Gather information about the systems before the vulnerability assessment. At least review if the device has open ports, processes and services that shouldn’t be opened. Also, understand the approved drivers and software (that should be installed on the device) and the basic configuration of each device (if the device is a perimeter device, it shouldn’t have a default administrator username configured).

Gather public information and vulnerabilities regarding the device platform, version, vendor and other relevant details.

Use the right policy on your scanner to accomplish the desired results. Prior to starting the vulnerability scan, look for any compliance requirements based on your company’s posture and business, and know the best time and date to perform the scan. It’s important to recognize the client industry context and determine if the scan can be performed all at once or if a segmentation is needed. An important step is to re-define and get the approval of the policy for the vulnerability scan to be performed.

Best scan (i.e., popular ports)

CMS web scan (Joomla, WordPress, Drupal, general CMS, etc.)

Quick scan

Most common ports best scan (i.e., 65,535 ports)

Firewall scan

Stealth scan

Aggressive scan

Full scan, exploits and distributed denial-of-service (DDoS) attacks

Open Web Application Security Project (OWASP) Top 10 Scan, OWASP Checks

Payment Card Industry Data Security Standard (PCI DSS) preparation for web applications

Health Insurance Portability and Accountability Act (HIPAA) policy scan for compliance

What is Vulnerability Assessment?

VULNERABILITY ASSESSMENT is a process to evaluate the security risks in the software system in order to reduce the probability of a threat. It is also called Vulnerability Testing.

A vulnerability is any mistakes or weakness in the system security procedures, design, implementation or any internal control that may result in the violation of the system's security policy. The purpose of Vulnerability Assessment is to reduce the possibility for intruders (hackers) to get unauthorized access. Vulnerability Analysis depends upon two mechanisms namely Vulnerability Assessment and Penetration Testing(VAPT).

Advantages of Vulnerability Assessment

Open Source tools are available.

Identifies almost all vulnerabilities

Automated for Scanning.

Easy to run on a regular basis.

Disadvantages of Vulnerability Assessment

High false positive rate

Can easily detect by Intrusion Detection System Firewall.

Often fail to notice the latest vulnerabilities.

Inactive Testing, a tester introduces new test data and analyzes the results.

During the testing process, the testers create a mental model of the process, and it will grow further during the interaction with the software under test.

While doing the test, the tester will actively involve in the process of finding out the new test cases and new ideas. That's why it is called Active Testing.

Passive testing, monitoring the result of running software under test without introducing new test cases or data

Network Testing is the process of measuring and recording the current state of network operation over a period of time.

Testing is mainly done for predicting the network operating under load or to find out the problems created by new services.

We need to Test the following Network Characteristics:-

Utilization levels

Number of Users

Application Utilization

This post describes the key phases in the life cycles of Vulnerability Assessment and Penetration Testing. These life cycles are almost identical; Penetration Testing involves the additional step of exploiting the identified vulnerabilities.

It is recommended that you perform testing based on the requirements and business objectives of testing in an organization, be it Vulnerability Assessment or Penetration Testing. The following stages are involved in this life cycle:

1. Scoping

2. Information gathering

3. Vulnerability scanning

4. False positive analysis

5. Vulnerability exploitation (Penetration Testing)

6. Report generation

Stage 1 – Scoping

Scoping is the primary step of any security assessment activity. In order to execute a VA or PenTest, the first step is to identify the scope of the assessment in terms of infrastructure against which the assessment is to be conducted, for example, servers, network devices, security devices, databases, and applications.

Scoping depends on the business objective of the Vulnerability Assessment. During the scoping, a scanning window should also be agreed upon. Also, the types of attacks that are permitted should be agreed upon. After deciding on the scope of assessment, this phase also includes planning and preparation for the test, which includes deciding

on the team, date, and time of the test.

Another major factor that should be taken care of prior to beginning the engagement is signing a formal engagement agreement between the security tester and the party on whose infrastructure these tests will be performed. Scoping should also include identifying the count of infrastructure elements to be tested.

Apart from the infrastructure scope and other program management modalities, the exact scope, the organization’s approach to the business objective, and the methodology of the assessment should be decided. For deciding on the business objective, the organization should identify the type of attack that it would like to get mimicked.

An example of an objective that a company might seek is: “To find out what an external attacker can achieve by targeting externally exposed infrastructure with only the knowledge of a publicly exposed IP address.” This type of requirement will be met through an external Black box penetration testing of infrastructure and applications,

and the approach and the methodology should be in accordance with that.

Based on the accessibility of infrastructure from the Internet or intranet, the testing can be done from an external or internal network. Also, based on the type of details, the infrastructure testing can be Black box or Grey box. And depending on the type of infrastructure, the plugins or features of a vulnerability scanning tool should be enabled, aided by appropriate manual checks.

Stage 2 – Information gathering

Information gathering is the second and most important stage of a VA-PT assessment. This stage includes finding out information about the target system using both technical (WhoIS) and nontechnical passive methods such as the search engine.

This step is critical as it helps in getting a better picture of the target infrastructure and its resources. As the timeline of the assessment is generally time bound, information captured during this phase helps in streamlining the effort of testing in the right direction by using the right tools and approach applicable to target systems.

This step becomes more important for a Black box assessment where very limited information about the target system is shared. Information gathering is followed by a more technical approach to map the target network using utilities such as pings and Telnet and using port scanners such as NMAP. The use of such tools would enable assessors to find a live host, open services, operating systems, and other information.

The information gathered through network mapping will further validate information gathered through other passive means about the target infrastructure, which is important to configure the vulnerability scanning tool. This ensures that scanning is done more appropriately.

Stage 3 – Vulnerability scanning

This stage involves the actual scanning of the target infrastructure to identify existing vulnerabilities of the system. This is done using vulnerability scanners such as Nessus. Prior to scanning, the tool should be configured optimally as per the target infrastructure information captured during the initial phases.

Care should also be taken that the tool is able to reach the target infrastructure by allowing access through relevant intermediate systems such as firewalls.

Such scanners perform protocol TCP, UDP, and ICMP scans to find open ports and services running on the target machine and match them to well-known published vulnerabilities updated regularly in the tool’s signature database if they exist in the target infrastructure.

The output of this phase gives an overall view of what kind of vulnerabilities exist in the target infrastructure that if exploited can lead to system compromise.

Stage 4 – False positive analysis

As an output of the scanning phase, one would obtain a list of vulnerabilities of the target infrastructure. One of the key activities to be performed with the output would be false positive analysis, that is, removing any vulnerability that is falsely reported by the tool and does not exist in reality.

All scanning tools are prone to report false positives, and this analysis can be done using methods such as correlating vulnerabilities with each other and previously gathered information and scan reports, along with actually checking whether system access is available.

Vulnerability scanners give their own risk rating to the identified vulnerabilities; these can be revisited considering the actual criticality of the infrastructure element (server or network device) to the network and impact of the vulnerability.

Stage 5 – Vulnerability exploitation (Penetration Testing)

In case system owners require proof of existing vulnerabilities or exploits to understand the extent to which an attacker can compromise a vulnerable system, testers will be required to demonstrate exploits in a controlled environment with out actually making the infrastructure unavailable, unless that’s a requirement.

Penetration Testing is the next step to Vulnerability Assessment aiming to penetrate the target system based on exploits available for the identified vulnerabilities. For exploitation, our own knowledge or publicly available exploits of well-known vulnerabilities can be utilized.

Penetration Testing or Vulnerability Exploitation can be broadly divided into phases such as pre exploitation, exploitation, and post exploitation.

Activities in the pre-exploitation phase are explained in phases 1 to 4, that is, enumerating the infrastructure and identifying the vulnerability.

Once any vulnerability is exploited to gain access to the system, the attacker should aim to further detail the network by sniffing traffic, mapping the internal network, and trying to obtain a higher privilege account to gain the maximum level of access to the system.

This will enable testers to launch further attacks on the network to further increase the scope of compromised systems.

The post exploitation step will also involve clearing of tracks by conducting activities such as clearing logs and disabling antivirus.As a post-exploitation phase tester, you can demonstrate how an attacker can maintain access to the system through backdoors and rootkits.

Stage 6 – Report generation

After completing the assessment as per the scope of work, final reporting needs to be done covering the following key areas:

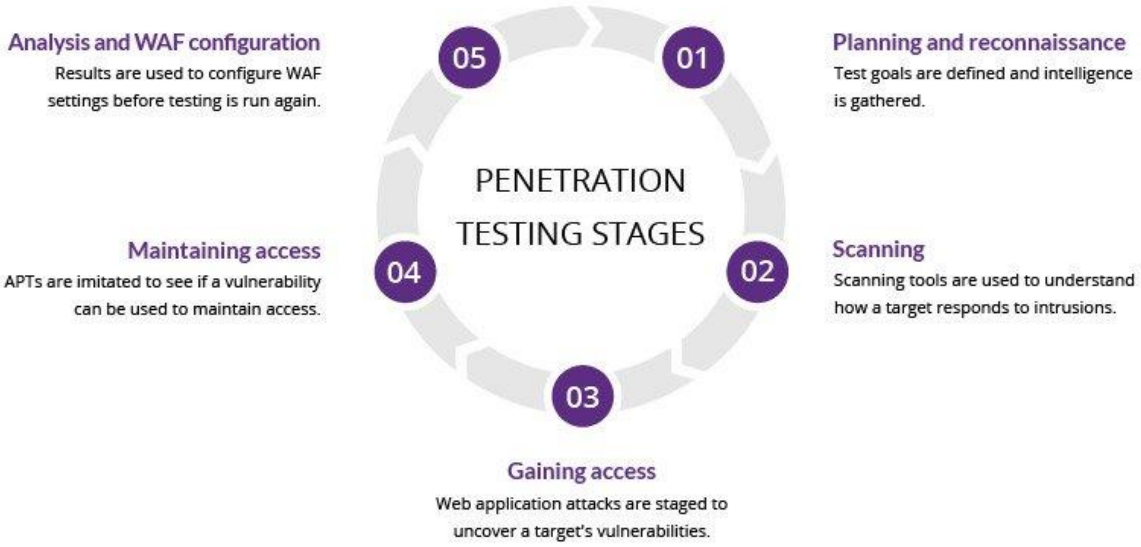
- A brief introduction about the assessment
- The scope of assessment
- The management/executive summary
- A synopsis of findings with risk severity
- Details about each finding with their impact and your recommendations to fix the vulnerability.

What is penetration testing

A penetration test, also known as a pen test, is a simulated cyber attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF).

Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

Insights provided by the penetration test can be used to fine-tune your WAF security policies and patch detected vulnerabilities.


PENETRATION TESTING STAGES
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.
04
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
05
Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

1. Planning and reconnaissance

The first stage involves:

Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used.

Gathering intelligence (e.g., network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

2. Scanning

The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

Static analysis – Inspecting an application’s code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.

Dynamic analysis – Inspecting an application’s code in a running state. This is a more practical way of scanning, as it provides a real-time view into an application’s performance.

3. Gaining Access

This stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target’s vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic, etc., to understand the damage they can cause.

4. Maintaining access

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization’s most sensitive data.

5. Analysis

The results of the penetration test are then compiled into a report detailing:

Specific vulnerabilities that were exploited

Sensitive data that was accessed

The amount of time the pen tester was able to remain in the system undetected

This information is analyzed by security personnel to help configure an enterprise’s WAF settings and other application security solutions to patch vulnerabilities and protect against future attacks.

Penetration testing methods

External testing

External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access and extract valuable data.

Internal testing

In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn’t necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.

Blind testing

In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.

Double-blind testing

In a double blind test, security personnel have no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defenses before an attempted breach.

Targeted testing

In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a hacker's point of view.

Who performs pen tests?

It's best to have a pen test performed by someone with little-to-no prior knowledge of how the system is secured because they may be able to expose blind spots missed by the developers who built the system. For this reason, outside contractors are usually brought in to perform the tests. These contractors are often referred to as 'ethical hackers' since they are being hired to hack into a system with permission and for the purpose of increasing security.

Many ethical hackers are experienced developers with advanced degrees and a certification for pen testing. On the other hand, some of the best ethical hackers are self-taught. In fact, some are reformed criminal hackers who now use their expertise to help fix security flaws rather than exploit them. The best candidate to carry out a pen test can vary greatly depending on the target company and what type of pen test they want to initiate.

What are the types of pen tests?

White box pen test - In a white box test, the hacker will be provided with some information ahead of time regarding the target company's security info.

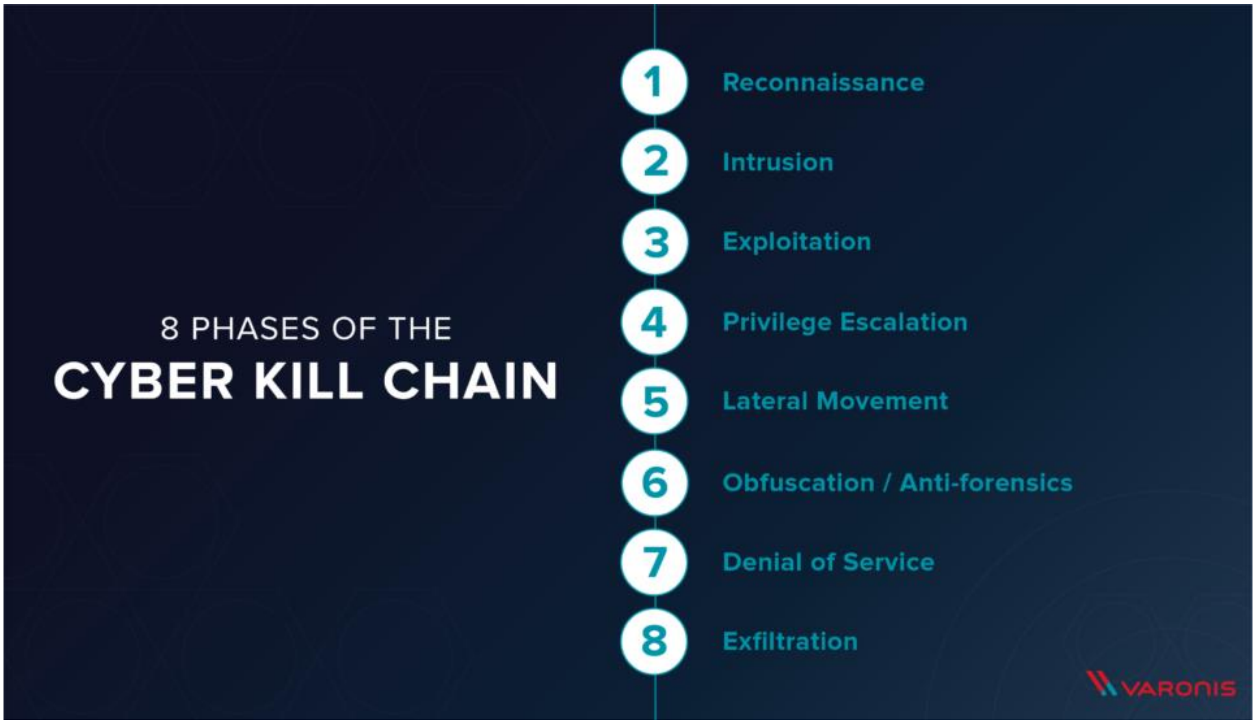
Black box pen test - Also known as a 'blind' test, this is one where the hacker is given no background information besides the name of the target company.

Covert pen test - Also known as a 'double-blind' pen test, this is a situation where almost no one in the company is aware that the pen test is happening, including the IT and security professionals who will be responding to the attack. For covert tests, it is especially important for the hacker to have the scope and other details of the test in writing beforehand to avoid any problems with law enforcement.

External pen test - In an external test, the ethical hacker goes up against the company's external-facing technology, such as their website and external network servers. In some cases, the hacker may not even be allowed to enter the company's building. This can mean conducting the attack from a remote location or carrying out the test from a truck or van parked nearby.

Internal pen test - In an internal test, the ethical hacker performs the test from the company's internal network. This kind of test is useful in determining how much damage a disgruntled employee can cause from behind the company's firewall.

The cyber kill chain is a series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data. The kill chain helps us understand and combat ransomware, security breaches, and advanced persistent attacks (APTs).



8 PHASES OF THE
CYBER KILL CHAIN

1. Reconnaissance
2. Intrusion
3. Exploitation
4. Privilege Escalation
5. Lateral Movement
6. Obfuscation / Anti-forensics
7. Denial of Service
8. Exfiltration

VARONIS

How the Cyber Kill Chain Works

There are several core stages in the cyber kill chain. They range from reconnaissance (often the first stage in a malware attack) to lateral movement (moving laterally throughout the network to get access to more data) to data exfiltration (getting the data out). All of your common attack vectors

– whether phishing or brute force or the latest strain of malware – trigger activity on the cyber kill chain.

Each stage is related to a certain type of activity in a cyber attack, regardless of whether it’s an internal or external attack:

Reconnaissance

The observation stage: attackers typically assess the situation from the outside-in, in order to identify both targets and tactics for the attack.

Intrusion

Based on what the attackers discovered in the reconnaissance phase, they’re able to get into your systems: often leveraging malware or security vulnerabilities.

Exploitation

The act of exploiting vulnerabilities, and delivering malicious code onto the system, in order to get a better foothold.

Privilege Escalation

Attackers often need more privileges on a system to get access to more data and permissions: for this, they need to escalate their privileges often to an Admin.

Lateral Movement

Once they’re in the system, attackers can move laterally to other systems and accounts in order to gain more leverage: whether that’s higher permissions, more data, or greater access to systems.

Obfuscation / Anti-forensics

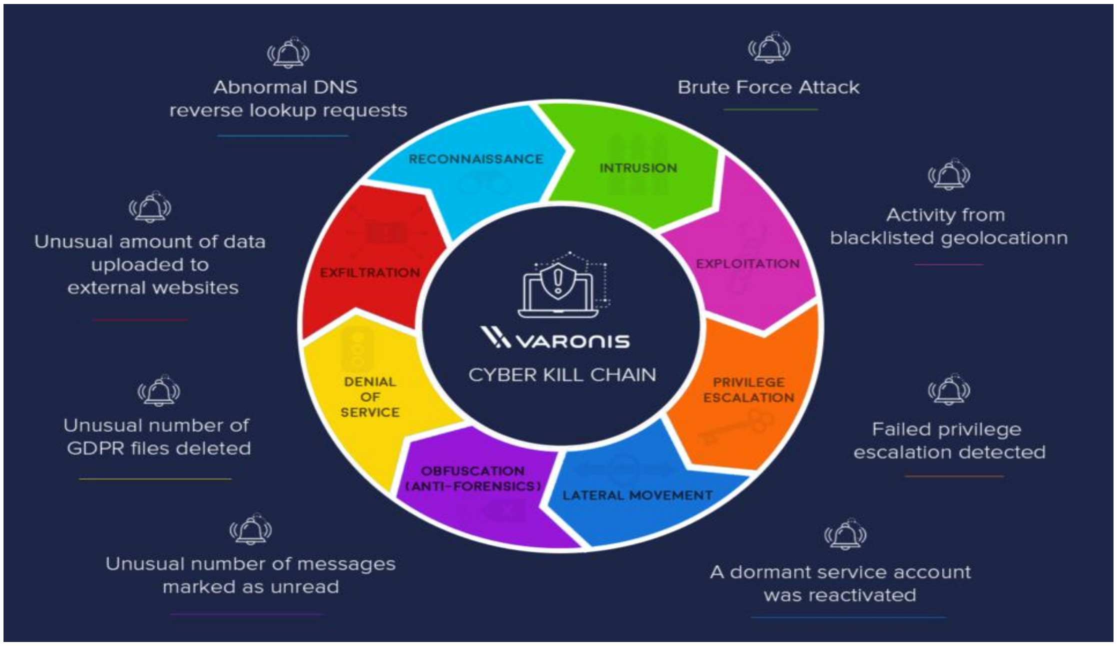
In order to successfully pull off a cyberattack, attackers need to cover their tracks, and in this stage they often lay false trails, compromise data, and clear logs to confuse and/or slow down any forensics team.

Denial of Service

Disruption of normal access for users and systems, in order to stop the attack from being monitored, tracked, or blocked

Exfiltration

The extraction stage: getting data out of the compromised system.


Abnormal DNS reverse lookup requests
Brute Force Attack
RECONNAISSANCE
INTRUSION
Activity from blacklisted geolocationn
Unusual amount of data uploaded to external websites
EXFILTRATION
EXPLOITATION
VARONIS
CYBER KILL CHAIN
DENIAL OF SERVICE
PRIVILEGE ESCALATION
Unusual number of GDPR files deleted
Failed privilege escalation detected
OBFUSCATION (ANTI-FORENSICS)
LATERAL MOVEMENT
Unusual number of messages marked as unread
A dormant service account was reactivated

Reconnaissance

In every heist, you've got to scope the joint first. Same principle applies in a cyber-heist: it's the preliminary step of an attack, the information gathering mission. During reconnaissance, an attacker is seeking information that might reveal vulnerabilities and weak points in the system. Firewalls, intrusion prevention systems, perimeter security – these days, even social media accounts – get ID'd and investigated. Reconnaissance tools scan corporate networks to search for points of entry and vulnerabilities to be exploited.

Intrusion

Once you've got the intel, it's time to break in. Intrusion is when the attack becomes active: attackers can send malware – including ransomware, spyware, and adware – to the system to gain entry. This is the delivery phase: it could be delivered by phishing email, it might be a compromised website or that really great coffee shop down the street with free, hacker-prone wifi. Intrusion is the point of entry for an attack, getting the attackers inside.

Exploitation

You're inside the door, and the perimeter is breached. The exploitation stage of the attack…well, exploits the system, for lack of a better term. Attackers can now get into the system and install additional tools, modify security certificates and create new script files for nefarious purposes.

Privilege Escalation

What’s the point of getting in the building, if you’re stuck in the lobby? Attackers use privilege escalation to get elevated access to resources. Privilege escalation techniques often include brute force attacks, preying on password vulnerabilities, and exploiting zero day vulnerabilities. They’ll modify GPO security settings, configuration files, change permissions, and try to extract credentials.

Lateral Movement

You’ve got the run of the place, but you still need to find the vault. Attackers will move from system to system, in a lateral movement, to gain more access and find more assets. It’s also an advanced data discovery mission, where attackers seek out critical data and sensitive information, admin access and email servers – often using the same resources as IT and leveraging built-in tools like PowerShell – and position themselves to do the most damage.

Obfuscation (anti-forensics)

Put the security cameras on a loop and show an empty elevator so nobody sees what’s happening behind the scenes. Cyber-attackers do the same thing: conceal their presence and mask activity to avoid detection and thwart the inevitable investigation. This might mean wiping files and metadata, overwriting data with false timestamps (timestomping) and misleading information, or modifying critical information so that it looks like the data was never touched.

Denial of Service

Jam the phone lines and shut down the power grid. Here’s where the attackers target the network and data infrastructure, so that the legitimate users can’t get what they need. The denial of service (DoS) attack disrupts and suspends access, and could crash systems and flood services.

Exfiltration

Always have an exit strategy. The attackers get the data: they’ll copy, transfer, or move sensitive data to a controlled location, where they do with the data what they will. Ransom it, sell it on ebay, send it to wikileaks. It can take days to get all of the data out, but once it’s out, it’s in their control.

The Takeaway

Different security techniques bring forward different approaches to the cyber kill chain – everyone from Gartner to Lockheed Martin defines the stages slightly differently. Alternative models of the cyber kill chain combine several of the above steps into a C&C stage (command and control, or C2) and others into an ‘Actions on Objective’ stage. Some combine lateral movement and privilege escalation into an exploration stage; others combine intrusion and exploitation into a ‘point of entry’ stage.

It’s a model often criticized for focusing on perimeter security and limited to malware prevention. When combined with advanced analytics and predictive modeling, however, the cyber kill chain becomes critical to data security.

With the above breakdown, the kill chain is structured to reveal the active state of a data breach. Each stage of the kill chain requires specific instrumentation to detect cyber attacks, and Varonis has out-of-the-box threat models to detect those attacks at every stage of the kill chain.

Varonis monitors attacks at the entry, exit, and everywhere in between. By monitoring outside activity – like VPN, DNS, and Proxy, Varonis helps guard the primary ways to get in and out of an organization. By monitoring file activity and user behavior, Varonis can detect attack activity on every stage of the kill chain – from kerberos attacks to malware behavior.