Policy - Defines what is and what is not allowed.

Attack – sequence of actions that create a violation of a security policy.

When attackers launch attack they have a goal in mind.

Goal may be ill formed as in one of exploration ;

may be very general ;as in disrupting proper operation of a system.

Or it may be very specific – acquiring copy of a specific file.

A goal is that which attacker hopes to achieve.

Attacker launches an attack against an entity or entities .The attack may affect other entities but that’s incidental to purpose of attack.

A target of an attack is the entity that the attacker wishes to affect.

Targets of the 2 attacks mentioned above were the computer system.

Acquiring control of computer may be step towards a larger goal ,example obtaining copy of confidential document or changing information on system.

Multistage attack is an attack that requires several steps to achieve its goal.

Most attacks are multistage.

Intrusion response

Once an attack is detected, how can the system be protected.

Field of intrusion response deals with the problem. Goal is to handle the attack in such a way that damage is minimized.

Some mechanisms may be augmented to thwart intrusions.

Others require human intrusion to respond to the attack and repair any damage

Incident prevention

Ideally intrusion attempts will be detected and stopped before they succeed.

Involves closely monitoring the system and taking action to defeat the attack.

Prevention requires attack be identified before it completes.

Defenders use real time intrusion detection systems and other techniques to identify attacks.

Attack surface – set of entry points attackers use to compromise system.

Intrusion handling

Directed attacks – more labour and skill intensive. They are more likely to be perpetrated on targets where there is a prize to win i.e large organizations.

Not that directed attacks aren’t perpetrated with the aid of malware.

You could design malware for a specific target ,as was case with Stuxnet worm.

Directed attacks generally take more sophistication. On the other hand , we shouldn’t discount ease of use of automated tools for attacking systems.

Due to automation ,may be easier to lower the skill level required, we get a phenomenon known as Script Kiddies. People who don’t know much about systems but know where they can find tools to attack systems. Tools that don’t require much expertise to use.

Automated attack tools may become a problem for all computer users as economic of threat picture changes. Attacks can be numerous and diverse .So it’s difficult to present an overview of them.

Seen classification of attacks in early part of course , in chapter 1.2 threats section.

Had overview of Disclosure, Deception ,Disruption and Usurpation.

Disclosure – unauthorized access to information.

Deception – Acceptance of false data.

Disruption – Interruption or prevention of correct operation.

Usurpation – Unauthorized control of some part of a system.

Snooping or eavesdropping – unauthorized interception of information , a form of disclosure.

Modification or alteration- Unauthorized change of information

Masquerading or spoofing – impersonation of one entity by another.

Lures victim into believing entity with which it is communicating is a different entity.

Repudiation of origin

Denial of service

We get many threats though we don’t know how to perpetrate them.

When an intrusion occurs , the security policy of the site has been violated. Handling the intrusion means restoring the system to comply with site security policy and taking any actions against attacker that the policy specifies.

Intrusion handling has several phases

1.Preparation for an attack – Occurs before any attacks are detected. Establishes procedures and mechanisms for detecting and responding to attacks.

2.Identification of an attack – This triggers the remaining phases.

3.Containment of attack – limits effect of attack as much as possible.

4.Eradication of attack – Stops attack and blocks further similar attacks.

5.Recovery from attack – restores system to a secure state with respect to site security policy

6.Follow up to attack – Taking action against attacker .

PICERF

Containment phase

Containing or Confining attack means limiting access of attacker to system resources.

Protection domain of attacker reduced as much as possible

2 approaches

1)Passively monitoring the attack

2)constraining access to prevent further damage to system.

Damage – any action that causes system to deviate from secure state as per site security policy.

Passive monitoring records the attacker’s actions for later use. Monitors do not interfere with attack in any way. Marginally useful as it will reveal information about attack and goals of attack. However intruded system is vulnerable throughout.

a "protection domain" defines the resources that a process or user is authorized to access and the types of operations that are allowed on those resources

Other approach – steps taken to constrain actions of attacker – more difficult.

Goal is to minimize protection domain of attacker while preventing attacker from achieving their goal. But system defenders may not know what goal of attacker is and thus may misdirect confinement

So that data or resources attacker seeks lie within minimal protection domain of attacker.

Honeypot (within containment phase)

Stoll detected an attacker in a computer system at the Lawrence laboratory.

Attacker looking for nuclear weapons documents.  
He tried to trace attacker, tracing ended at attacker’s point of entry into US.

The foreign authorities said they would need a longer connection to trace attacker to point of origin.

Stoll created a large file containing keywords for which attacker has been searching. When the attacker next entered, he found the file and started downloading. The time for upload was enough for attacker to be traced and he was arrested

Document stoll wrote is a honeypot. The file designed to entice attacker to download, but contains meaningless information.

This technique extended to systems and networks . Honeypots sometimes called decoy servers, are servers that offer many targets for attackers.

The targets designed to entice attackers to take actions indicating their goals.

Honeypots are instrumented and closely monitored.

When system detects an attack,it takes action to shift attack to honeypot system.

Wrappers ,Firewalls - > Eradication phase

Eradication phase

Eradicating an attack means stopping the attack. The usual approach is to deny access to the system completely (such as by terminating the network connection) or terminate processes involved in the attack.

Important aspect of eradication – ensure that attack doesn’t immediately resume. This requires

attacks be blocked.

Approach to blocking -place wrappers around suspected targets with various forms of access control.

Wrappers implement various forms of access control.

Wrappers that control access to resources embedded in kernel to make them difficult to bypass.

Firewalls

Firewalls sits between an organization’s internal network and some external network (such as internet).

Firewall controls access from external network to internal network and vice versa. Advantage of firewalls is that they can filter network traffic before it reaches target host.

Can also redirect network connections, throttle traffic to limit traffic that flows into internal network.

Follow up phase

In the follow up phase the systems take some action against the attacker.

Most common follow up pursue some form – legal action either criminal or civil.

Confine ourselves to technical issue of tracing attack through network.

Two techniques for tracing are thumbprinting and IP header marking.

Thumbprinting takes advantage of connections passing through several hosts.

Attacker may go from one host through many intermediate hosts till he reaches target.

If one monitors connections at any 2 hosts that connections pass through, contents of connections will be the same ,excluding data at lower layers.

One can construct chain of hosts.

Good thumbprint

1)Take as little space as possible.

2)Cost little to compute and compare

Counterattacking or attacking attacker takes several forms.

CSIRT – computer security incident response team.

Team established to assist and coordinate responses to a security incident among a defined constituency.

Counter attacking – attacking the attacker takes several forms.

A technical Counterattack -goal of damaging the attacker seriously enough to stop current attack and discourage future attacks.

It has consequences that need to be considered.

1.May harm an innocent party. The attacker maybe impersonating another party.

2.May have unintended consequences.

3.It is antithetical to shared use of network.  
4. May be legally actionable.

Match the following measures with the intrusion handling phases that they most closely belong to.

Feedback

Your answer is correct.

The correct answer is:

CSIRT → Follow-up phase,

Honeypot → Containment phase,

"Wrappers" around suspected targets → Eradication phase,

Legal action → Follow-up phase

A screenshot of a chat

Description automatically generated

Intrusion response and incident prevention

Prevention requires attack be identified before it completes.

Jailing – approach that allows attackers to think they have succeeded but places them in confined area in which their observed behaviour can be controlled.

Attack surface – set of entry points and data attackers can use to compromise a system.

Attacker need only find one such avenue to compromise the system.

Traditionally defenses simply hardened the system to reduce the attack surface.

But surfaces was not empty so still ways for attacker to gain entry.

Attacker is free to change tactics and has more flexibility than defender ,this asymmetry is defender’s dilemma.

Moving target defenses reduce asymmetry. They change attack surface while system running so attack that works at one time won’t work at another time.

Moving target defenses – change system as it runs to thwart attacks.

Port hopping

Attacker want to attack port 80

Port is changing every hour. From outside firewall port appears the same.

Changing what is being attacked

Recovery

One important recovery mechanism – backup. Backup most important security mechanism.

Have a regular backup to the cloud.

Attacks can see that backups are also destroyed at the same time.

Good to have 2 backups in case one is lost.

Difference between honeypot and a jail

Honeypots sometimes called decoy servers, are servers that offer many targets for attackers.

The targets designed to entice attackers to take actions indicating their goals.

Honeypots are instrumented and closely monitored.

Jailing – attacker is not stuck there and can leave.

Jailing – approach that allows attackers to think they have succeeded but places them in confined area in which their observed behaviour can be controlled.