A Study on the Motivations and the Techniques Used to Find, Conduct Reconnaissance On, and Infiltrate Computer Systems

Justin Tyler Hungerbuhler  
Mike Cottrell College of Business  
University of North GeorgiaDahlonega GA, USA  
jthung0726@ung.edu

*Abstract*—The motivations and techniques used to conduct reconnaissance on, scan, and infiltrate computer systems are a major worry for Cybersecurity professionals. Hackers have a variety of motivations and techniques that they use to find, conduct reconnaissance on, and infiltrate computer systems. At each step of the infiltration process, hackers use different tools and techniques when exploiting computer systems. The techniques used by hackers are constantly evolving and becoming more sophisticated. Cybersecurity professionals are in a constant arms race with hackers to prevent and block hackers from gaining access to computer systems. In order to do this Cybersecurity professionals must know how any why hackers go after their targets.

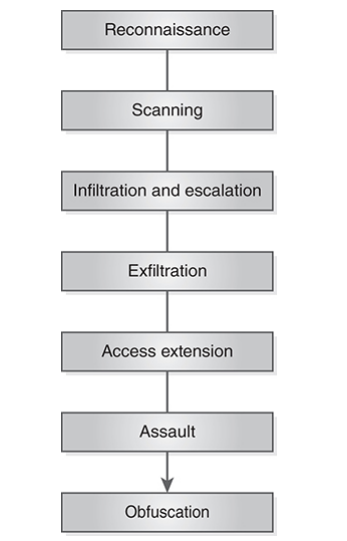
Keywords—hacker, hacker techniques, hacker motivations, computer reconnaissance, computer scanning, computer infiltration

# Introduction

Computers have become an integral part of our lives and economy and if they were shut down then the economy would shrink, and our lives would be harder. The term hacker or Cybercriminal is well known at this point, but it does little to describe their allegiance and motivations. A hacker is someone who gains unauthorized access to a computer system or its data. When describing hackers, they must be separated into different types based on their motivations and their targets. Cybercriminals typically search for vulnerable software used in the network infrastructure, which is readily accessible and easy to compromise; they exploit bugs or loopholes in infrastructure programs, without modifying the systems [7]. Then they use specialized criminal techniques that attack the operating systems, networks, databases, and other system applications of these sites and software, to affect the behavior of infrastructure computers. [7]. Malicious and Ethical hackers is the two categories of hackers that will be covered in the discussion section.

A lot is already known about hackers and how much damage they do to computer systems. This is shown by the weekly news articles of which company or organization was hacked and has their private information released or sold to the highest bidder. Because every company and organization uses computers and the internet in some capacity, they are all vulnerable to data theft and/or sabotage. It is predicted that cybercrime will cost in excess of 10.5 trillion USD annually by 2025 [6]. This high cost includes the amount paid in ransoms and how much is spent in preventing and responding to cyberattacks.

In the Background I will provide a generalized overview of the current Cybersecurity environment that professionals and hackers deal with. In the Discussion I will go deeper in depth of the motivations of hackers and the first 3 steps in the hacking process that is shown in Figure 1. In the Conclusion I will use all of the information collected from my sources and my knowledge to make some final conclusions about the current Cybersecurity environment.

Figure 1: Hacking steps (Hacking methodology) [5].

# Background

When a hacker attempts to attack a computer system, they must follow a set of steps they created or that they learned when becoming a hacker. There is no one specific step-by-step approach that all hackers use [5]. A major difference between a malicious hacker and an ethical hacker is the code of ethics to which each subscribes [5]. A Malicious hacker is a generalized name for hackers that attack computer systems for financial or social gain. More specific name types that are under this title include: Black hat, Gray hat, Script kiddies, Botnet hackers, Cryptojackers, State-sponsored hackers, Hacktivists, and Cyberterrorists. Ethical hacker is

a generalized name for hackers that attack computer systems under a contract and the written permission of the owner of the computer. Another specific name type that is under this title includes White hat, Red hat hackers.

Reconnaissance is when an attacker passively acquires information about the intended victim and/or the intended victim’s systems..., and potential exploratory contact with the victim [5]. Scanning is when an attacker uses the information from the reconnaissance step and uses it to get detailed information about a target’s computer network. One of the goals is to identify weaknesses in target systems and this can result in lists of users, groups, applications, configuration settings and other similar information [5]. Infiltration and escalation is when a hacker used information from the previous steps to exploit one or more identified vulnerabilities in the computer system [5]. The goal of this phase is for the hacker to gain access to a system that manages access to the computer’s data so they can escalate access privileges to allow them to move freely around a system or computer environment. After the hacker has the necessary privileges, they can then conduct the next phases of the attack.

Even though I will only cover the hacking steps that involve how hackers gain access to a computer and/or computer network; I will provide details on the next four steps a hacker should follow in order to stay out of prison as long as possible and get the most they can from a target. Exfiltration is when an attacker uses their unrestricted access to a computer or network to access protected software and data. This is where the attacker extracts data, modifies or deletes sensitive files, or obtains configuration information [5]. If a hacker just wants the data, this is where they stop, or they can go to Obfuscation to hide the infiltration. For most hackers, they continue onto the next step because their goals require them to complete all of the steps.

Access extension is when an attacker implements a backdoor into a computer or network that they just infiltrated to more easily regain unrestricted access to the data and software now on the computer network. If they fail to implement a silent method of access using rootkits or similar tools, then the backdoor they implemented can only be used a few times before it is discovered and removed.

I have put Obfuscation before Assault because if a hacker hides how they infiltrated the computer network before they start the Assault then there is a higher chance they can attack the computer again. Obfuscation is when the attacker modifies log files and other artifacts of their activities or installs additional malware to erase any traces of their presence [5]. Obfuscation is not a step that is done by every hacker. Most hackers should hide their actions because it takes 277 days (9 months) on average for the breach to be discovered [3]. This time allows for a hacker to hide from authorities and better hide their attack. The only time Obfuscation is not done is when a hacker wants to bring attention to their cause by news companies covering the attack.

Assault is when the computer network is attacked by the hacker to cause damage to the computer’s data or physical damage if possible. Assault is usually done after a hacker finishes their work on collecting and ex-filtrating data from the computer network. One way Assault is done is by removing or modifying critical configuration files to alter the way in which a computer or device operates [5]. This attack type can devastating because computers don’t work if not configured correctly. This is not a necessary step if the hacker wants to remain hidden and not attract attention to themselves. A hacker can't do both the Assault and Obfuscation steps because they are mutually exclusive. The only time obfuscation can occur is when a hacker wants to hide specific information about themselves (location of the hacker, how they entered the network, etc.)

# Discussion

## Motivations

Depending on what type of hacker, they had a different list of potential targets and reasons why they wish to attack a specific target. Criminal hacking is usually designed to target the largest possible number of victims in order to increase the chances that someone will click on a malicious link or mistakenly transfer money [11]. Money is one of the largest motivations of many types of hackers. Hackers perceive a low level of social sanction, a high level of severity punishment from the court, but a low likelihood of getting caught and receiving the punishment [12]. Hackers also perceive a relatively high utility value resulting from engaging in illegal hacking activities [12]. Hackers believe that they will not be caught for their actions, but if they do get caught, they will be punished harshly. In addition, hackers will not be punished by the people they rely on, and they will get lots of value out of their hacking targets. The following is the list of hacker types that are popular: White hat, Black hat, Red hat, Gray hat, Script kiddies, Botnet hackers, Cryptojackers, State-sponsored hackers, Hacktivists, and Cyberterrorists.

White hat hackers may hack for financial gain or to make computer systems more secure from attacks from malicious hackers. White hat hackers do this work by preforming penetration tests against a computer network and reporting the results of the test back to the organization who contracted them to preform the test. A White hat hacker may have similar techniques to black hat hackers, but they find and report security vulnerabilities to governments and businesses and advise them on ways to patch the exploit to prevent cyberattacks.

A Black hat hacker could attack anyone and uses ransomware, spyware, and phishing techniques to break into computers and networks. Black hat hackers are motivated by money and financial gain...and, while they may take a warped kind of professional pride in a job well done, they tend never to be caught or even come to the attention of the authorities [8]. Black hat hackers are experts in their field, do most of the hacks, and some of the highest profile hacks. They may also be hired under contract by an organization to do any of the hacking tasks that are done by the other hacker types.

A Red hat hacker is like a white hat hacker, but they differ from them by going after black hat hackers by using social engineering techniques to stop or disrupt their activities [10]. Any attempt to slowdown or stop some malicious hackers have saved people, and organizations money and/or their information. Red hat hackers have played a role in the capture, and identification of Black hat hackers.

A Gray hat hacker is like a black hat hacker, but attacks computers and networks for fun but they may also demand payment for the details for the exploit they discovered. The primary motivation is sheer curiosity...They like to discover things on the Internet [1]. Gray hat hackers hack because they can, and it is their favorite thing to do, like how many people have side projects.

Script kiddies are inexperienced hackers, and use existing malware and tools to attack computers and networks and they can make a profit off of the data. They go to Internet chat rooms to swap information about hacking tools and pass on stories [1]. This can increase their skills past what they get from using tools to eventually become a Black hat hacker.

Botnet hackers use thousands to millions of hijacked computers called bots/minions that are pre-programmed to do actions from the hacker [10]. The bots steal or compromise information on the infected computer and/or take control of the computer and they can infect over a network very quickly.

Cryptojackers use social engineering techniques to carry out cryptocurrency scams. Cryptojackers have used a Trojan to get control over victims computers to steal cryptocurrency wallet credentials [10]. Cryptojackers are similar to a Black hat hacker but they are different because Cryptojackers steal cryptocurrency which in someplace/websites is another usable currency.

State-sponsored hackers are contracted by a government to attack computers and networks belonging to rival governments and/or companies in rival nations. These are the most well funded and highest skilled group of hackers and do most of the highest profile attacks against rival nations.

It takes time and a lot of people and money to find where the vulnerabilities exist...and it requires different skill sets [4]. With money, you can have more people looking across platforms at more vulnerabilities, at more ways in which you can attack and break things [4]. State-sponsored hackers are resource rich, so they have the funds to attack any target and hire any hacker to assist in that effort. State hackers are more likely to have a particular high-value target in their sights and, as such, will often dedicate more time and effort to finding an entry point [11]. Because State-sponsored hackers are employed by a state and care less about fast profit they can take the time to find an easy entry into a target network.

Hacktivists are hackers that hack in order to attract attention to their political or social cause by attacking organizations that oppose the Hacktivists cause. They employ certain types of attack vectors (SQL injection, web server misconfiguration, DDoS, social media account compromises, etc.) to take over databases and leak their contents which may contain sensitive and private information, deface high-profile websites, disable widely-used public services, send fake news or posts containing phishing/malware/trojan links to a large follower audience which can help them gain the attention of public and authorities to give publicity to their cause [9]. Because they want the hack they did to become known they do anything needed to accomplish that, and hide their location so the cause can continue to spread.

Cyberterrorists are hackers that use their hacking techniques to attract attention to their cause by disrupting information systems [10]. These Cyberterrorists have the same goals as regular terrorists; where they attempt to attack the highest profile targets possible to maximize the attention they get without regard to who may get injured. Hacktivists and Cyberterrorists may have similar goals and one nation’s Hacktivists could be another’s Cyberterrorists. The thing to know, is both hacker types seek government or policy change and they may continue until their demand is met.

## Reconnaissance

Reconnaissance is the phase where hackers narrow down their list of potential targets. When hackers are looking for a target to attack there is much they need to look for. Because Reconnaissance is the passive collection of information about a target that is not secret to the organization; it is easier to collect. This is called Footprinting: the gathering of information about a

target site (its computer systems and

employees) by passive means without the

organization’s knowledge [5]. A hacker is required be look for information about a target on lots of websites and using many tools. For a hacker to be willing to enter an organization’s network they should obtain the following information: information from general resources, Determining the network’s logical and physical

dimensions [5]. A Hacker should do this step passively (Not interacting with any of the organization’s staff or password protected systems) because this interactions may be reported to their Cybersecurity team and will be expecting an attack and will have a shorter response time to the attack; reducing the amount of data the hacker could obtain. Footprinting may be the easiest

part of the hacking process because most

organizations generate massive amounts of information that is made available online [5]. This data can be found across the internet from their websites, Google, blogs, social media, news articles, interviews, and many more other places.

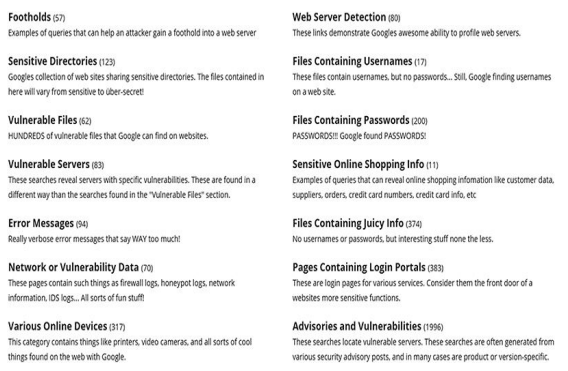
HTML code is an easily overlooked part of any website that could reveal sensitive information. A HTML comment may look harmless, but it may tell an attacker the name of the server that is being accessed and/or its password, thus assisting in targeting an attack [5]. Even if any sensitive information is removed from the website before it can be exploited it may still be found on third party websites. The most well-known is the Internet Archive’s Wayback Machine. This tool takes screenshots of a wide variety of websites at a variety of times a day. This means that any information stored in the websites HTML code must be changed and not included in any future versions of the website. The most popular websites get imaged daily many times a day while less popular ones are imaged once or twice weekly.

Job postings are another information source providing insight into what the company happens to be using at the current time [5]. They can use information to attempt to fine-tune a later attack, doing some research and locating vulnerabilities such as: Vulnerabilities in the discovered products, Application-specific configuration issues and Product-specific defects [5]. Any information in job postings must be limited to not include any information about the current software or structure of the computer network.

Financial Information may seem innocuous but Cybersecurity professionals should know that these publicly available financial records show how much a company makes [5]. This allows Black hat hackers to narrow down the target list to only companies that make more than a million US dollars to make thousands or millions off of the attack. Because the data must be public under US law at www.sec.gov and can’t be sanitized it does allow companies to know how much they should invest in Cybersecurity products. i.e. organizations that spend and make millions of dollars must have a larger Cybersecurity budget than organizations that spend, and make less than a million.

Google Hacking/Search Engine Hacking is using properly constructed queries in order to find information or files on a website that was indexed by the search engine but not easy to find by clicking around the website. This is most commonly done on Google but can be done on any search engine to find as much information as possible [5]. This is abusing how the search engines are supposed to work. This works because

Google indexes vast amounts of information in an untold numbers of formats [5]. Google can also index images, videos, discussion group postings, and all sorts of file types; such as PDF, PPT, and more. All the information that Google, or any other search engine, gathers is held in mind-numbingly large data stores that are designed to be searchable; you only need to know how to look [5]. To solve this exploit the website, and the sensitive data stored on it must be built to not be easily indexed by a search engine.

Figure 2: Google Hacking Database (GHDB) [5]

The Google Hacking Database (GHDB) at www.offensive-security.com/community-projects/google-hacking-database/ is one site that lists query templates that identifies sensitive data and content [5]. By customizing the template, the hacker can now have a query the hacker can then find information listed in the Figure 2. These queries and variations are powerful information-gathering mechanisms that can reveal

information that may not be so obvious or accessible normally [5]. Cybersecurity professionals must understand how a query finds information and experiment with the tools. Only then can they develop solutions to prevent sensitive information from being located using this method.

A necessity for doing a cyberattack is knowing basic information about the target organization uses and can be found in their registration of an Internet domain. The following information can be found using the following methods: Whois was designed to query databases to look up and identify the registrant of a domain name. Whois information contains the name, address, and phone number of the administrative, billing, and technical contacts of the domain name; Nslookup is used find information about a resource stored in the Domain Name System (DNS), including domain name, DNS server, List the MX (mail) server for a specific range of IP

Addresses, and IP address(es); Internet Assigned Numbers Authority (IANA) and regional Internet registries (RIRs) record the range of Internet Protocol (IP) addresses that an organization has access to; Traceroute is used determine the location of the network. This is done by displaying the list of routers on a path to a target network destination (specific IP address) by using time-to-live (TTL) time-outs and Internet Control Message Protocol (ICMP) error messages [5]. Collecting this information is a requirement because a hacker needs to know where the target is to know if they might attack the wrong target in the process. This information can also be collected using automated tools that include but are not limited to: [www.betterwhois.com](http://www.betterwhois.com/) and [https://whois.domaintools.com](https://whois.domaintools.com/). This information is damaging to the organization’s computer network so it should be as generic as possible.

Social media posts by employees talking about their work could reveal sensitive information about the organization that hackers could use in their footprinting of the organization. Leadership at the organization should create systems, to prevent the sharing of sensitive information about the organization and check in on employees of important systems of the organization.

## *Scanning*

Scanning is the phase where the target list is reduced even further. This is done by using information from the reconnaissance step and using more advanced tools to collect more detailed information about a target’s computer network. This is the step that involves actively communicating with the target’s computer network. The information collected in that step can include IP addresses of active computers connected to the internet, open ports on those active computers, and active services running on those active computers that use those ports.

Ping sweep is the technique used to determine whether a computer is connected to the network and active [5]. This is used to know if any of the computers found from the reconnaissance step are connected to the internet. Because a computer will only respond to a ping request with a ping reply or echo; it is quickly sent and responded to. The following information can be learned from a ping request: identify active machines and measure the speed at which packets are moved from one host to another and time to live (TTL) [5]. This information is useful to a network administrator to know how a computer is operating. Because of how easy this scanning feature is, Cybercriminals usually do this first to see if a computer is online to connect to. Network administrators usually block Internet Control Message Protocol (ICMP) messages, because of how easy it is to send ICMP messages by a firewall, and may be notified of a ICMP message by an intrusion detection system (IDS) or intrusion prevention system (IPS). Before doing a ping sweep hackers should know that network administrators will be notified that a ping sweep was done or was attempted on their network. This means that the administrators will have a higher alertness level than before the ping sweep attempt.

Nmap is the best known port-scanning tools and can use multiple techniques and

includes a very useful operating system fingerprinter which is useful in determining which vulnerabilities your victim may have [2]. Nmap is versatile and can run using a command line or GUI. Nmap is also run-able on almost every operating system. Nmap is a very versatile tool that is capable and will continue to be a useful tool.

Nessus is an excellent tool, providing a capability as a vulnerability scanner with a client/server architecture [2]. One excellent feature is that it does not assume any defined bindings for ports and services (e.g. HTTP is normally situated at port 80 but may be it at ports in the 8000 range) [2]. If administrators move ports around, they can still be identified [2]. It is simple to move services from the default port to a lesser used port to reduce the likelihood of cyberattacks. Nessus makes this hiding attempt pointless; because it is advanced enough to find out what service is running on any particular port. Nessus is getting updates frequently and gets new frequently to make Nessus more capable.

D. *Infiltration and escalation*

Infiltration and escalation are the phase of hacking where the best target in the target list is selected for Infiltration and attack. The information from the last two steps is used to find a vulnerable computer or website portal, and once that is done, it is attacked using any method. Everything possible should be done by Cybersecurity professionals and network administrators to enable and have every possible precaution possible which includes a firewall, IDS, and IPS.

Password crackers are one of the simplest ways to gain access to an account protected by a password. There are various methods that are used by hackers to crack passwords which include: Social Engineering, Brute-Force Attacks, Dictionary Attacks, Hybrid Attacks, and Rainbow Tables. Social engineering methods can also be used to obtain a password based on trust or ignorance on the user’s end...alarming number of users will comply and provide their passwords to a “trusted” individual [5]. Social engineering is effective; because we believe others to be honest and not to have bad intentions. This can be combined with phishing, which relies on social engineering to entice the victim to respond and provide their credentials [5]. Phishing through emails, texts, or messages is one of the most common ways to have your password stolen. This is done by tricking you though a variety of feelings from fear to excitement. Brute-Force attacks function by attempting all possible combinations or a suspected subset of possible passwords [5]. Brute force has the benefit of always working, but the downside is that it takes a long time [5]. Brute-Force attacks aren't always the best tool because of the long attack time, and because passwords on long lists of previously hacked passwords are usually used again on other websites, and this allows for a faster attack. Dictionary attacks are similar to the last attack type in that all combinations are tried, but different cause an attacker reads the list of passwords looking for hashes that match the hashed values of words in the dictionary [5]. This attack type is faster because of the reduced number of possible combinations, but it can still be detected and blocked by the website because of the number of login attempts. This is usually the first type hackers use because of the large number of previously hacked passwords. Hybrid attacks start out like a dictionary attack, in which different combinations of words from the dictionary are attempted; if this is unsuccessful at uncovering the password, the process changes [5]. In the next phase of the attack, characters and symbols are added to the combinations of characters to attempt to reveal the password [5]. This type is a bit slower than a dictionary attack because of the increased combinations, but it can take advantage of any incorrect or improper use of salting.

Rainbow tables compute hashes using every possible combination of characters within some range prior to capturing a password [5]. It takes a long time to compute the large number of combinations, but after using them they can be reused. Once all the hashes have been generated, the attacker can then capture the password hash from the network and compare it with the hashes that have already been generated [5]. This is a very fast and simple step that can usually finish in under a minute.

In the early days of Web access, Secure Socket Layer (SSL) encryption seemed to stop hackers from doing anything, but they soon found out that SSL is only one component in an E-commerce system [2]. Session hijacking is the hijacking of a SSL session, and stealing of cookies in order to assume control over already logged in websites. This method of attack is simple to attempt only requiring a malware latent file to be run on a target computer for the Internet browser’s cookies to be stolen and sent back to the hacker to then be used to access websites the target was logged into and steal data or do as much damage as possible to the target. While this is an assault method it can also be used to infiltrate if access is gained stealthy enough and the hacker can gain complete access over the computer and network using other tools. One example of this damage has been shown the last few years with the hijacking of many YouTube channels to show a live stream of the same Elon Musk and Tesla video, while asking that channels views to send money or cryptocurrency to the address in the chat or in the live stream's description.

Rootkits are commonly used by Cybercriminals to attack computers and networks. Rootkits are collections of tools that give hackers administrator-level access, or ‘root’ access, to computer systems [7]. Rootkits incorporate malware, such as Trojans, worms, and viruses, which conceal its presence and activity from users and other system processes [7]. Rootkits and the malware types contained inside are given many purposes but are helpful in the infiltration and escalation steps because of their effectiveness in completing this step.

An organizations Cybersecurity Team should prevent the use of any Insecure Applications like Telnet, File Transport

Protocol (FTP), Post Office Protocol (POP), Hypertext Transfer Protocol (HTTP), and Simple Network Management Protocol (SNMP) because they have no encryption and can open a backdoor into the network.

After a hacker has infiltrated a computer or network, they may not be using an administrator or high-level access account so they must get an account that has less restrictions and use tools to give it more permissions. This is called privilege escalation, and this is the first goal of a hacker after they get access to a target’s computer because the account they hacked may not be able to do everything the hacker wants to do with the computer. One way to escalate privileges is to identify an account that has the access desired and then change the password [5]. There are several tools that offer this ability, including the following: Active@ Password Changer, Trinity Rescue Kit, ERD Commander, Recovery Console [5]. Because administrator accounts have higher security the best way to get access to those accounts is to use a tool to change the password on those accounts after logging in user a lower-level account. This is made easier because of the large amount of lower-level accounts and their weaker security.

# Conclusion

## Conclusion

A constant review of how and why hackers conduct reconnaissance on, scan, and infiltrate computer systems is required. Each of the hacker types have their own goals in their hacking attempt. The potential targets of hackers have and will change over time, but their goals will remain the same. This means that companies and government agencies must constantly review who the current targets are and compare that data with the identities of previous hacking targets. In the last 30 years hackers have made a lot of gains in their techniques and the wide variety of tools available. Reconnaissance is the step of public and open-source intelligence, and tools for this don’t require communication with the target’s computer network. Scanning requires direct interaction with the target’s computer network, and tools used in this step find vulnerabilities and services in the target’s network. Infiltration and escalation have hackers exploit the vulnerabilities found in the target’s computer network to access their data, and also to gain administrate control to do any action. Hackers must also keep up to date with companies and government agencies to know when a tool or technique has been identified and neutralized. Malicious and Ethical hackers bring different effects to society, with Ethical hackers making us safer, while Malicious hackers cause a lot of damage. Companies and organizations must keep up to date with the current and future hacking communities to know how and why they attack computer systems. If they don’t or fall behind their competitors, then they will inevitably be hacked, and they might lose market share and profit. This is especially true if they are an internet-based company. For as long as we use computers to do or assist us in doing tasks; we will have hackers attempt to attack and steal from those computers.

##### References

1. Barber, R. (2001). Hackers Profiled — Who Are They and What Are Their Motivations? *Computer Fraud & Security*, *2001*(2), 14–17. https://doi-org.libproxy.ung.edu/10.1016/S1361-3723(01)02017-6

1. Barber, R. (2001). Hacking Techniques: The tools that hackers use, and how they are evolving to become more sophisticated. *Computer Fraud & Security*, *2001*(3), 9–12. https://doi-org.libproxy.ung.edu/10.1016/S1361-3723(01)03014-7
2. IBM. (2022, July). *Cost of a data breach 2022*. IBM. https://www.ibm.com/reports/data-breach
3. Mansfield-Devine, S. (2018). Nation-state hacking – a threat to everyone. *Computer Fraud & Security*, *2018*(8), 17–20. https://doi-org.libproxy.ung.edu/10.1016/S1361-3723(18)30077-0
4. Oriyano, S., & Solomon, M. (2018). *Hacker Techniques, Tools, and Incident Handling, 3rd edition*.
5. Owen, K., & Head, M. (2023). Motivation and Demotivation of Hackers in Selecting a Hacking Task. *Journal of Computer Information Systems*, *63*(3), 522–536. https://doi-org.libproxy.ung.edu/10.1080/08874417.2022.2081883

1. Rege, P. A. (2009). Cybercrimes against critical infrastructures: a study of online criminal organization and techniques. *Criminal Justice Studies*, *22*(3), 261–271. https://doi-org.libproxy.ung.edu/10.1080/14786010903166965
2. Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, *3*(2), 97–102. https://doi-org.libproxy.ung.edu/10.1016/j.diin.2006.03.001
3. Samuel Chng, Han Yu Lu, Ayush Kumar, & David Yau. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*, *5*(100167-). https://doi-org.libproxy.ung.edu/10.1016/j.chbr.2022.100167
4. Stouffer, C. (2023, June 28). 15 Types of hackers + hacking protection tips for 2023 [web log]. Retrieved July 4, 2023, from https://us.norton.com/blog/emerging-threats/types-of-hackers.
5. Vincent, A. (2017). State-sponsored hackers: the new normal for business. *Network Security*, *2017*(9), 10–12. https://doi-org.libproxy.ung.edu/10.1016/S1353-4858(17)30113-7
6. Young, R., Zhang, L., & Prybutok, V. (2007). Hacking into the Minds of Hackers. *Information Systems Management*, *24*(4), 281–287. https://doi-org.libproxy.ung.edu/10.1080/10580530701585823