

## Fact sheet: Hacking

### Definition criminal hacking:










Criminal hacking means finding out weaknesses in a computer software or computer networks and exploiting them for profit, protest, sabotage terrorism, cyber war. In this fact-sheet we focus on the risk of criminal hacking. This means that the hackers never have permission to perform their illegal activities on the network of entities.

This definition has been derived from the hacking definition on Wikipedia.


### Starting point:

The starting point of this hacking fact-sheet is the assumption that you will get hacked, sooner or later.<sup>i</sup> Getting hacked is certain and organizations should proof that they have appropriate control measures in place to detect intrusions early. The goal of these control measures would be to detect the hack early and reduce the time a hacker has available to compromise the entire network of a specific target. According to Debora Plunkett, even the NSA considers its networks compromised.<sup>ii</sup>

The goal for the victims (organizations) would be to correlate several sources of evidence that usually are already present within a organization and detect intruder attempts as early as possible. These sources should be analyzed based on malicious threat indicators and events. Usually these indicators are called indicators of compromise or IOC's. These initial sources of evidence are among others<sup>iii</sup>:

-  Firewall logging
-  Network traffic (Netflow data)
-  Intrusions/Extrusion detection systems logging
-  Mail and messaging (spam) logging
-  Host intrusion prevention systems logging
-  Web application logging (logfiles web servers)
-  Anti-virus logging
-  System and Security logging (Authentication logging)
-  Proxy logging

 DNS logging

 Remote access/ VPN logging

These initial sources of evidence can be used to create a better visibility on malicious activities by hackers on the network of the organization. We assume that these sources are active and present in most organizations. If these sources are still unavailable implement them. Within large organizations usually a Security Information and Event Management (SIEM) solution is chosen to analyze and correlate security events based on the sources mentioned above. Usually SIEM technology provides real-time analysis of security alerts generated by network and/or software applications.

## Autonomy of a hacking attack (The five P's):<sup>iv</sup>

A hacking attack consists of several phases in which a hacker or hacker group can reveal its interest for a particular organization. These phases are:

1. Probe
2. Penetrate
3. Persist
4. Propagate
5. Paralyze

The several phases of an attack and their common control measures are described briefly below.

The autonomy of an attack described below can be confirmed by the personal experience of the authors of this fact-sheet.

### Probe

In this phase an attacker gathers intelligence about its target. This phase is also known as reconnaissance of the target. This means the attacker tries to gather as much information about the network, people (social media) and web services as possible, in order to find vulnerable services or systems. In this phase an attacker usually scans the network with port scanners, web application scanners (sql mapping, DirBustering<sup>v</sup> etc) originating from multiple IP-addresses. Usually an attacker sends e-mails with web bugs or links to a group of employees working at a specific target. The goal of these harvesting e-mails is to determine which security measures are active at a specific target. Is a proxy server in place and which spam and anti-virus software is used is valuable information for a hacker. This information can be used by the hacker to avoid detection of the malware the hacker uses on the specific target.

General Control measures:

1. Make sure that Service Level Agreements exist that address an obligation to notify whether the service provider is hacked and sensitive data was obtained.
2. Make sure software that is used is up-to-date!
3. Make sure time is synchronized on the network equipment, servers and workstations.
4. Implement secure coding and configuration principles.
5. Have a computer security incident handling process in place <sup>vi</sup>

Specific Control measures:

1. Continuously analyze and correlate IP-addresses used by attackers (from the different sources off evidence like the firewall logging, ids logging, spam, anti-virus and web application logging)
2. Continuously block suspicious IP's and alert providers or organizations via abuse messages and monitor on the origin.
3. Inspect if these suspicious IP-addresses can already be linked to malicious activities.
4. Report serious hacking attempts to Nationaal Cyber Security Centrum (NCSC), the former Govcert.
5. Security Awareness training should address the risks of being openly exposing sensitive information on the Internet. Make clear that everything what's on the web will stay on the web for a long time.
6. Employees should have the ability to report security incidents to the internal or external security organization.
7. Analyze the output of the hacker probes to learn what he has learned, either by inspecting the log files or run the tools yourself on the systems.

## Penetrate

A result from the Probing phase are vulnerable servers, interesting targets (people). The next thing an attacker does is to penetrate the network. The attackers usually uses a lot of different IP-addresses that already been discovered. From recent incidents it can be learned that most of the cybercriminals possess multiple Botnets of controlled or compromised servers. A hacker usually uses different methods to obtain his goal, obtain sensitive information, profit etc. A hacker could choose to penetrate a target for a very short period thus evading detection if he reached his goal by the initial penetration.

The list below gives an insight on penetration methods used by hackers:

1. Brute force authentication services

A hacker may try to brute force certain services to obtain access by just guessing known user name and password combinations.

## 2. Exploiting programming errors/Buffer overflows

Sometimes software is not programmed correctly and its user input is not checked or sanitized correctly. If these vulnerabilities are detected by a hacker by for example fuzzing methods he can control the program flow and will usually insert his own carefully crafted malicious code, usually referenced as the payload. These malicious inputs are designed to execute malicious code or alter the way a software program operates. If the hacker can control the buffer (Instruction Pointer) he can execute every command. For example a hacker can dump user accounts with passwords or establish a reverse shell to the hacker controlled system.

Buffer overflows crash affected services or programs running on computer systems.

## 3. Exploiting application logic flaws

A hacker can use different techniques. A known technique that a hacker will use if the Probing phase is delivered that result is to test if it's possible to traverse directories or use different encoding techniques for a (../). Path traversals of remote or local file inclusions usually can be detected in web server logging.

## 4. System configuration errors

Too often networks, computers or network services are still configured badly which can expose sensitive information to a hacker and will be used by them. An example of these configuration errors are Simple Management Network Protocol with the default "public" community string or printers with a web server that is accessible via the internet and leaking sensitive information or is being used as a jump server to access the network further.

## 5. User input validation problems

Like buffer overflows, one of the most common hacking methods is called SQL-injection. Within SQL injection the input supplied by the user is not validated properly. This is also due to unsafe programming. If a hacker detected this in the Probing phase, he starts by exploiting it. Cross-site scripting (XSS) is also known attack method.

## 6. Phishing

Phishing is an efficient method in obtaining user credentials from employees by creating a malicious copy of the original website. The attacker will send e-mail messages try to convince users to log on the malicious website, stealing their credentials in the process.

### Spear Phishing

This method is known as a targeted attack where the hacker created a list of specific persons within the organization and will send them a custom e-mail with a malware attachment or a link to an malicious website where users will get infected by just browsing that malicious website. This method is also known as drive by hacking or drive by exploiting.

## 7. Physical Attacks

These types of attacks could involve distributing USB sticks with malware infected software on parking lots, symposia. Also WI-FI attacks are common methods to gain access to the network. Furthermore a cyber criminal could gain physical access to the office or home networks of persons of interest.

General Control measures:

1. Implement corporate error reporting<sup>vii</sup>
2. Secure coding and configuration principles (never trust anything a user or other process tells you)
3. Implement ICT technology that leaves forensic traces of user activity on data carriers. If you make use of thin client technology (Citrix, RDP), be sure to implement a compensating control on user, security and system activity monitoring.
4. Implement a security awareness program where users are taught in detecting the signs of malicious activities like phishing or spear phishing.
5. Regularly perform pentests on the entire infrastructure of the organization. Detect and address the weakest spots in the security. Also perform pentest on the strength of the control measures, like the quality of anti-virus scanners or intrusion detection systems for example.
6. Audit on how quick a new network intrusion signature can be created and implemented within the network. This in order to create more visibility on the hacker and compromised hosts within the corporate network.

Specific Control measures:

1. Continuously analyze and correlate IP-addresses used by attackers (from the different sources off evidence like the firewall logging, ids logging, spam, anti-virus and web application logging).
2. Analyze malware found on client computers or in spam and anti-virus control measures.
3. Continuously block suspicious IP's and alert providers or organizations via abuse messages and monitor on the origin of the IP's.
4. Inspect if these suspicious IP-addresses can already be linked to malicious activities.
5. Report confirmed intrusions to the Dutch National Police and Nationaal Cyber Security Centrum (NCSC).
6. Notice and takedown procedures<sup>viii</sup>.
7. Investigate the cause of unexpected crashes from services and computer systems and whether these events are related to hacking attempts.

## Persist

In this phase the hacker has been successful in exploiting a serious weakness in some vulnerable application, network service or outdated software version. The intruder often starts by using webshells like AspxSpy or http tunneling software like ReduH to give him a convenient access method to the compromised server. One of the first things an intruder usually does is retrieve administrator accounts by dumping passwords from the compromised server or network infrastructure. This means within Windows environments usually executing password tools like pwdump or gdump on Domain Controllers. Also the tools, Wireshark, Hyena and Sysinternals tool collection is encountered often in forensic cybercrime investigations. In Linux/Unix environments the hacker retrieves the passwords stored in the known shadow files or from NIS databases. Next the intruder will try to crack these passwords with tools like John the Ripper or Ophcrack on the systems.

After the administrator passwords are cracked the intruder can use these compromised accounts to backdoor the network further. Also the creation of backdoor accounts is standard procedure for a hacker. Usually the hacker installs multiple backdoors or custom malware that communicate with different command & control servers within the compromised network or the Internet. During this usually strange DNS-requests will be made to suspicious domains. In this phase it often occurs that systems will be rebooted by the attacker or eventlog files will be deleted.<sup>ix</sup> For more information about specific control measures see the malware fact-sheet.

General Control measures:

1. Setup a separate logging mechanism where security logging is stored on a secured server. This is necessary to preserve the integrity of the logging in case a hacker deletes its footprints, like eventlogs etc..

Specific Control measures:

1. Perform forensics and malware analyses on the malware found on compromised servers.
2. Analyze network traffic on indicators of compromise.
3. Blackhole certain and discovered malicious malware domains within DNS.<sup>x</sup>
4. Change passwords from the users.
5. Create lists of compromised accounts and compromised hosts.
6. Analyze relevant log files, like security eventlogs, DNS, network dumps (pcap) or outbound traffic.
7. Create new network signatures for the intrusions detection systems.

## Propagate

The next phase the attacker will try to do is to establish more control and try to control more segments of the compromised network. If the infection is for example a malicious worm the worm will try to infect as many systems it can connect to. Usually the hacker tries to install malware on as much servers he has access to. Usually the malware will be installed by regular system administration tools like, psexec from Sysinternals.

## Paralyze

This is the final stage in a targeted attack where an hacker reveals his true motivations of the attack. Is he interested in obtaining classified information, steal money or disrupt mission critical business services. This could be done by deleting critical components which could disturb the continuity of a mission critical server. For more information about Denial of services see the DDoS fact-sheet.

## Top 5 recommendations for the IT auditor:

See the recommendations in the malware fact-sheet.

1. Test the early warning signs to detect hacking in the Probing and Penetration phase.
2. Audit the response mechanisms when a hack is detected: incident response and escalation.

## Conclusion:

Most of the hacks can be detected early if a victim organization understands the signs of being hacked. Usually a lot of information is available in different log files of various services during the first stages of Probing and Penetrating. From our experience we know that most if not all of these signs are being overlooked from extended periods of time. This period could be several weeks of even years. It should be the main goal to integrate the logging information already present in the organization and to correlate them on signs of a compromise. If such a framework of controls is present and functions properly the window of the hacker will be detected in an early stage.

## Key documentation and website links:

<http://www.owasp.org>

<http://www.sans.org/top25-software-errors>

- 
- i Planning for failure, November 2011, Forrester report for Security and Risk professionals
  - ii NSA considers its networks compromised, <http://www.net-security.org/secworld.php?id=10333>
  - iii Of course there are other sources of evidence, like servers, computers, (e-mail) databases etc.
  - iv Managing Security with Snort & IDS Tools,  
[http://onlamp.com/pub/a/security/excerpt/SnortandIDSTools\\_chap1/index.html](http://onlamp.com/pub/a/security/excerpt/SnortandIDSTools_chap1/index.html)
  - v DirBuster is a tool to brute force directory and file names on web or application servers. Sqlmap is a tool to automate sql injections flaws.
  - vi NIST SP 800-61 Revision 1, Computer Security Incident Handling Guide
  - vii Microsoft Corporate Error Reporting, [http://download.microsoft.com/download/5/9/2/592d2308-a6a2-48ad-ae8f-72f888b9d361/CER\\_Implementation\\_Plan.pdf](http://download.microsoft.com/download/5/9/2/592d2308-a6a2-48ad-ae8f-72f888b9d361/CER_Implementation_Plan.pdf)
  - viii <https://www.cpmi.nl/projecten/notice-and-take-down>, The notice and takedown procedure involves four steps:
    1. Signaling from certain illegal or malicious content on the Internet.
    2. Notice the intermediary party involved
    3. Assessment of the report
    4. Action (Take-down)
  - ix This behavior is often seen in cybercrime hacking cases where the authors of this fact-sheet were involved in.
  - x <http://www.malwaredomains.com/bhdns.html>, A list of domains that are known to be used to propagate spyware or malware are loaded into internal dns servers. When an infected computer is requesting these discovered malware domains a fake reply is sent.