DTiF
Digital Technologies in focus
Initiative of and funded by the Australian Government Department of Education, Skills and Employment

acara
AUSTRALIAN CURRICULUM, ASSESSMENT AND REPORTING AUTHORITY

TEACHING TIPS

Hacker versus attacker

Clarifying the terminology

Most people have heard of hackers and malicious attackers. Many have even suffered the consequences of criminal actions. So, who are these people? And why do we have different names for them?

The typology of hackers is wide-reaching, especially as the identity of hackers has shifted and changed continuously since the 1980s (Söderberg 2010). To account for the different shades that characterise this community, we have examined the blurred boundaries that represent hackers and associated concepts such as attackers within cyber security.

Traditionally the hacker was the epitome of a cyber security threat and the embodied misuse of the internet. However, in recent years, notions of hacking have begun to change. Blurred boundaries mark the term, best expressed in its overlap with 'security researcher' (Tanczer 2020).

Previously, we saw hackers classified into coloured hats. The black hat/white hat terminology originates in the Western genre of popular American culture, in which black and white hats denote villainous and heroic cowboys respectively, to resemble the contrast of good and evil. (See figure 1) en.wikipedia.org/wiki/Black_hat_(computer_security) - :~:text=The black hat%2Fwhite hat,contrast of good and evil

Types of hackers

BLACK HAT	WHITE HAT	GREY HAT	GREEN HAT	BLUE HAT	RED HAT
Malicious hacker	Ethical hacker	Not malicious, but not always ethical	New, unskilled hacker	Vengeful hacker	Vigilante hacker

Figure 1: Former terminology for types of hackers
Image source: searchsecurity.techtarget.com/answer/What-is-red-and-white-hat-hacking

Developed by ACARA's Digital Technologies in focus project
Australian Government Department of Education, Skills and Employment CC BY 4.0

1

This system became quite complex, when in reality, regardless of skill level we were looking at 2 types of people:

- those who have the intent of researching systems ethically to find vulnerabilities
- those who have a malicious intent for accessing systems.

You will now see 2 terms in more prominent use:

- hackers or ethical hackers
- attackers or malicious attackers.

The Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC) provide advice and information about how to protect you, your family and businesses online. The ACSC provides a glossary to help understand the many cyber security terms: www.cyber.gov.au/acsc/view-all-content/glossary

Hacker: A computer expert that can gain unauthorised access to computer systems. Hacker is an overarching term; a hacker does not necessarily have malicious intent.

Figure 2: Sample ethical hacker chain
Image source: www.vpnmentor.com/blog/ultimate-guide-to-ethical-hacking/

Developed by ACARA's Digital Technologies in focus project
Australian Government Department of Education, Skills and Employment CC BY 4.0

2

Attacker: A person who hacks for personal gain and/or who engages in illicit and unsanctioned hacking activities

A cyber attack is usually performed following a number of steps often referred to as a 'cyber intrusion chain'. Knowing these steps can be useful. When we are designing and building digital systems we should keep these in mind to ensure our own systems are secure at key points of the design.
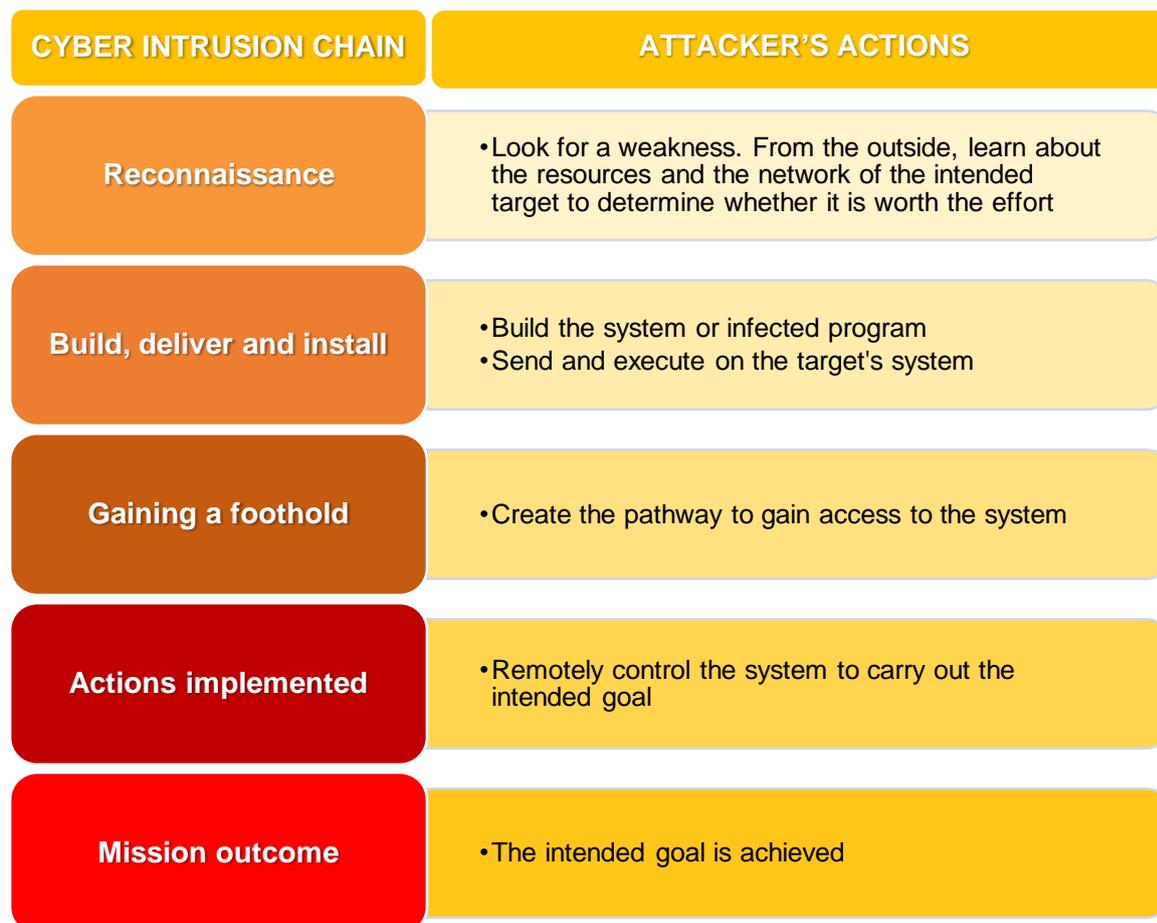
CYBER INTRUSION CHAIN	ATTACKER'S ACTIONS
Reconnaissance	• Look for a weakness. From the outside, learn about the resources and the network of the intended target to determine whether it is worth the effort
Build, deliver and install	• Build the system or infected program • Send and execute on the target's system
Gaining a foothold	• Create the pathway to gain access to the system
Actions implemented	• Remotely control the system to carry out the intended goal
Mission outcome	• The intended goal is achieved

Figure 2: Sample cyber attacker chain
Image source: ACARA

References

Oliver D & Randolph AB (2020) 'Hacker definitions in information systems research', *The Journal of Computer Information Systems*, 1–13, doi.org/10.1080/08874417.2020.1833379.

Söderberg J (2010) 'Misuser inventions and the invention of the misuser: hackers, crackers and filesharers', *Science as Culture*, 19(2):151–179, doi.org/10.1080/09505430903168177.

Tanczer LM (2020) '50 shades of hacking: how IT and cybersecurity industry actors perceive good, bad, and former hackers', *Contemporary Security Policy*, *41*(1):108–128, doi.org/10.1080/13523260.2019.1669336.

Developed by ACARA's Digital Technologies in focus project
Australian Government Department of Education, Skills and Employment CC BY 4.0

3