vulnerabilities in the systems/applications
- Discover attack vectors
- Evaluate potential vulnerabilities manually or …

  automatically with tools like Nessus or OpenVAS.

Penetration Testing Process Exploitation

Attempt to exploit the discovered vulnerabilities to gain initial (unauthorized) access to systems.

**Exploitation should only be performed within the agreed-upon scope and with explicit client consent.

Penetration Testing Process
Post Exploitation

- Once access is gained, further assess the environment, escalate privileges, and maintain access.
- Collect additional information and perform actions to demonstrate the potential impact of a real attacker.
- Actions taken here can help to the lateral movement process

Penetration Testing Process
Lateral Movement

Maybe more of a Post Exploitation process rather than a phase..

- Moving within the internal network of the target organization to access additional systems with the same or a higher privileges
- Can be repeated several times in order to reach our goal

Penetration Testing Process Documentation and Reporting (PoC)

- Document in a step-by-step manner all findings, including vulnerabilities, successful exploits, that gave us some level of access and the potential impact on the organization.
- Helps the organization to understand what we were able to do
- Helps the remediation process

Penetration Testing Process
Post Engagement (Communication)

- Documentation is presented to the IT administrators and the management level of the organization.
- We make sure they understand the severity of the vulnerabilities found.
- Clean up the tested infrastructure (traces from our actions on hosts and servers)
- Create the deliverables and present them
- Retain all the data of the pentest until retesting to ensure fixes are applied by the organization

Red Teaming

- Red teaming is the process of using Tactics, Techniques, and Procedures (TTPs) to emulate real-world threats with the goal of training and measuring the effectiveness of the people, processes, and technology used to defend an environment.
- In terms of business risk, a red team engagement focuses on understanding how well security operations deal with a threat through training or measurement. Technical findings are often revealed during an engagement but are not the focus.
- Red teaming engagements are designed to challenge security operation's defensive strategies and assumptions and to identify gaps or flaws in the defensive strategies.
- Improving security operations through training or measurement is the goal of a red teaming engagement.

…. Joe Vest & James Tubberville

Red Teaming

From an adversary perspective Red teams challenge some *dangerous* assumptions of the blue teams(defenders) such as:

- *"we're secure because we patch“*
- *"only X number of people can access that system“*
- *"technology Y would stop that"*

This way, a red team can identify areas for improvement in an organization's operational defense.

Red Teaming
First, do not harm

Red teams carry out harmful actions like:

- Disabling security controls (AVs/EDRs or host firewalls)
- Adding users to privileged groups (Local or Domain Admins)
- Creating various administrative backdoors to systems
- …so many others

These are dangerous because once in-place, they can be abused by another party and as a result the organization's risk exposure is increased.

Red Teaming
First, do not harm

On the opposite side of view….

These tactics are used by real adversaries…….our goal is to emulate them.

Judgement comes in play! For example:

We won’t actually ransomware the organisation just because that's what an adversary might do…

When we are not sure: seek advice from your team lead or client contact

Red Teaming

- Red teaming is the process of using Tactics, Techniques, and Procedures (TTPs) to emulate real-world threats with the goal of training and measuring the effectiveness of the people, processes, and technology used to defend an environment.
- In terms of business risk, a red team engagement focuses on understanding how well security operations deal with a threat through training or measurement. Technical findings are often revealed during an engagement but are not the focus.
- Red teaming engagements are designed to challenge security operation's defensive strategies and assumptions and to identify gaps or flaws in the defensive strategies.
- Improving security operations through training or measurement is the goal of a red teaming engagement.

…. Joe Vest & James Tubberville

Red Teaming vs Penetration Testing

A typical penetration test will focus on a single technology stack (project lifecycle requirement OR compliance requirement). "exploit the system(s)“. The goal is to:

- Identify as many vulnerabilities as possible
- Demonstrate how those may be exploited
- Provide some contextual risk ratings
- Reports each vulnerability and remediation actions (install a patch or reconfigure some software)
- No explicit focus on detection or response
- Does not assess people or processes

Red Teaming vs Penetration Testing

Red Teams

- Clear objective defined by the organization (e.x gain access to a particular system, email account, database or file share)
- Emulate a real-life threat to the organization (study and re-use (where appropriate) the TTPs of the threat they're emulating → help organisations to build detections and processes designed to combat these threat(s))
- Search holistically at the overall security posture of an organization (people, processes and technology)
- Heavy emphasis is put on stealth and the "principal of least privilege". Reach objectives without getting caught.

OPSEC (Operational Security)

- Operations Security (OPSEC) is a term originally coined by the US military and adopted by the information security community. It's generally used to describe the "ease" by which actions can be observed by "enemy" intelligence.
- From Red Teaming perspective: measure of how easily actions can be observed by the defenders.
  - every action RT takes will leave indicators
  - how well those indicators are understood
  - what is the likelihood that the defenders will see and/or respond to them
- Both red and blue team actions are being monitored and disrupted by the opposite side. It is wise to assume that the team we ‘re up against are better than us.

Attack Lifecycle

- Reconnaissance - scout a target and find potential attack vectors.
- Weaponization - develop a malicious payload.
- Delivery - develop a means of delivery the payload.
- Exploitation - the initial attack of delivering the weaponized payload.
- Installation - installing persistent malware on the target.
- Command & Control - establish a means of controlling compromised targets.
- Actions on Objectives - achieve the operational goal (defacement, data theft, etc).

Cyber Kill Chain by Lockheed Martin

Attack Lifecycle

Cyber Kill Chain by Lockheed Martin purpose was to provide a framework for informing defensive measures but:

- phases 1, 2 and 3 occur on the attacker's machine, so there’s no much one can do to mitigate them
- no detail in phase 7 - i.e. once an attacker has compromised one or more targets, how do they actually go about achieving their objective?

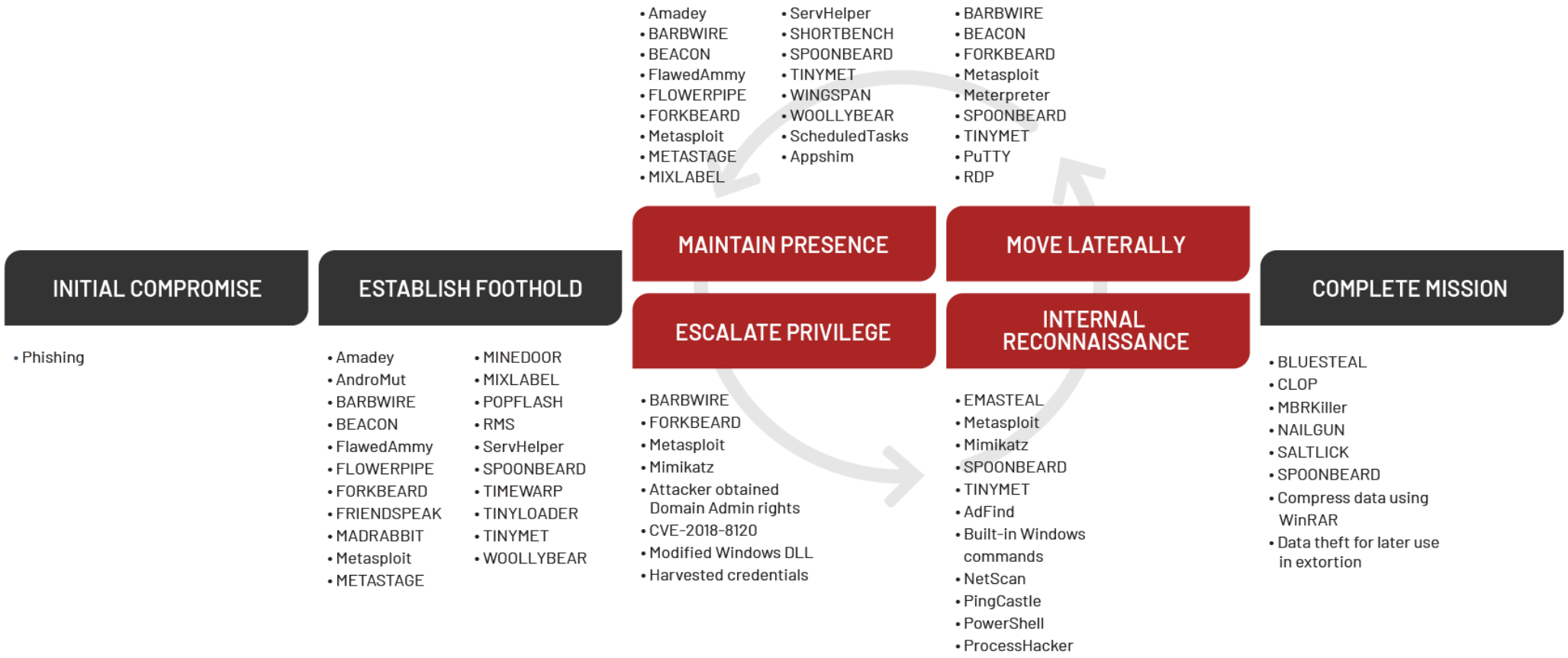
So that led other companies to give their own versions to better address these issues.

Attack Lifecycle (Mandiant)

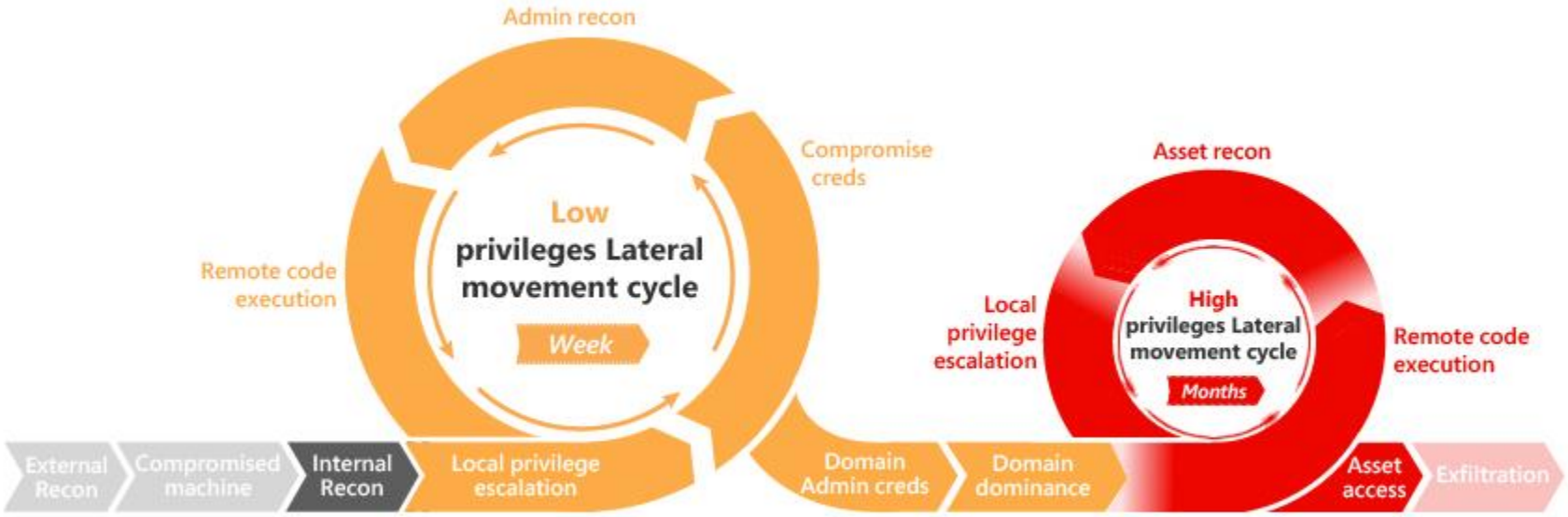
- Initial Reconnaissance - research the targets systems and employees to develop a methodology for the intrusion.
- Initial Compromise - execute malicious code on one or more targets via the attack vector planned during phase 1.
- Establish Foothold - maintain continued control over a compromised system by installing persistent backdoors.
- Escalate Privileges - exploit system vulnerabilities or misconfigurations to obtain local admin access to compromised systems.
- Internal Reconnaissance - explore the target's internal infrastructure and environment.
- Move Laterally - use credentials obtained from phase 4 to compromised additional systems.
- Maintain Presence - maintain highly privileged access to domains and systems.
- Complete Mission - accomplish the operational objective.

Mandiant's Targeted Attack Lifecycle

Attack Lifecycle (Mandiant)



Attack Lifecycle (Microsoft)



Penetration Testing Standards

- PTES - Penetration Testing Execution Standard applied to all types of penetration tests
- OSSTMM - Open Source Security Testing Methodology Manual is another set of guidelines pentesters can use. Can be used alongside other pentest standards
- NIST (National Institute of Standards and Technology) with the NIST Cybersecurity Framework
- OWASP - Open Web Application Security Project with:
  - Web Security Testing Guide (WSTG)
  - Mobile Security Testing Guide (MSTG)
  - Firmware Security Testing Methodology

Penetration Testing Standards Vulnerability Scoring

- Common Vulnerability Scoring System (CVSS)

  with Microsoft DREAD

- Common Vulnerabilities and Exposures (CVE): a publicly available catalog of security issues sponsored by the United States Department of Homeland Security (DHS)

Getting Started Preparation

- Choose a Distro
  - Kali Linux, ParrotOS, Windows
- Setup the Distro
  - Using a hypervisor (HyperV, VirtualBox, VWMare Workstation Player)
  - Hackthebox Custom ParrotOS version (Pawnbox) – for labs and demos
- Stay organized
  - Keeping well formated notes (scoping data, enumeration data, evidence for PoCs)
  - Note tools (Cherrytree, Visual Studio Code, Sublime Text, Notepad++)

Getting Started
Common Terms

Shell: A term we use a lot….

on Linux: a program with which a user can interact with the operating system to run commands.

- Bash (Bourne Again Shell)
- Sh
- Zsh
- Tcsh
- Ksh,
- Fish shell
- etc…

Getting Started
Shell types

Shell Type	Description
Reverse shell	Initiates a connection back to a "listener" on the “attackers” machine (host).
Bind shell	"Binds" to a specific port on the target host and waits for a connection from the attacker.
Web shell	Runs operating system commands via the HTTP/S protocol usually via a web browser, typically not interactive or semi-interactive. It can be used to run specific tasks like exploiting a file upload vulnerability and uploading a PHP (| Python | Perl | Go | Bash | …) script to run a single command (one liner).

Payload All The Things : a comprehensive list of reverse shell commands we can use that cover a wide range of options depending on our compromised host

Getting Started
Ports

Port(s)	Protocol
20/21 (TCP)	FTP
22 (TCP)	SSH
23 (TCP)	Telnet
25 (TCP)	SMTP
80 (TCP)	HTTP

Port(s)	Protocol
161 (TCP/UDP)	SNMP
389 (TCP/UDP)	LDAP
443 (TCP)	SSL/TLS (HTTPS)
445 (TCP)	SMB
3389 (TCP)	RDP

There are two categories of ports, Transmission Control Protocol (TCP), and User Datagram Protocol (UDP).

as pentesters, we have to be able to recognize them from just their number quickly (i.e., 21 is FTP, 80 is HTTP, 88 is Kerberos) without always having to look it up

Getting Started
Web Server

- an application that runs on the back-end server
- handles all of the HTTP traffic from the client-side
- Routes to specific pages
- Usually runs on ports 80/443 (HTTP/S)
- Public facing interaction over the internet
- Provide a vast attack surface → High value target

Getting Started
Web App Vulns - OWASP Top 10

- OWASP (Open Web Application Security Project) is a list of the top 10 web application vulnerabilities
- A starting point. Most dangerous vulnerabilities and not an exhaustive list of all possible web application vulnerabilities.

- Web application vulnerabilities will be covered in-depth in later presentations and labs (mostly on HTB)

Getting Started
Tools

- **SSH** - used to remotely access systems locally, over the internet, initiate connections in other networks using port forwarding/proxying, and upload/download files
- **Netcat** (ncat/nc) - used to connect to any listening port and interact with the service running on that port
- **Nmap** – for service scanning and attacking nerwork services (grab banners, FTP, SMB, SNMP, Shares, …)

  identify the operating system and any available services that might be running in order to further look for possible vulnerabilities.
- **Gobuster** - For Web Enumeration (Direcory/File Enumeration, DNS Subdomain Enumeration)
- **Whatweb**, **Certificates**
- **Public available exploits (Metasploit Framework - MSF)**

Questions?