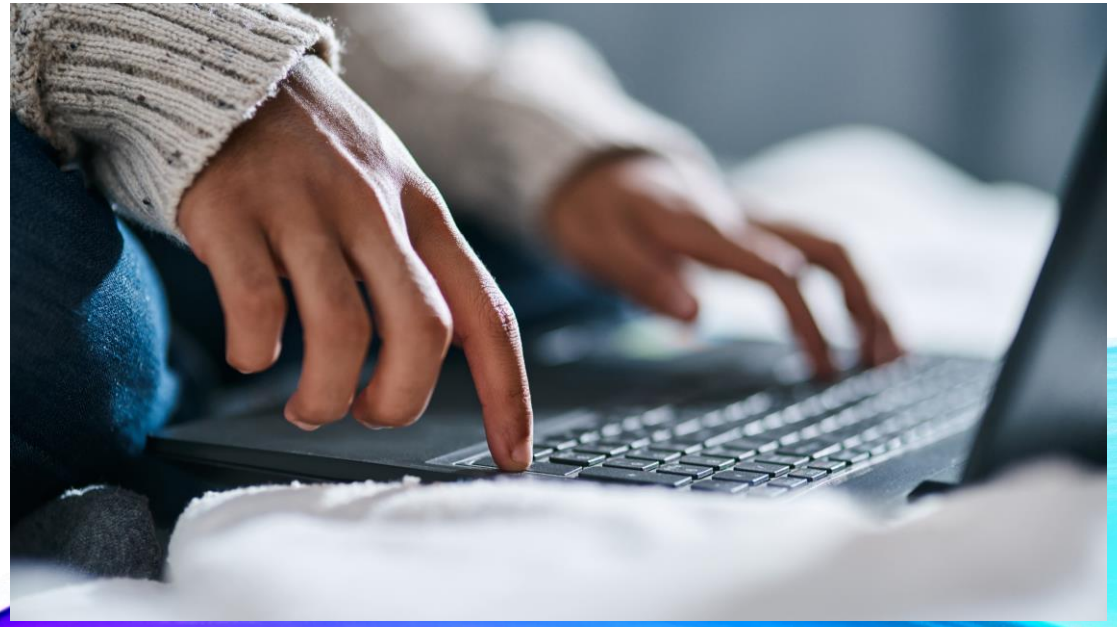
Harper College

ETHICAL HACKING LECTURE

Ravindra Das



THIS COURSE IS ABOUT AN AREA OF CYBERSECURITY THAT IS KNOWN AS “PENETRATION TESTING”. THIS IS WHERE AN INDIVIDUAL OR AN ENTIRE TEAM WILL GO FORWARD AND BREAK DOWN THE ENTIRE WALLS OF DEFENSES FOR A CLIENT WHO HAS REQUESTED SUCH A TEST.

BUT, AS IT WILL BE EXPLORED LATER IN THIS CLASS, THIS IS ALL DONE WITHIN THE CONFINES OF THE LAW, WITH THE FULL PERMISSION OF THE CLIENT. THUS, IT HAS RECENTLY BECOME KNOWN AS “ETHICAL HACKING”

BEFORE WE GO ANY FURTHER, IT IS FIRST IMPORTANT TO DEFINE SOME TERMS THAT DRIVE AN ETHICAL HACKING TEST. THEY ARE “VULNERABILITY” AND “EXPLOITATION”.

VULNERABILITIES VS EXPLOITATIONS

A Vulnerability can be technically defined as follows:

“Weakness in an information system, system security procedures, internal controls, or implementation.”

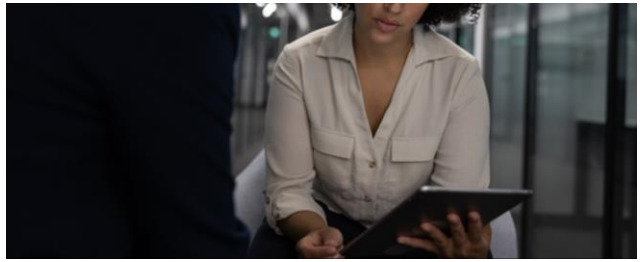
SOURCE: https://csrc.nist.gov/glossary/term/vulnerability

An Exploitation can be technically defined as follows:

“An exploit is a program, or piece of code, designed to find and take advantage of a security flaw or vulnerability in an application or computer system.”

SOURCE: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html

So, as you can see, a Vulnerability is a weakness, which is either known or unknown, gap, or weakness, in a software application, server, wireless device, or even a server. Once the Cyberattacker has determined what they are when they have profiled their victim, they then make their way into this gap to further Exploit it. From here, they will typically deploy a malicious payload to cause further damage.

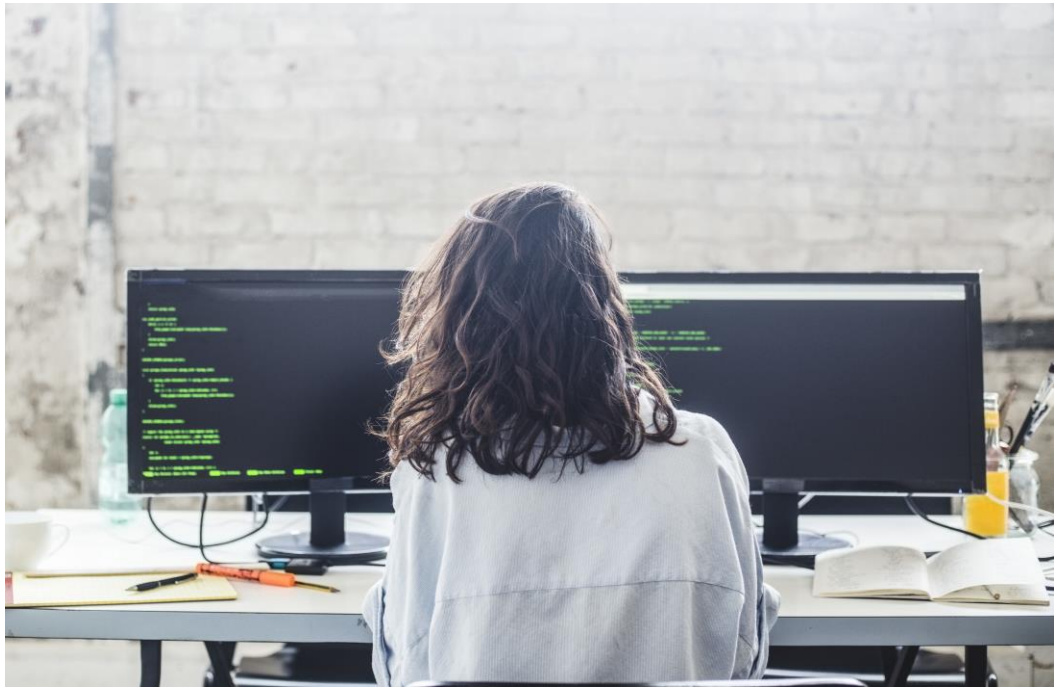


THUS, THE PRIMARY GOAL OF ETHICAL HACKING IS TO CONDUCT A SERIES OF TESTS IN ORDER TO ASCERTAIN WHERE THESE GAPS AND WEAKNESSES ARE AND PROVIDE RECOMMENDATIONS TO THE CLIENT AS TO HOW THEY FIXED, WITH THE PRIMARY MISSION OF FIXING THEM AS QUICKLY AS POSSIBLE.

A TECHNICAL DEFINITION OF ETHICAL HACKING IS:
"ETHICAL HACKING IS THE PRACTICE OF PERFORMING SECURITY ASSESSMENTS USING THE SAME TECHNIQUES THAT HACKERS USE, BUT WITH PROPER APPROVALS AND AUTHORIZATION FROM THE ORGANIZATION YOU'RE HACKING INTO."
SOURCE: HTTPS://WWW.COURSERA.ORG/ARTICLES/WHAT-IS-ETHICAL-HACKING

AS YOU CAN SEE, THE ETHICAL HACKING TEAM WILL TAKE THE MINDSET OF AN ACTUAL CYBERATTACKER, IN AN ATTEMPT TO FIND ALL THE WEAKNESSES THAT ARE POSSIBLE.

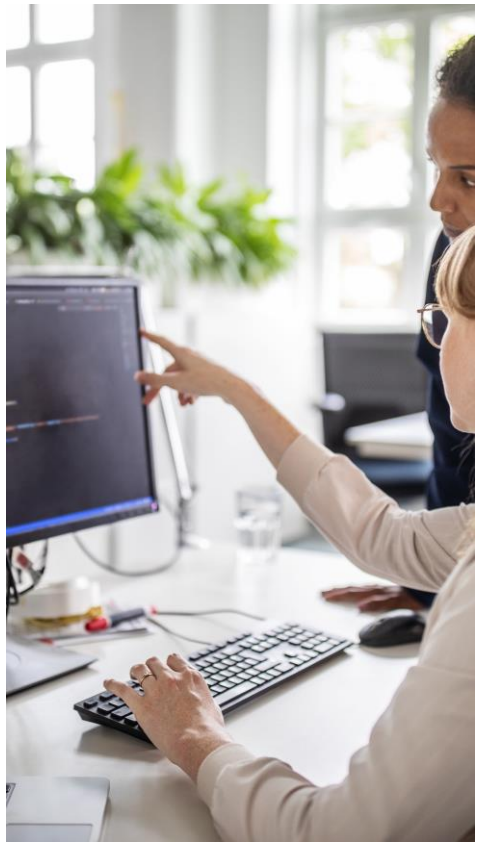
ETHICAL HACKING CHECKS

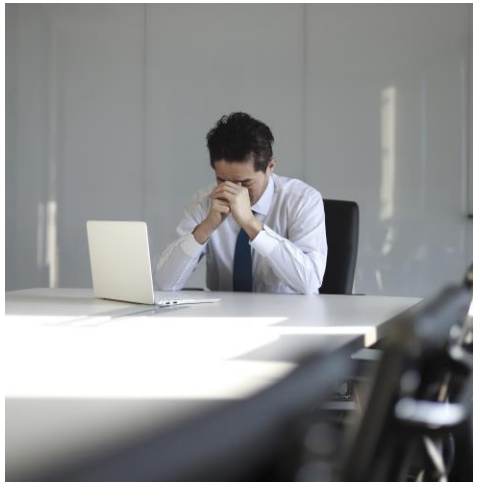


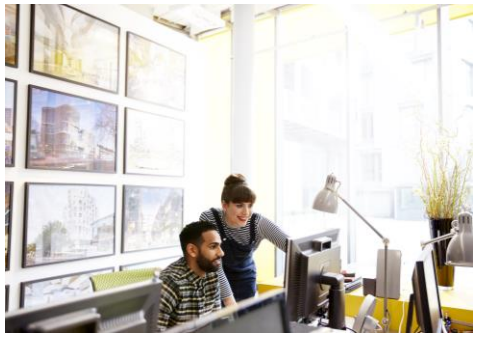
- Any business, no matter how large or small they are, can benefit from having an Ethical Hacking exercise conducted, as threat variants keep growing exponentially, and are even that much more difficult to detect.
- Probably one of the biggest threat variants that illustrates the need for Ethical Hacking has been the recent Solar Winds attack.
- Solar Winds is a large software company that creates and deploys network monitoring tools.
- They have many customers that rely upon their software packages, in order to fully keep up with the optimization of their IT and Network Infrastructures.

ETHICAL HACKING CHECKS CONTINUED

- One of the software packages of Solar Winds is called "Orion". In it, there was an undetected weakness that the Cyberattacking group was able to discover, and from there, they were able to deploy a malicious payload.
- Thus, once a customer had downloaded this particular software package, they were infected with this malicious payload.
- The most amazing thing about this Cyberattack is that it actually first occurred on December 8th, 2019, and was not noticed until over a year later, on December 12th, 2020.
- In fact, over 1,000 customers were impacted by this malicious payload.



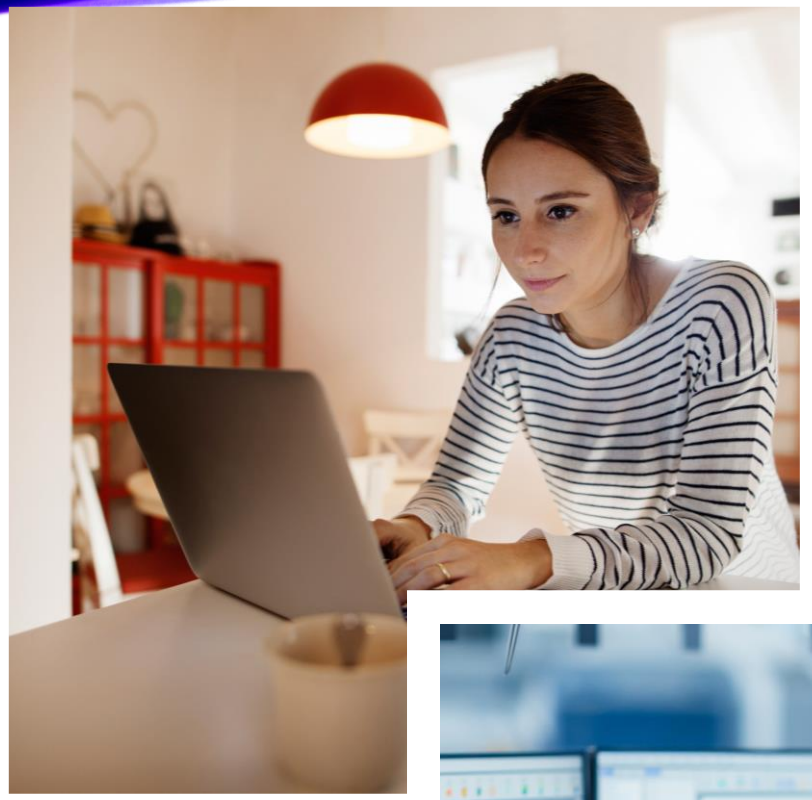


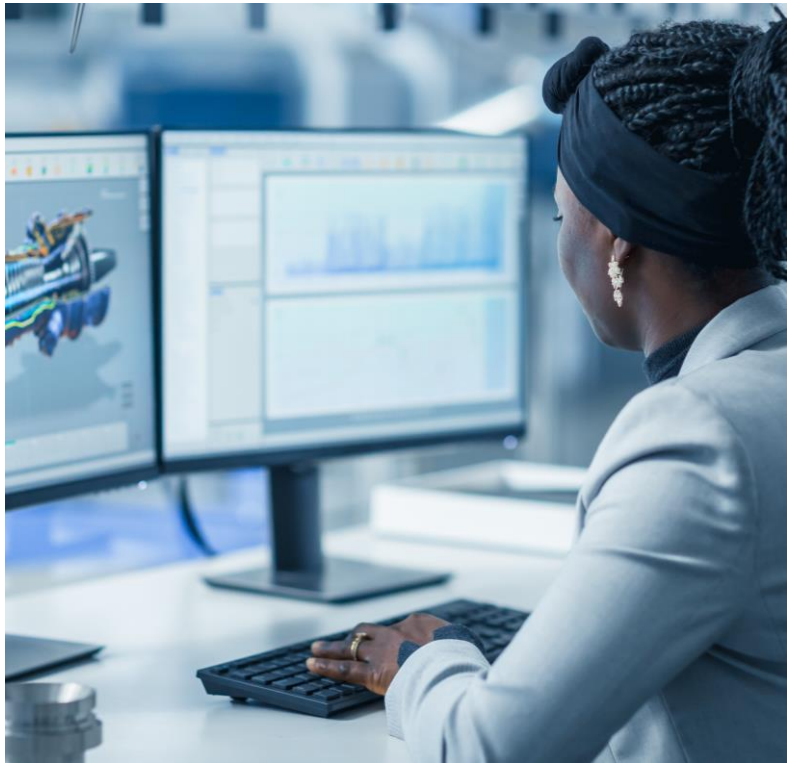


HERE IS A SAMPLING OF WHO WAS IMPACTED:

US Department of Commerce	Department of Defense	Department of Energy	Department of Homeland Security
Department of State	Department of the Treasury	Microsoft	Intel
Cisco	Mount Sinai Hospital	Ciena	NCR
SAP	Regina Public Schools	Public Hospitals Authority, Caribbean	INSEAD Business School
DenizBank			

Harper College





LONG-TERM EFFECTS:

- As you can see, the victims ranged from the Federal Government to the Fortune 100, schools, non-profit organizations, and much smaller businesses.
- But apart from the magnitude of damage that was created, another unique aspect is that this hack was termed as a "Supply Chain Attack". It can be technically defined as follows:
- "A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain."
- SOURCE: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/supply-chain-attacks/
- In the case of Solar Winds, they were a trusted third party that their customers depended upon for software packages, Through just a few vulnerabilities the Cyberattackers were able to inflict a large amount of damage. Had an Ethical Hacking exercise been conducted, the chance of this actually happening would have been greatly mitigated.

PENETRATION TESTING & ETHICAL HACKING

It was mentioned at the beginning of this course that Penetration Testing is also known as “Ethical Hacking”.

The primary reason for this is that Ethical Hacking must be done within the direction of the client and the confines of the law.

Both the client and the Ethical Hacking take this very seriously. For example:

A contract is very carefully created and signed between the Ethical Hacking team and the client. This strictly enforces as to what can and cannot be done. This is something that cannot be done arbitrarily, very often a lawyer is involved in this process.

SAFEGUARDS FOR ETHICAL HACKING:

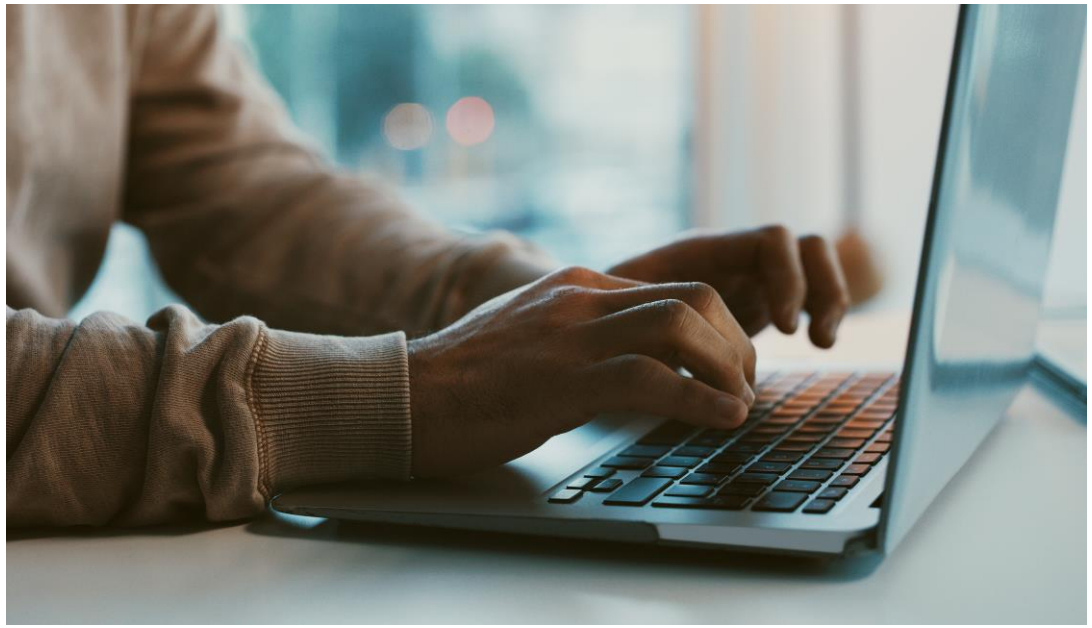
- If the Ethical Hacking team feels that more targets need to be examined in the exercise, they must have explicit and written consent from the client. Further, this has to be an addendum to the signed contract.
- Although the Ethical Hacking team will be highly professional and knowledgeable in what they do, there are instances when mistakes can happen. Therefore, the contract must also stipulate that the client must maintain backups before and during the exercise.
- Although it is not required by law, most Ethical Hacking teams do carry insurance, which is known as "Errors and Omissions".
- An example of a contract can be seen at this link:

http://cyberresources.solutions/Harper_College_CE/Campbell%20Companies_App&PT%20SOW_2024.docx

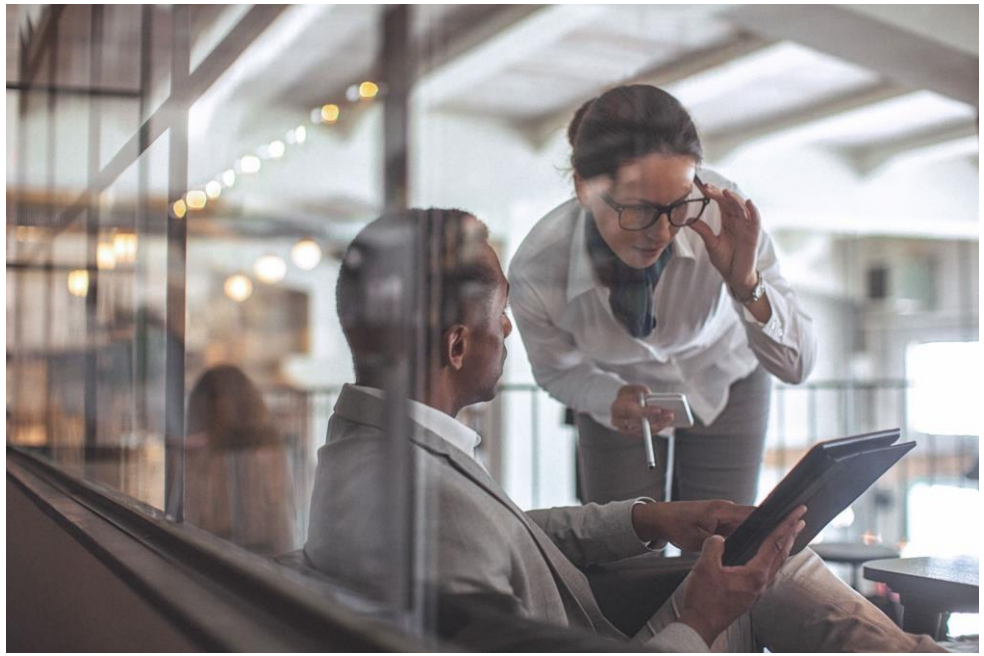
Harper College

ETHICAL HACKING TEAM:

- Once the contract has been signed and the targets have been selected for further analysis, the Ethical Hacking exercise can commence.
- Depending upon the depth of the examination, only one or two Ethical Hackers may do it, or even an entire team of individuals.
- But the common denominator is that the Ethical Hackers will have different titles associated with them, such as:
- **The Red Team:** These are people that try to break down the walls of defense established by the client. They typically work from the external environment inwards.



ETHICAL HACKING TEAM, CONTINUED:



- **The Blue Team:** These are the “Good Guys”. They work in concert with the IT Security team of the business in order to try to fend off the Red Team.
- **The Purple Team:** This team is a combination of the Red and Blue Teams. It has members from both and is typically deployed to serve as a balance between the two.
- The traditional model of Ethical Hacking has been to do the needed tests on site. But since the COVID19 pandemic, most of the tests are now done remotely, with the interactions taking place with the client over a video conferencing platform, like Zoom, Teams, etc.

ETHICAL HACKING TESTS:

There can be many types of Ethical Hacking exercises that can be conducted, when it comes to digital assets. Here is a sampling of them:

- **Web Application Testing:** This is where Ethical Hackers test the front end (the actual GUI) and the backend (the database) for any weaknesses. Also, any APIs that are used to bridge the two together are also tested.
- **External Testing:** This is where the Perimeter Lines of Defenses are tested. For example, this will include network security devices, such as the Firewalls, Network Intrusion Devices, Routers, etc.
- **Vulnerability Scanning:** This is not as sophisticated as an Ethical Hacking exercise is, as it is considered to be a "passive test", and primarily tests for open network ports.

ETHICAL HACKING TESTS, CONTINUED:

- **Dark Web Monitoring:** The Dark Web is that part of the Internet that is publicly visible. This can be viewed as the "Underworld", where a lot of criminal activity happens. Whenever datasets are stolen, they are typically sold here. As a result, many Ethical Hacking teams have now devised ways to penetrate the Dark Web, to see if your information has been stolen.
- **Wireless Testing:** This is where all sorts of devices can be tested, both from the hardware and software sides. Examples include tablets, laptops, iOS and Android devices, etc.
- **Source Code Testing:** This is where the underlying software code makes up an application. Of particular interest here is to check for any back doors that have been left open by the software development team.

PHYSICAL ETHICAL HACKING EXERCISES:

Ethical Hacking teams can also conduct exercises to see how well the Physical Security of a business is doing. Examples of this include:

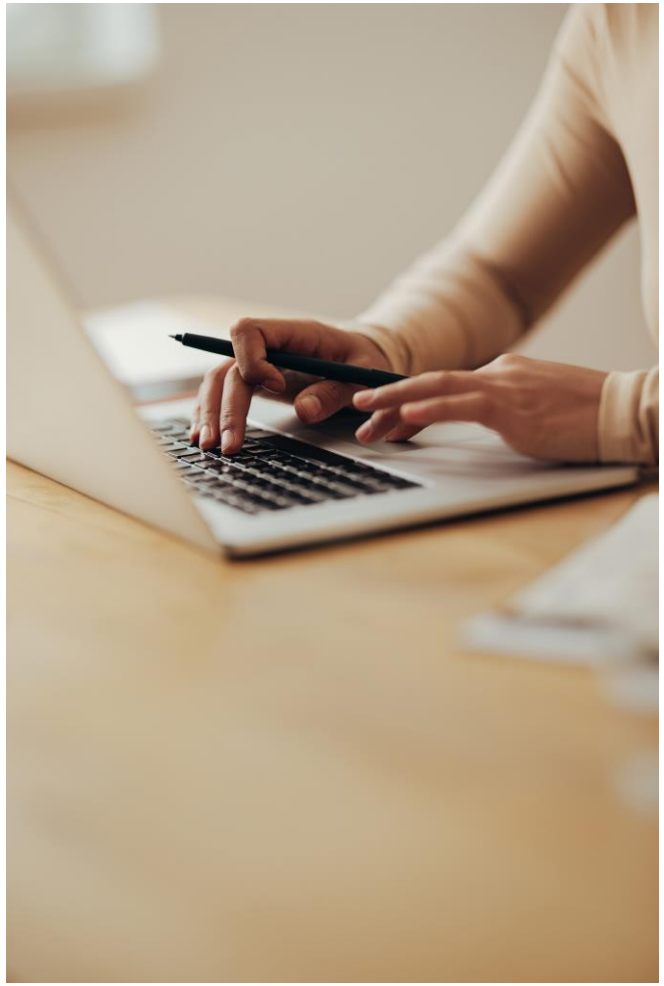
- Seeing how proactive they are in making sure that only authorized personnel can enter into the physical premises of the business.
- Seeing how easily employees fall prey to Social Engineering Attacks.
- Conducting surveillance activities from within the physical confines of business.

PHYSICAL ETHICAL HACKING EXERCISES, CONTINUED:

Of particular interest to Ethical Hackers are the following:

- **Dumpster Diving:** This is where anybody from the public can scour through the garbage bins of a business, in search of any information that can be exploited. At the present time, there are currently no laws against this.
- **Shoulder Surfing:** This is where an employee will covertly look over the shoulders of a co worker to see what they are doing on their workstation, in the hopes of finding something that they can steal and use it for nefarious purposes.

ETHICAL HACKING TOOLS:

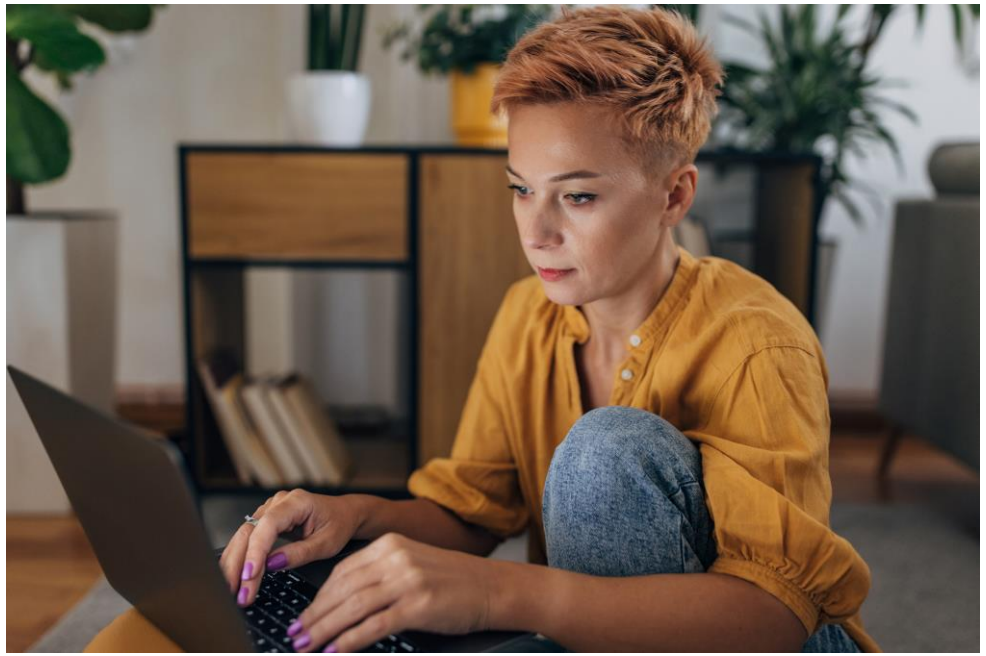


Along with their own toolsets, Ethical Hackers have a wide array of software platforms that they can use when conducting their tests. Some of the most widely used ones include the following:

- **Kali Linux:** This is a different variation of the Linux OS, and it is open source. It is probably amongst the most popular tools that is used today by Ethical Hackers. Also, it can be used for conducting Digital Forensics examinations.
- **Burp Suite:** This is a tool used primarily for probing the gaps in web-based applications.
- **Wireshark:** This is used for examining network traffic, and searches for any anomalies which exist.
- **John The Ripper:** This is a platform which can be used to test how weak passwords are. It can also be used to launch a “Dictionary Attack” against a database. This is where all sorts of naming combinations are launched, in an effort to see how easy it is to crack a password database.

ETHICAL HACKING TOOLS, CONTINUED:

- **Nmap:** This is stands for “Network Mapping” and is quite often used to map out the entire Network Infrastructure of the client, before embarking on an Ethical Hacking exercise.
- **Metasploit:** This is deemed to be one of the most powerful platforms available, and it can be used to create further, customized tools, and produce new ideas as to what should be further tested.
- **Nessus:** This is a tool that can be used to test for vulnerabilities in devices, applications, operating systems, cloud services and other network resources.
- **SQL Map:** This is used to test vulnerabilities in SQL databases, such as SQL Server and MySQL. It is primarily used to test to see how vulnerable these databases are to a SQL Injection Attack.



ETHICAL HACKING METHODOLOGY:

The methodology of an Ethical Hacking exercise will differ of course upon the needs of the client and the nature of the tests to be conducted. But in general, the methodology can be defined as follows:

Reconnaissance:

"The tester acquires as much data as they can on the target system during this phase, including details about the user accounts, operating systems, and applications, as well as the network topology."

SOURCE: https://www.centraleyes.com/glossary/penetration-testing/

Discovery:

"The Ethical Hacker employs a variety of tools during this phase to find open ports and examine network activity on the target system. Ethical Hackers must find as many open ports as they can in order to prepare for the subsequent penetration testing phase because open ports are potential points of entry for attackers."

SOURCE: https://www.centraleyes.com/glossary/penetration-testing/

ETHICAL HACKING METHODOLOGY, CONTINUED:

Vulnerability Analysis:

"Ethical Hackers can use a variety of tools to assess the risk of vulnerabilities found at this stage."

SOURCE: https://www.centraleyes.com/glossary/penetration-testing/

The tools mentioned in the above definition are those that were just reviewed in the lecture.

Exploitation:

"Exploitation begins when vulnerabilities have been found. The Ethical Hacker makes an attempt to get access to the target system and exploit the vulnerabilities found during this phase of testing, generally by simulating actual attacks with a program like Metasploit."

SOURCE: https://www.centraleyes.com/glossary/penetration-testing/

ETHICAL HACKING METHODOLOGY, CONTINUED:

Maintaining the presence:

"The objective here is to determine whether the flaw can be used to establish a persistent presence in the system being exploited—long enough for a malicious actor to obtain in-depth access."

SOURCE: https://www.Centraleyes.Com/glossary/penetration-testing/

When it comes to an actual security breach, these are also known as "advanced persistent threats".

Reporting:

"The tester creates a report summarizing the results of the penetration test when the exploitation phase is over. The final penetration testing phase's report can be used to close any security holes detected in the system and strengthen the organization's security posture."

SOURCE: https://www.Centraleyes.Com/glossary/penetration-testing/

The exact components of the final report to the client will be reviewed in the next slides.

ETHICAL HACKING FINAL REPORT:

Once the Ethical Hacking exercise has been completed, a final report is usually submitted to the client. Each report will vary, but in general, they contain the following sections:

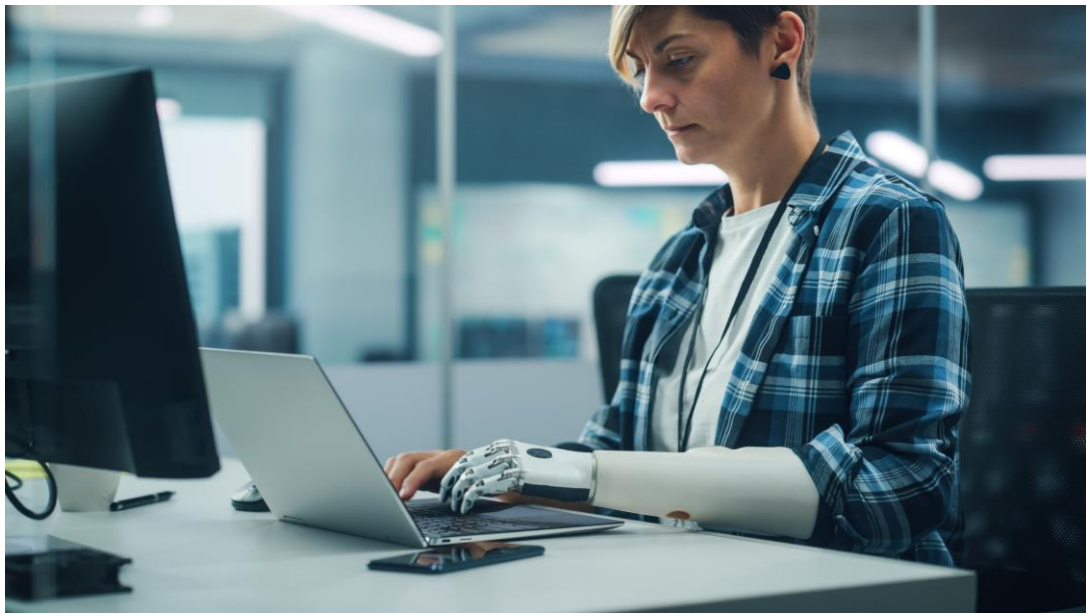
- The Executive Summary
- The Targets That Were Selected.
- What Kinds of Penetration Testing Were Conducted
- The Methodology As To How The Testing Was Done
- The Penetration Tools That Were Used: Typically, these will be the software packages that have been used, as reviewed earlier.

ETHICAL HACKING FINAL REPORT, CONTINUED:

- The Vulnerabilities That Were Discovered: This will include both the digital and physical assets that were tested.
- The Degree Of Severity Of The Discovered Vulnerabilities: Typically, an Ethical Hacker will use some sort of numerical scale, such as 1-10. In this case, “1” would be those assets that are least vulnerable, and “10” would be those assets that are most vulnerable.

ETHICAL HACKING FINAL REPORT, CONTINUED:

- Which Vulnerabilities Should Be Addressed First: Typically, it will be those digital and physical assets that are ranked as moderate to most severe. These of course will need the highest priority, and from there, the others will follow.
- The Remediation Plan for Correcting The Vulnerabilities: Typically, this section will describe what remediated actions need to be taken in order to fix the gaps and vulnerabilities that were discovered.
- Recommendations On How To Move Forward: This is typically the last section of the report. In it, the Ethical Hackers will provide a way as to how the remediative actions should be carried out. Very often, they will refer the client to either a Managed Services Provider (MSP) or a Managed Security Services Provider (MSSP) to deploy the needed controls.
- An example of an actual final report submitted to a client can be seen at the link below:
- http://cyberresources.solutions/Harper_College_CE/Pen_Test_Client_Report.pdf



- As was reviewed earlier in this class, Ethical Hacking has always been traditionally done on a manual basis, with some automation being done for the more repetitive tasks.
- This can be done with a scripting language, such as Perl, PHP, Ruby On Rails, or even Python.
- But with the explosion of Generative AI, there has been a very strong movement amongst the Cyber Vendors and Ethical Hackers to now have tools to be completely automated, with no human intervention whatsoever involved in the testing exercise.

There are advantages and disadvantages to this. For example:

- A manual Ethical Hacking exercise can cost upwards of up to $30,000 or more for just one test.
- With a tool that is powered by Generative AI, you still pay a substantial fee, but with that, it is an annual license, so you can run as many Ethical Hacking exercises as needed, without additional expense.
- One such example of this is an Ethical Hacking Vendor known as “Horizon3.ai”. They have a platform called “Node Zero”, and for about $50,000.00, you can get an annual license for unlimited testing.
- But the question arises just how reliable is it to have an Ethical Hacking platform that is totally “autonomous and automatic”?

In my view, you need both in order to deliver a high-quality product to the client, especially when it comes to the final report, and making the recommendations as to how to proceed further.

In this regard, Generative AI can be used to add more sophistication to automating those repetitive tasks where the traditional scripting languages have been used.

Also, Generative AI can be used to augment the thought processes of all the Ethical Hackers that are involved in conducting the exercise.

THANK YOU

This concludes our course. I am always available if you ever need help with anything on this topic or have further questions.

The best way to get me is via email, which is: Ravindra.das@harpercollege.edu

SLIDES CREATED BY ADEE MARKETING

Transparent Marketing with Integrity

If you are looking for help creating professional presentations, please do not hesitate to reach out. 224-908-7434 or Info@adeemarketing.com

Harper College