Threatlandscape

Access: Vulnerabilities

Irfan Kanat

Department of Digitization
Copenhagen Business School

February 21, 2022

Threatlandscape

Threatlandscape
Access: Vulnerabilities

Irfan Kanat

Department of Digitization
Copenhagen Business School

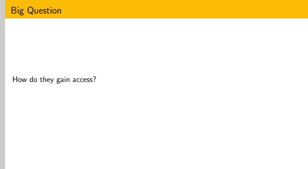
February 21, 2022

This work is licensed under a Creative Commons Attribution 4.0 International License.

In this presentation we focus on how malicious actors gain access to information assets.

Big Question

How do they gain access?



Big Question

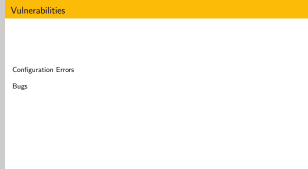
How do they gain access?

Now that we know who all is out there, let us take a look at how they do what they do. According to DBIR 2021 report, 85% of the breaches involved some sort of human involvement. 61% of the breaches involved credentials.

Vulnerabilities

Configuration Errors

Bugs



Vulnerabilities

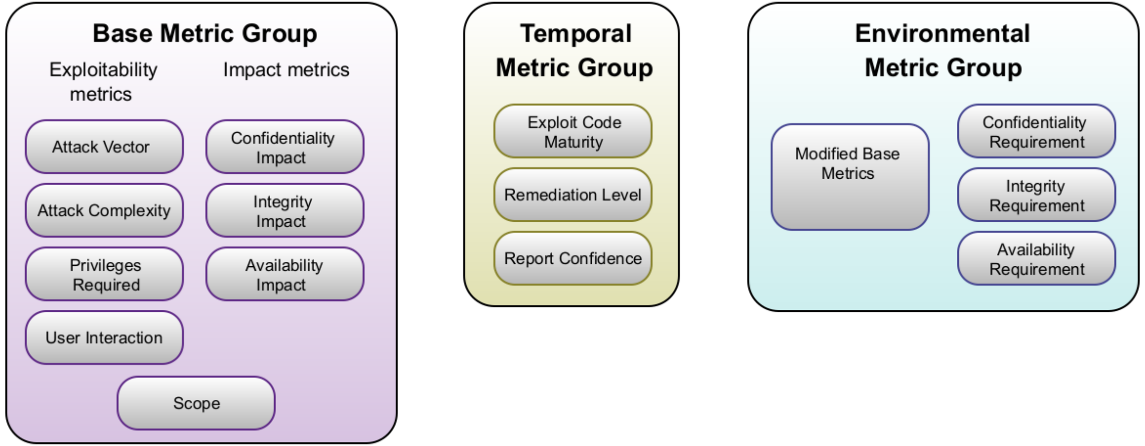
Configuration Errors

Bugs

While credentials are a convenient way to gain access, they are not the only way.
Another way of gaining access is to exploit the vulnerabilities in the systems themselves.
The vulnerability may be misconfiguration of the system. Such as leaving default passwords unchanged, allowing backwards compatibility to older protocols, and so on.
The bugs are errors in the code, that allow a malicious actor to force the system to behave in ways it is not supposed to behave.
Often the bugs and vulnerabilities will come with a way to exploit them. This may be an exploit code, like those found in metasploit framework. Or be embedded in some malware like ransomware that uses these vulnerabilities to propagate through the network.
By exploiting the vulnerability the malicious actors can crash, run arbitrary code on, or escelate their privileges on a system.

You may hear about the 0day, a 0day is a vulnerability that is not yet publicly known and is freely exploitable. Once a vulnerability is discovered, developers rush to develop updates to their software to patch it. An unknown vulnerability will not be patched until it is made known to the developers and is therefore is a very valuable asset.

Vulnerabilities: How Bad Can It Be Really?



Base Metric Group

Exploitability metrics

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction

Impact metrics

- Confidentiality Impact
- Integrity Impact
- Availability Impact

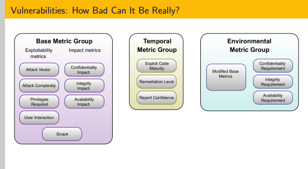
Scope

Temporal Metric Group

- Exploit Code Maturity
- Remediation Level
- Report Confidence

Environmental Metric Group

- Modified Base Metrics
- Confidentiality Requirement
- Integrity Requirement
- Availability Requirement



Vulnerabilities: How Bad Can It Be Really?

How bad the vulnerability depends on a number of factors.
For example a vulnerability that requires a legitimate user to do something (like click a link, run a program) will be less severe than one that doesn't require any user interaction.
A vulnerability that can be exploited remotely will be more severe than one that requires physical access.

Availability of exploit code in the wild will make the vulnerability more severe. While official patch will make it less severe.

Closing the Vulnerabilities

Update your software

Update your operating system

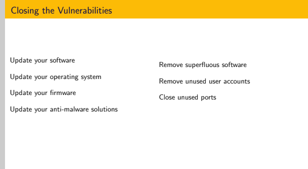
Update your firmware

Update your anti-malware solutions

Remove superfluous software

Remove unused user accounts

Close unused ports



Closing the Vulnerabilities

Update your software

Update your operating system

Update your firmware

Update your anti-malware solutions

Remove superfluous software

Remove unused user accounts

Close unused ports

Whether you are a big organization or a high-school student it is good advice to keep your systems up to date.

Another consideration is to reduce the attack surface. Remove the software, accounts, and ports that are not strictly necessary for the functioning of the system. Each additional piece of software is a potential hotbed of bugs and vulnerabilities.

For corporations there may be additional controls that are viable such as air-gaping critical systems, or monitoring network traffic.