



# INFORMATION SECURITY 101 – STUDENT GUIDE

Version: 1 Rev A



# Information Security 101



# Information Security 101

- What motivates attackers?
- Review common system vulnerabilities.
- Examine how attacks are delivered.
- Consider attack types.



In this section we will be reviewing some of the fundamental elements of Information Security.

This material is not a replacement for a full Information Security course and is provided as a value add to students that have an IT background but may not be familiar with IT Security.

In this module, we will

- look at the reasons attackers attempt to exploit networks and systems.
- review some of the most common system vulnerabilities.
- examine the methods by which attacks are delivered .
- consider attack types and how they are implemented at a high level.

## What motivates attackers?



### Criminals

- ✔ Credit Cards
- ✔ Personal Data
- ✔ Resources



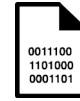
### Governments

- ✔ Surveillance
- ✔ Steal Secrets
- ✔ Cause Harm



### Activists

- ✔ Further Cause
- ✔ Steal Data
- ✔ Cause Harm



Copyright© 2017 AlienVault. All rights reserved

3



So, what drives someone to want to break into a company's infrastructure? Who would benefit from taking these risks?

The first group we will discuss are criminals looking to profit from user information.

Criminals seek to gain access to personal and financial data, whether by accessing database records or by logging information directly from a victim's laptop.

Once this sensitive data has been captured the consequences can be devastating for the victim.

Information is not the only thing at stake here, as attackers may also steal computer resources unbeknownst to an unsuspecting company to carry out further attacks.

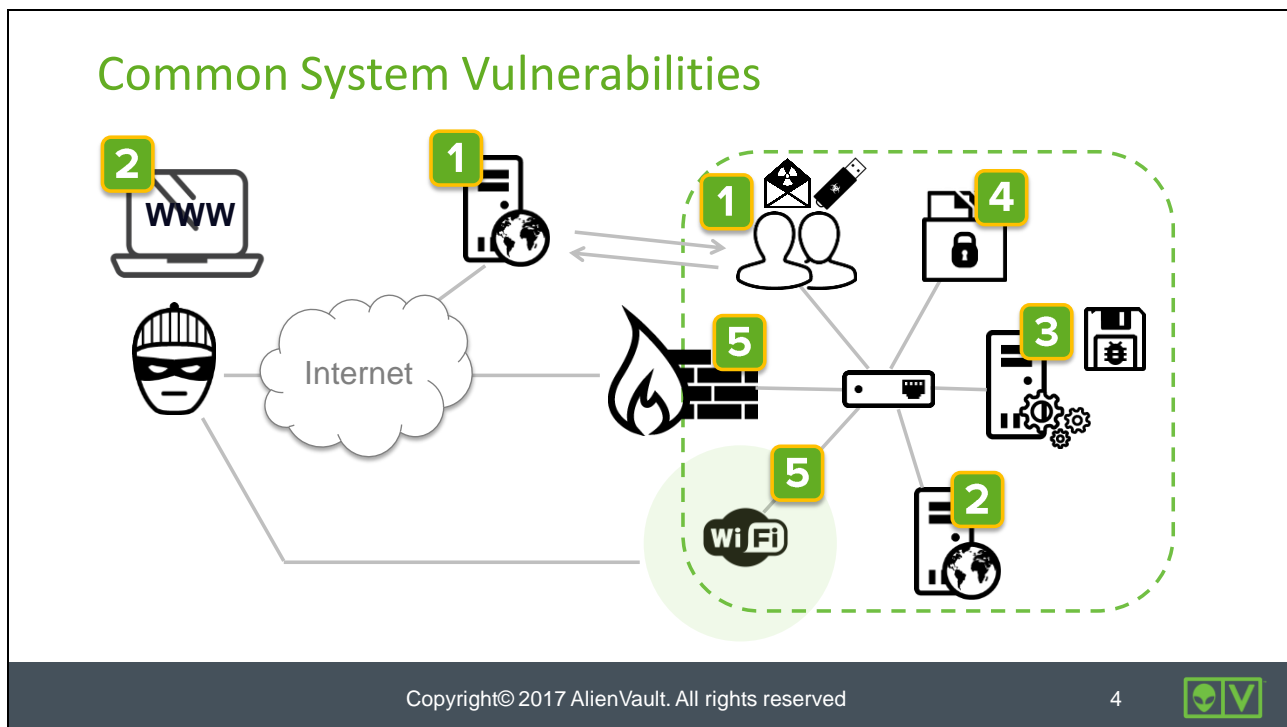
Governments are also key players, whether it be against individuals, corporations, or other governments.

Surveillance is carried out against individuals for national security in an attempt to protect against terrorism.

They also engage in cyber-espionage programs aimed at stealing trade secrets from corporations as well as obtaining political and military information from their adversaries.

Last but not least are activists who are working to further their cause by whatever means necessary.

Activists typically seek to cause harm by bringing down their targets' systems or stealing sensitive data to release to the public.



When an attacker is looking at your network and systems, they are attempting to identify weak spots or vulnerabilities they can use as entry points.

They will look at poor security practices and how to exploit inputs by using them in unexpected ways.

Let's discuss some common vulnerabilities that exist in today's IT infrastructures.

**People** — Out of all the components that make up your environment, the biggest risk to security is not a piece of hardware or software but the company's employees themselves.

People are a prime target for attack as they can be fooled into executing malicious software on your company systems, especially if there is limited security awareness in the organization. We will be looking at attacks that target people on the next slide.

**Web Applications** — A web page can be like a gateway for attackers if it is not protected correctly. An attacker can use the interface to not only attack the backend servers and database but also plant traps on the site itself to do harm to other visitors.

It is essential that all inputs be properly sanitized to ensure that there are no opportunities for would-be attackers to use inputs for any purpose other than that intended.

**Misconfigured Systems** — A common occurrence among system administrators is to install an operating system without knowing what is actually being installed. This can be troublesome, as

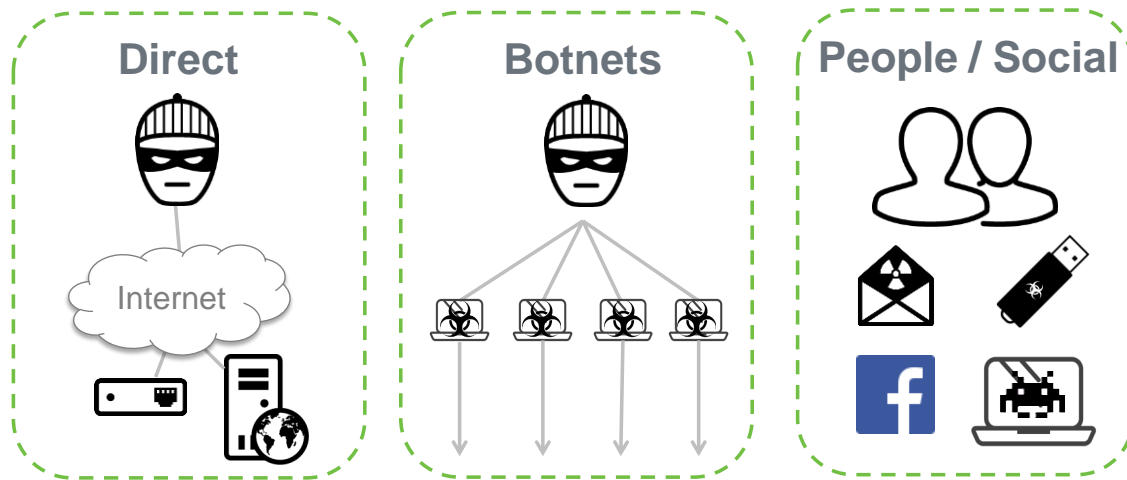
most operating systems will not only install the applications, but also set up a base configuration and turn services on. This can cause unwanted services, such as telnet, DHCP, or DNS to be running on a server without the administrator realizing it, leading to unwanted traffic to the server.

**Unpatched Systems** — There is no such thing as perfect software and developers and system administrators often find exploitable bugs that are in turn resolved by system updates. However, even then, it is up to system administrators to patch these bugs whenever they are made public. This requires vigilance, constant tracking of bugs, and proper system maintenance, to ensure a secure computing environment and avoid the possibility that the vulnerability will be exploited.

**User Accounts and Access** — As we mentioned previously, people are a vulnerability on your network and it is only a matter of time before an attacker succeeds in exploiting this avenue. It is very important to make sure that users only have just enough privileges to systems and data to successfully do their work versus giving them full access to everything. While it can be easier to give a user full read, write, and execute access to a folder, or to allow them to log into a server as root instead of a specific account, these shortcuts can give an attacker far more access to cause damage.

**Network security** — Your network, unsurprisingly, is a prime target for attackers. They will scan to see what ports are open, and based on this information, learn about the services and applications that are available and that potentially can be exploited. Companies employ firewalls to manage the traffic that goes in and out of their networks but those firewalls are only as good as the rules that are put in place. Network administrators need to create effective rules to only allow the necessary traffic in or out which includes minimizing the open ports. Remember that an attacker does not have to break into your network through the front door. As mentioned, users on your network can unwittingly open the door by accidentally installing malicious software or attackers may gain access through wireless networks that are not properly secured.

## How Attacks are Delivered



Copyright© 2017 AlienVault. All rights reserved

5



Let us now take a look at the different methods of attack that are used to exploit the vulnerabilities we just discussed.

The first type of attack delivery method we will talk about is a Direct Network Attack from one individual. This intruder will first analyze your environment and collect information in order to exploit existing vulnerabilities. An attack whose purpose is only to determine system information is called a *passive attack*. Once the attacker has a picture of your vulnerabilities, they will tailor an attack or use preexisting software to exploit these weak spots.

The second type of attack we will discuss are Botnets . Botnets are a collection of compromised computers that can be controlled by remote perpetrators to perform various types of attacks on other computers or networks.

Some common types of attacks perpetrated by Botnets are distributed denial of service attacks (DDoS) where multiple systems submit as many requests as possible to the victim machine in order to overload it. Botnets are also used to distribute spam that contains or connects to malware, in an attempt to infect even more systems .

Finally we look at attacks directed at the employees in your company, and anyone on an internet-connected device for that matter. These attacks can be delivered by either individuals or botnets and prey on people's curiosity, fears, and lack of information security IQ.

Social engineering attacks can be delivered through:



Emails, (commonly known as phishing).

Phishing attacks involving spoofed emails sent to users that either have attached infected files or lead them to malware infected websites designed to appear authentic, an online banking portal for example.

Emails received by users in most cases will look authentic, sent from sources known to the user, like a customer or a colleague, and attempt to manipulate the victim into opening the file or link without thinking. An example would be an “Urgent Invoice” that is attached to an email that needs to be proceed immediately or there will be some consequence.

Media such as DVDs and USB drives.

An attacker could put some form of malicious software on any removable media and have it masquerade under some title like “Top Secret – Area 51 - WikiLeaks” and leave the media in a coffee shop that they know is frequented by their victim, hoping that they take the bait and bring it into their “secure” workplace.

An attacker can also just get lucky by targeting someone's personal accounts in the hopes that they will unwittingly bring the infected payload into their office, piggy backing on a USB drive. Even the most non-technical of users can easily insert a thumb drive into the USB slot of any foreign machine and begin copying/downloading data.

Social Media and commonly visited sites.

Attacks delivered through social media are very similar to the email phishing attacks we discussed, just the delivery mechanism is different and includes special links or posts that attract the user with their content and convince them to click on them. The link then redirects the victim to a malicious website or similar harmful content.

In some cases the user is redirected to a mirror website that asks them to like a post before even viewing it. The user, not suspecting any harm in this, clicks the "like" button but doesn't realize that the "like" button has been spoofed and in reality is an "accept" button for a fake app that will access the user's personal information.

Watering Hole Attacks focus on a way of breaking into a very secure network by exploiting a vulnerable site commonly visited by its employees. Take this example:

- A sandwich shop located 5 minutes' walk from the target company has an online ordering form that hundreds of employees order through.
- The attacker exploits the form and plants an exploit.
- An employee from the victim company orders lunch and inadvertently downloads the exploit, giving the attacker access to the company network.

This is a small and not exhaustive list of the ways attacks are delivered, which will hopefully give you a greater perspective of some of the methods used by attackers.

## Types of attack



Malware Attacks



Brute force Attacks



Web Application Attacks



Network Attacks



Denial of Service Attacks



Cryptographic Attacks

Copyright© 2017 AlienVault. All rights reserved

6



We now know what motivates attackers, the vulnerabilities and weak spots they want to exploit, and how they try to deliver these exploits.

Now let's examine the types of attacks that are delivered, looking at how they work from a high level, and what the attacker has to gain from each type.

In the following sections we will be covering:

Malware (short for **Malicious Software**) attacks represent various forms of code that damage or infiltrate computer systems without informing the owner.

Web Application Attacks are perpetrated through a website that leverages the standard browser-based interface to attack the host company or other visitors to the site.

Denial of Service Attacks are designed to cause an interruption or suspension of services of a specific host/server by flooding it with large quantities of useless traffic or requests.

Brute Force Attacks are trial-and-error methods of attack that generate a large number of consecutive guesses used to obtain information sought, such as a user password.

Network Attacks refer to attempts to either eavesdrop on network traffic to gather confidential information, or gain access to secure resources by masquerading as a trusted system.

Cryptographic Attacks look to decipher or break the security protocols put in place to keep information secure.



# Malware Attacks

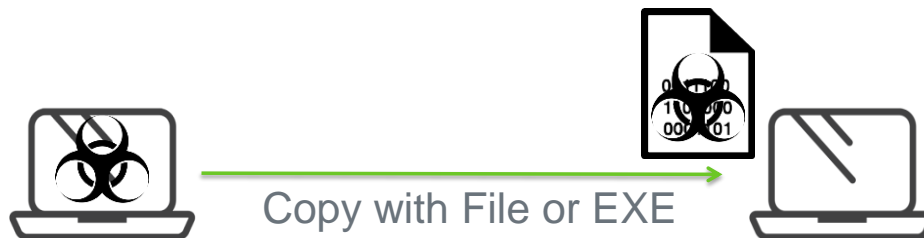
Copyright© 2017 AlienVault. All rights reserved

7



## What is a Virus?

- Code injected into programs and files.
- User intervention is required.
- Spread through sharing.



Copyright© 2017 AlienVault. All rights reserved

8



### What is a Virus?

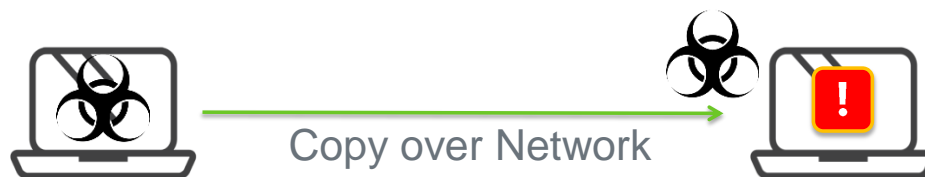
A Virus is a malicious program able to inject its code into other programs, applications, or data files without the user's consent.

User intervention is required for a virus to be successful. End-users are either tricked into downloading and executing malicious files, or opening malicious email attachments, which cause their systems to become infected.

Viruses do not self-replicate, and depend on the sharing of files and executables through email, file sharing, or removable media to spread across the network.

## What is a Worm?

- ✔ Exploits operating system vulnerabilities.
- ✔ No user interaction is required.
- ✔ Reproduce/duplicate and spreads by itself.



Copyright© 2017 AlienVault. All rights reserved

9



What is a Worm?

A Worm is a malicious program that exploits operating system vulnerabilities to spread itself.

No user interaction is required to be infected by a Worm, making them especially dangerous once on a network.

Unlike a virus, worms can reproduce/duplicate and spread by themselves; they don't need to attach themselves to a file or executable.

As they spread across the network they can have devastating effects on the host servers, as well as consuming network bandwidth.

## What is a Trojan?

- ✔ Masquerades as a not-malicious application.
- ✔ User intervention is required.
- ✔ Can cause damage but often stealthy.



Copyright© 2017 AlienVault. All rights reserved

10



### What is a Trojan?

A Trojan is a type of malware that masquerades as a not-malicious, even useful, application but it will actually do damage to the host computer after its installation.

Trojans do not self-replicate and require user intervention to install themselves. What happens in most scenarios is a user is tricked into thinking they are installing a legitimate program, and in many cases the program will perform the expected actions but will also run the malicious software in the background.

While some Trojans can cause damage to your system, many Trojans are stealthy and do not advertise their presence, to avoid detection. Trojans allow attackers entrance into your system, allowing other threats to infect it, or allowing remote access to it.

## Malware Attacks

Rootkit / Backdoor

Adware / Spyware  
/ Keylogger

Botnet

Ransomware



Copyright© 2017 AlienVault. All rights reserved

11



Now let's look at some other malicious software and what it does. Many of the items we will be mentioning are variants or evolutions of the viruses, worms and trojans we just discussed.

A rootkit is designed to hide certain processes or programs from detection. A rootkit usually acquires and maintains privileged system access, while hiding its presence at the same time. The privileged access can allow the rootkit to provide the attacker with a backdoor to a system.

A backdoor, sometimes known as a Remote Access Trojans or R.A.T, is a type of trojan that opens a backdoor on the targeted system to allow the attacker remote access to the system or even complete control over it. This can also make it possible for a system to become a "zombie" or a "bot" as part of a botnet.

We discussed botnets when looking at attack delivery but let's quickly recap.

Botnets are a collection of compromised computers that can be controlled by remote perpetrators to perform various types of attacks on other computers or networks.

Some common types of attacks perpetrated by botnets are DDoS attacks, and spam or malware distribution.

The next collection of malware we will discuss focuses on tracking movements and actions on your system, and taking action based on what you are doing.



Adware is more annoying than malicious and is something seen more and more. Adware performs analysis of end user internet habits and then tailors advertisements directly to users' interests.

Spyware on the other hand is much more sinister and dangerous for the user and their organization. It monitors and collects information about the user, their computer and/or their organization without their knowledge and sends it back to the attacker.

Keyloggers are a subset of Spyware that keeps track of every keystroke, even the clipboard, on your system. This can obviously capture usernames, passwords, and personal information which is sent back to the attacker.

The final major area we will look at is ransomware.

Ransomware typically locks down an infected machine and demands payment (ransom) to restore the full functionality or files. Many ransomware attacks will also come with a threatening lock screen that looks to come from a reputable source such as a governmental or law enforcement agency, usually accusing the victim of performing illegal activities.

A variation of ransomware called a Cryptolock Trojan emerged in 2013. It encrypts and locks files on not only your system but potentially any system on any network that you have access to, including file servers, network attached storage, and so on. In this attack the files are encrypted with a very strong encryption key and the ransom is paid in exchange for the key required to unencrypt the files.



# Web Application Attacks

Copyright© 2017 AlienVault. All rights reserved

12



## Web Application Attacks (SQL Injection)



Exploits of a Mom: <https://xkcd.com/327/>

Copyright© 2017 AlienVault. All rights reserved

13



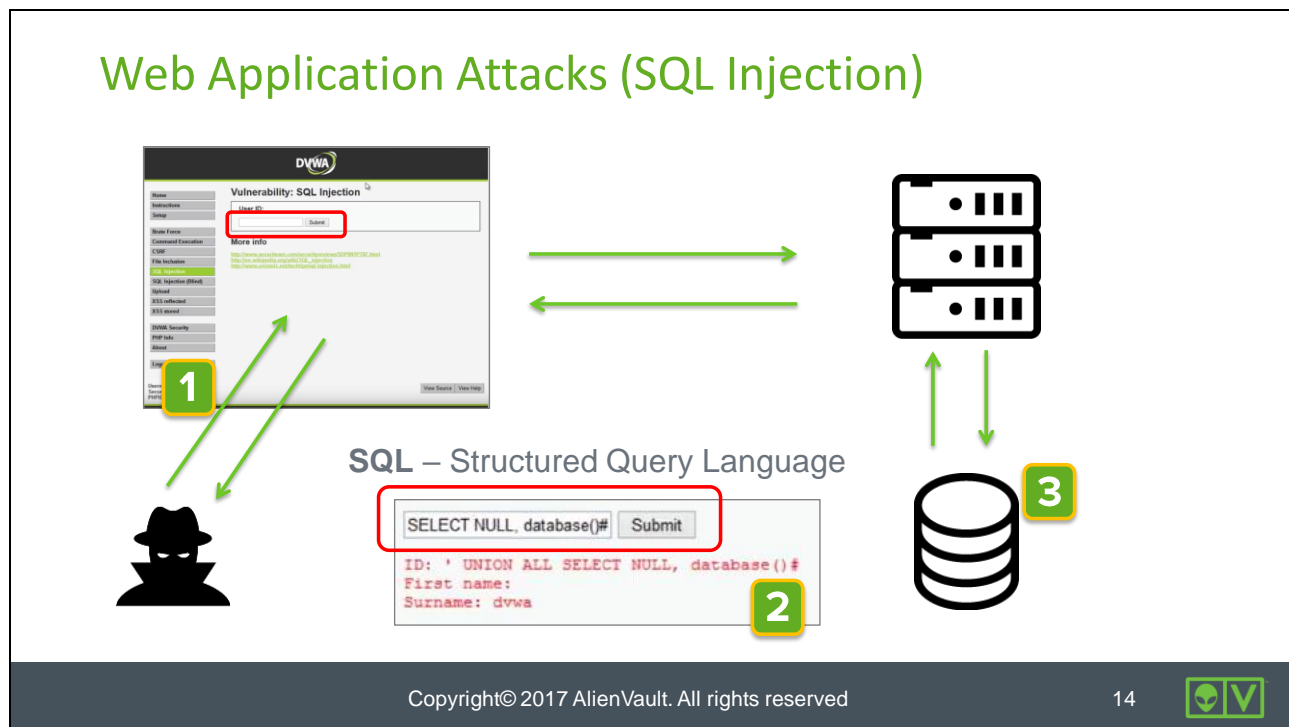
This is a funny cartoon but SQL Injection attacks are no laughing matter and can be some of the most dangerous to your systems and data.

In simple terms a SQL injection attack is when an attacker is able to execute or “inject” a malicious SQL query (also commonly referred to as a malicious payload) against a database to either obtain data or cause harm.

In the above example the boy’s name is appended with a SQL instruction which causes the deletion of the database table called Student and thus all the data.

Thanks to the good people at xkcd.com for usage of this image.

## Web Application Attacks (SQL Injection)



So how does a SQL Injection attack work?

An attacker will look for an interface that they can use to execute a database command to achieve a specific result.

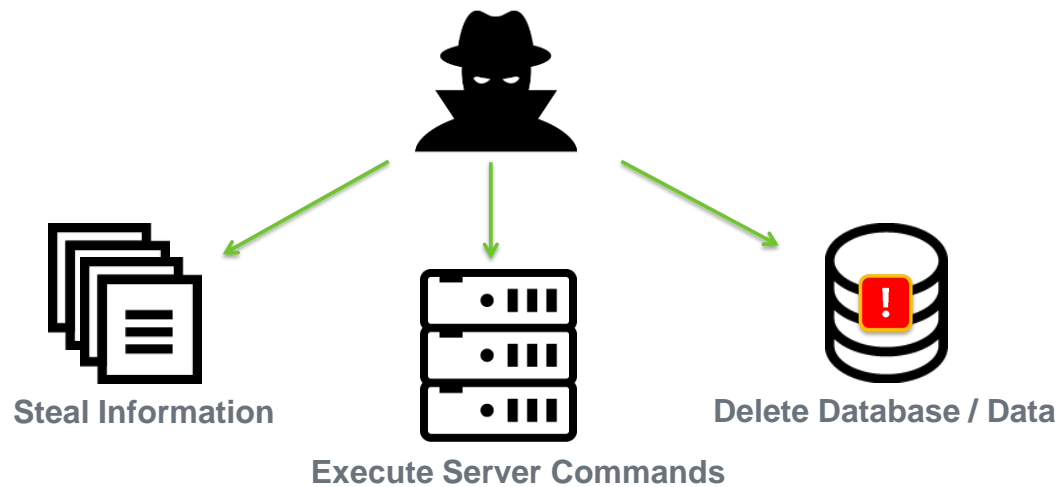
In this case they select a web page with a basic form which they will test with specific commands to see what information they can extract, and attempt to identify vulnerabilities they can exploit.

Here we see how the User ID field is being used for purposes other than it was intended.

Since this field queries the database it allows the attacker to enter a SQL string that will pull back information other than that intended by design; in this case it's the name of the database.

The attacker can use queries such as this to build up a picture of the structure of the database and in turn execute increasingly dangerous and destructive commands.

## Web Application Attacks (SQL Injection)



Copyright© 2017 AlienVault. All rights reserved

15



Here are some examples of potential compromises that an attacker could cause through SQL Injection.

An attacker can steal information by querying the database and potentially gaining access to tables containing sensitive customer information. They could also manipulate data in the database for their own agenda.

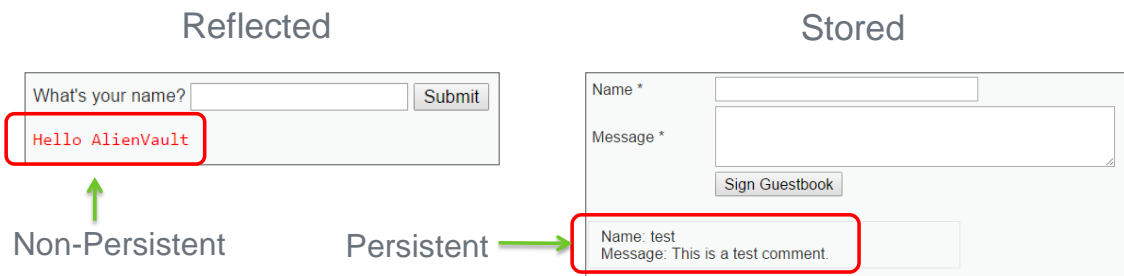
Depending on the system user that owns your database, there may be options for the attacker to execute system commands that allow access to information on the server itself outside the database. This would be especially dangerous if the database owner is the root or administrator account.

A malicious attacker may simply want to destroy data or impact your business and can “drop” or delete tables from your database.

Ideally all interfaces that query a database should have their input properly sanitized to make sure would-be attackers do not have the potential to perform such an attack.

## Web Application Attacks (Cross Site Scripting)

- 🟢 Cross Site Scripting is also known as XSS.
- 🟢 Reflected XSS: Link is crafted, the user is tricked into clicking it.
- 🟢 Stored XSS: Impacts all visitors to an exploited page.



Copyright© 2017 AlienVault. All rights reserved

16



Cross-Site Scripting or XSS for short is when malicious scripts are injected into the otherwise benign and trusted web sites.

Cross-Site Scripting attacks occur when an attacker uses a web application to send malicious code to a different end user. Flaws that allow these attacks to succeed can occur anywhere a web application using input from a user in the output, without validating or encoding it. The end user's browser has no way to know that the script should not be trusted, and will execute it. The script can then access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.

There are 2 main types of XSS, Reflected and Stored.

Reflected XSS occurs when an attacker injects browser executable code within a single HTTP response. The injected attack is not stored within the application itself, it is non-persistent and only impacts users who open a maliciously crafted link or are redirected from a third-party web page.

In this example, the name typed into the field is displayed when the user hits submit. An attacker would have to build a specific link that would take a victim to this page, inject a malicious script into the field, and submit it, causing the script to execute.

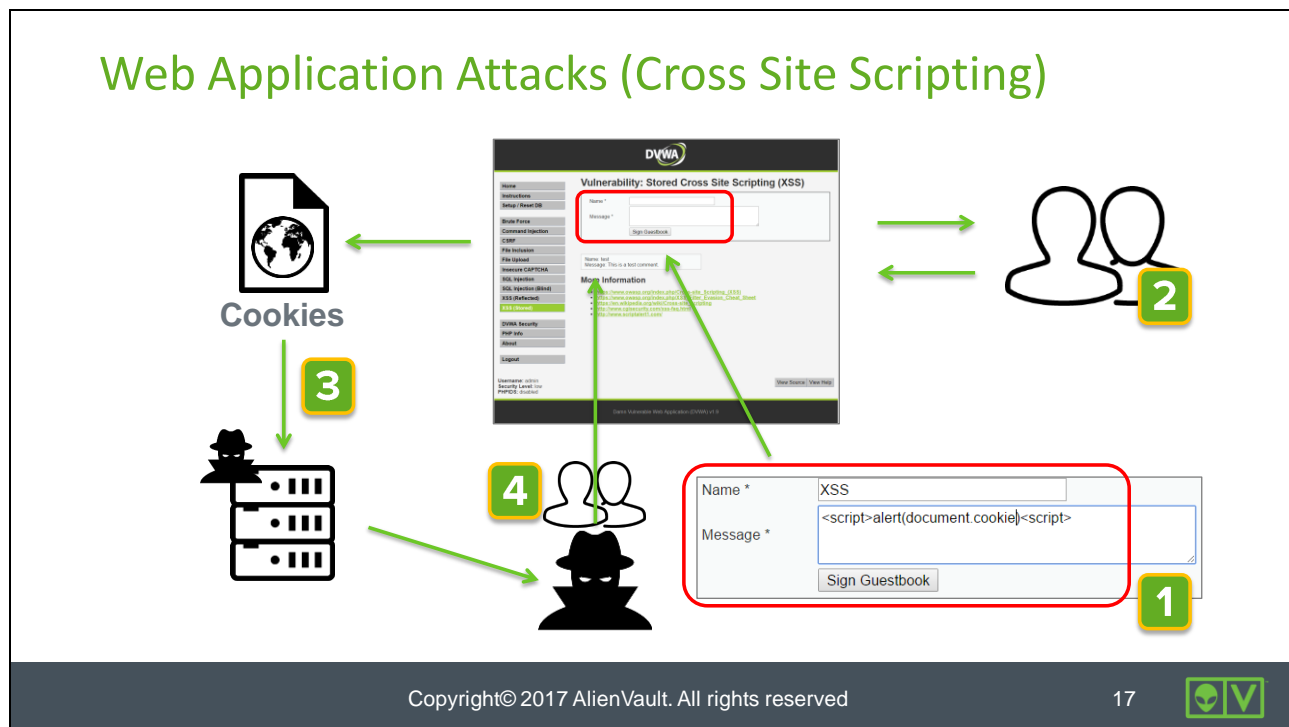
Stored XSS is the most dangerous type of Cross Site Scripting. Web applications that allow users to store data are potentially exposed to this type of attack. Stored Cross-Site Scripting occurs when a web application gathers input from a user which might be malicious, and then

stores that input in a data store for later use. As a consequence, the malicious data will appear to be part of the web site and run within the user's browser under the privileges of the web application.

In this example, the details typed are added to the guestbook and loaded by everyone that visits the page. An attacker could hide a script on the page by posting on the guestbook and everyone who visits the page has the potential to be a victim as the script runs when the page loads.

We will look at this in a little more detail on the next slide.

## Web Application Attacks (Cross Site Scripting)



We will now look at how a Stored Cross-Site Scripting attack would occur.

The attacker posts a message to the guestbook that contains some hidden JavaScript.

Note that the script in the screenshot is just as an example and will just pop up a message with the contents of the document.cookie file. A real script would be much more complex and stealthy.

When people log in and go to this page, the script runs when the page is loaded. As it is part of the guestbook entries, the victims are not aware that this is happening.

In this example the script sends the contents of document.cookie for the logged-in user to a site the attacker has set up to collect this information.

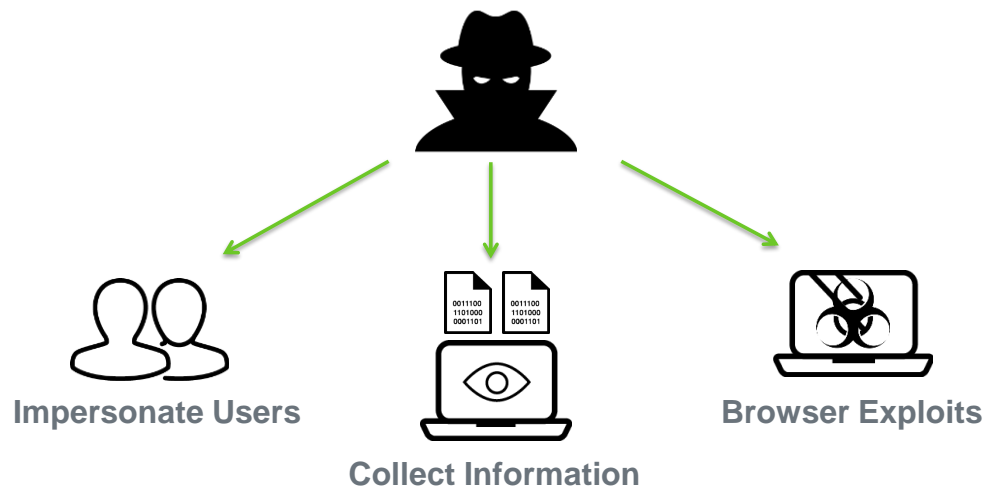
The document.cookie file holds information about the victim's session while visiting the site.

The attacker can now log into the site and then alter their own session ID in their browser to match that of one they have stolen, thus impersonating the user.

This can be especially dangerous if they happen to capture the site administrator's session, potentially allowing them to "own" the site.



## Web Application Attacks (Cross Site Scripting)



Copyright© 2017 AlienVault. All rights reserved

18



Here are some examples of potential compromises that an attacker could cause through Cross-Site Scripting.

The first we have seen in our example, when an attacker hijacks a user's session to impersonate them. This can give the attacker elevated privileges on the site or expose the user's personal data.

Once the attacker is logged in as the victim they have access to addresses, phone numbers, and personal information that could be used for identity theft or potentially to craft a more targeted attack against that user.

Thankfully most sites do not list full details of extremely confidential information such as credit card numbers; however an XSS attack could present the victim with a form created by the attacker that looks similar to what the victim was expecting and fool them into providing this information.

The final items we will discuss are browser-based attacks that can piggyback on an XSS attack.

The attacker may use the attack to redirect the victim to a site with some malware that is downloaded to their system, thus offering the attacker even more opportunities to exploit the victim and their organization.

## Web Application Attacks (Broken Authentication)

- 🚩 Unencrypted Connection
- 🚩 Session values don't expire
- 🚩 Session IDs in the URL



Copyright© 2017 AlienVault. All rights reserved

19



As we saw in the Cross-Site Scripting section, Session IDs can be exploited to log into a website and impersonate a user thus breaking the authentication mechanism.

A website can be vulnerable to this type of attack if:

Communications are not being encrypted between the user and the site.

The Session values don't time out or invalidate after a user logs out of the site.

The Session ID is present in the URL.

There are other ways and means to exploit this type of vulnerability apart from XSS and we will review such an example in the next slide.

## Web Application Attacks (Broken Authentication)



The scenario we are about to cover has several major security flaws that you would hope would not all occur in the real world but help to illustrate the point.

In this example, the website that the user is connecting to has 2 visible vulnerabilities — it is not using a secure encrypted connects, that is it is using HTTP not HTTPS — and it is showing the session ID of the current user in the URL itself.

Let's say the user is visiting this site from an internet café and is connected to a public wireless connection. It is possible for an attacker to connect to this network also and eavesdrop on the communications between the user and the web server. We will discuss how this occurs on the Network Attacks section coming later.

Once this information has been obtained, the attacker can either log in directly with the user's credentials or choose to hijack their session by substituting in the user's Session ID for their own.



# Denial of Service Attacks

Copyright© 2017 AlienVault. All rights reserved

21



## Denial of Service Attacks

### Denial of Service



### Distributed Denial of Service



Copyright© 2017 AlienVault. All rights reserved

22



Denial of Service Attack or DDoS for short, are attacks designed to cause an interruption or suspension of services of a specific host.

This is achieved by sending a malicious request to the server that the attacker knows will crash it, or overloading the server so that it exhausts all its available resources and eventually becomes unresponsive and unable to answer any legitimate new requests, or responds but is so delayed that the service is unusable.

The other type of Denial of Service Attack is known as a Distributed Denial of Service Attack or DDoS in which the attacker uses multiple systems to perform the attack.

DDoS attacks can be executed in various ways but commonly use a botnet.

The attacker sends an instruction from the Command and Control Center (C&C) to the botnet instructing it to begin an attack against a particular host.

A DDoS occurs when the botnet floods the target system with traffic simultaneously and eventually overwhelms it.

So why would someone mount a DoS attack?

The reasons behind this range from activism where the site is perceived as being somehow harmful, to simple vandalism, to gaining a competitive advantage.

## Denial of Service Attacks

- 📍 ICMP Flood Attack
- 📍 Smurf Attack
- 📍 TCP SYN Flood Attack



Copyright© 2017 AlienVault. All rights reserved

23



Let's briefly discuss some of the common DoS and DDoS-type attacks that can occur.

All these attacks look at exhausting one or a number of the victim's resources until that resource becomes unresponsive.

An ICMP Flood attack is when the victim is flooded with ping requests that don't wait for a reply; the attacker just keeps sending the requests until the host cannot answer them any more due to exhaustion of the available network bandwidth or lack of CPU resources on the host itself.

A Smurf Attack is a similar approach to the ICMP Flood with one distinct difference; the attacker in this case masquerades as the victim and sends a broadcast to the computer network using an IP Broadcast address as a way to leverage a range of legitimate IP addresses to attack the victim.

Most devices on a network will, by default, respond to this by sending a reply to the source IP address which is the victim. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's system to the point where it becomes unresponsive.

This type of attack is not only disruptive to the victim but also to all the hosts as the additional traffic can clog up the network.

The third type of attack we will consider is the TCP SYN Flood Attack. The TCP protocol follows a 3-way handshake when establishing a connection. The client sends a SYN packet to the host

asking to connect, the host responds with a SYN ACK packet confirming the connection, and finally the client responds with an ACK to acknowledge, and the connection is established.

This attack exploits this by never completing the handshake; that is it does not send the ACK packet, it just keeps sending SYN packets to the host, creating open session after open session on the victim host while it waits for the ACK. This continues until the victim server exhausts all its available connections and legitimate clients are unable to connect.



# Brute Force Attack

Copyright© 2017 AlienVault. All rights reserved

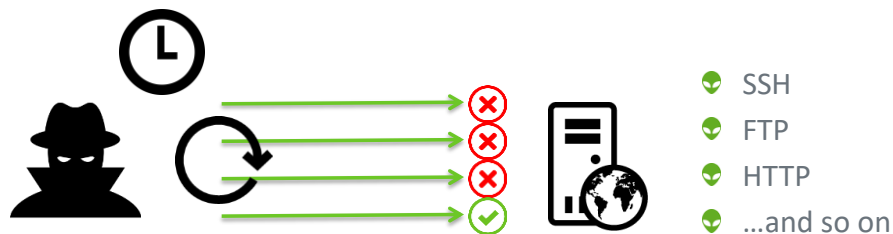
24





## Brute Force Attack

- ✔ Attempts every combination
- ✔ Time-consuming
- ✔ Guaranteed to work given enough time



Copyright© 2017 AlienVault. All rights reserved

25



A brute force attack is a trial-and-error method used by attackers in an attempt to gain access to a site or service.

The attacker goes through every possible combination until they find the correct combination to gain access, rather than employing intellectual strategies.

As you can imagine this can be extremely time consuming; the longer the password the longer it will take for a brute force attempt to be successful.

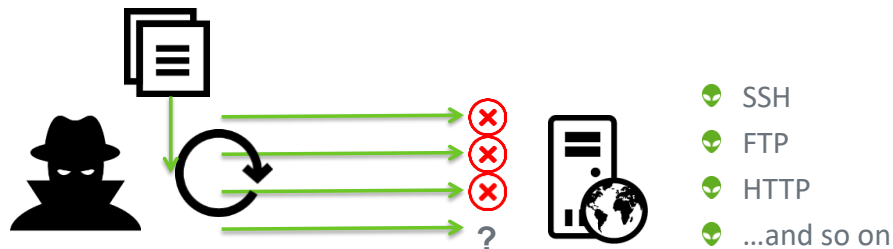
A brute force attack is considered to be infallible because given enough time it is guaranteed to succeed. However the time it might take makes it impractical as depending on the complexity and length of the password, the time required could range from tens to thousands of years.

A brute force attack can be mounted against a multitude of different services from SSH to FTP to HTTP and so on; basically anything that the attacker is presented a login prompt for.

As a point of note, the brute force approach can also be applied in attacks on cryptography and we will discuss this topic in a later section.

## Dictionary Attack

- ✔ Uses a file with common usernames and passwords
- ✔ Faster than an exhaustive brute force attack
- ✔ Not exhaustive and not guaranteed to succeed



Copyright© 2017 AlienVault. All rights reserved

26



A Dictionary Attack is a method used to try and achieve the same goal as a brute force attack but in a smarter way.

Instead of trying every combination to crack the password, a dictionary file, also known as a wordlist file, is used. These files contain commonly used usernames and password as well as leaked information from sites that have had data breaches in the past.

The attack will systematically go through all the entries and try and discover the correct username and password combination.

Since not every combination is being attempted this obviously is a much faster way to try and break into a system.

However, there is a tradeoff; since not every option is being attempted, there is no guarantee that it will be successful.

Dictionary attacks work against systems that use ordinary words as passwords and will try some of the common bad passwords such as “qwerty”, “password”, and “123456”.

Dictionary attacks are rarely successful against systems that employ multiple-word phrases, and unsuccessful against systems that employ random combinations of uppercase and lowercase letters mixed up with numerals.



# Network Attacks




Copyright© 2017 AlienVault. All rights reserved

27



## Network Attacks (A Brief Introduction)

- 📌 Network Sniffing
- 📌 Promiscuous Mode
- 📌 Hubs, Switches, and Routers

|        |                                                                                   |                     |                            |
|--------|-----------------------------------------------------------------------------------|---------------------|----------------------------|
| Router |  | Layer 3 (Network)   | Internet Protocol (IP)     |
| Switch |  | Layer 2 (Data Link) | Media Access Control (MAC) |
| Hub    |  | Layer 1 (Physical)  |                            |



Before we examine the various types of network attacks let's start by reviewing some basic concepts.

You may have heard the term network sniffing before but might not be 100% clear on what it means.

In common terms it means to eavesdrop on the traffic on a network you are connected to using sniffing software.

To allow this to happen, the network interface that you are using to sniff the network must be set to promiscuous mode.

Promiscuous mode means that the network interface will accept anything it sees regardless of whether it is meant for it or not, thus allowing the sniffer to see all the traffic.

In the past when hubs were used, they would forward all traffic to every device on a network, which would allow the sniffer to see everything.

Now, the use of switches and routers on the network insures traffic is sent only to the system that it is meant for.

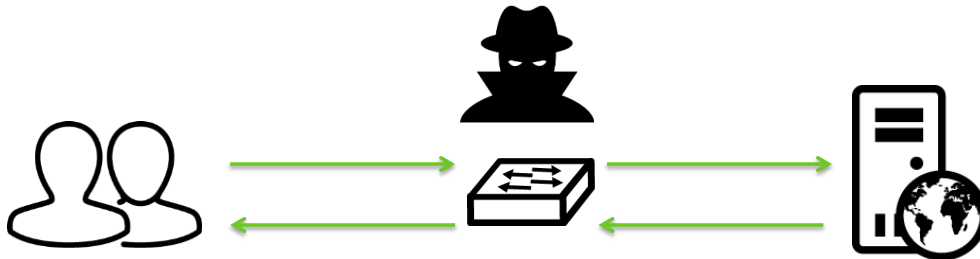
Switches operate at Layer 2 (MAC) and forward frames to their destination within the local network based on the MAC address of the device which is its unique physical address on the network.

Routers operate at Layer 3 (IP), connect networks together, and will route packets to their destination based on IP address or their logical address.

As a result, attackers have had to come up with more complex forms of attack which we will be discussing in the coming slides.

## Network Attacks (ARP Spoofing)

- ❖ Manipulates the **Address Resolution Protocol**
- ❖ ARP Poisoning
- ❖ Used in a “Man in the middle” attack



Copyright© 2017 AlienVault. All rights reserved

29






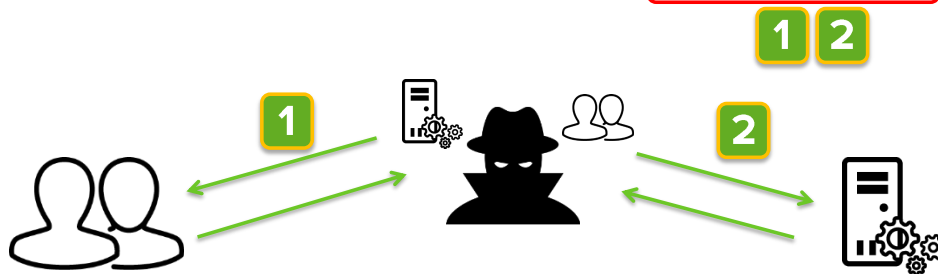
This attack uses ARP which stands for Address Resolution Protocol which is responsible for mapping the logical IP address of a device to the physical MAC address.

ARP spoofing, which is also known as ARP poisoning, operates by sending faked ARP messages in the network in an attempt to fool devices into thinking they are communicating with each other where they are in fact communicating through the attacker.

The purpose of this spoofing is to associate the attacker's MAC address with the IP address of another legitimate host, causing traffic redirection to the attacker host. This allows the attacker to sniff the traffic that is passing through it. This kind of spoofing is often used in man-in-the-middle attacks.

## Network Attacks (ARP Spoofing)

| Device                                                                                        | IP             | MAC               |
|-----------------------------------------------------------------------------------------------|----------------|-------------------|
|  Destination | 1 192.168.1.5  | ec-08-6b-d1-1e-c4 |
|  Victim      | 2 192.168.1.10 | 00-50-56-C0-00-08 |
|  Attacker    | 192.168.1.20   | 00-50-56-C0-00-01 |



Copyright© 2017 AlienVault. All rights reserved

30



Now let's step through how such an attack might occur.

Here we see a table with the IP and MAC address of the Attacker, Victim, and the Server they are trying to connect to.

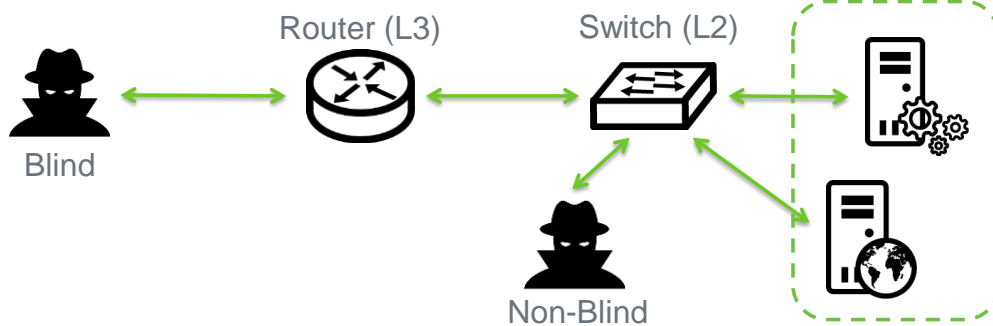
The Attacker will send an ARP message to the Victim mapping its own MAC address to the IP address of the Destination server.

The Attacker will then do the same except this time they will contact the Destination server representing themselves as the victim.

Now both the victim and destination believe they are talking to each other when in fact all their information is going through the Attacker, who is seeing all the information being transmitted.

## Network Attacks (IP Spoofing)

- 📌 Source IP modified in the packet header
- 📌 Trying to gain access by impersonating authorized system
- 📌 **Non-Blind** — Uses the TCP handshake
- 📌 **Blind** — TCP handshake with modified network packet



Copyright© 2017 AlienVault. All rights reserved

31



In simple terms, IP spoofing is done by modifying the packets sent to a target system by changing the source address in the packet header, modified to reflect an address other than that of the sender.

This type of IP spoofing would be used when the attacker is not as concerned about the response they get and would be common in Denial of Service attacks.

In this section, we are going to focus on a more complex attack in which the attacker is using IP spoofing to gain authorized access to a system by impersonating a trusted system.

We will look at two variations of IP spoofing that depend on the TCP 3-way handshake.

The TCP protocol follows a 3-way handshake when establishing a connection. The client sends a SYN packet to the host asking to connect, the host responds with a SYN ACK packet confirming the connection and finally the client responds with an ACK to acknowledge and the connection is established.

With Non-Blind IP Spoofing, the attacker leverages the TCP handshake between the target and authorized systems to gain authorized access.

This type of IP spoofing takes place when the attacker is on the same network segment as the target and the authorized system.



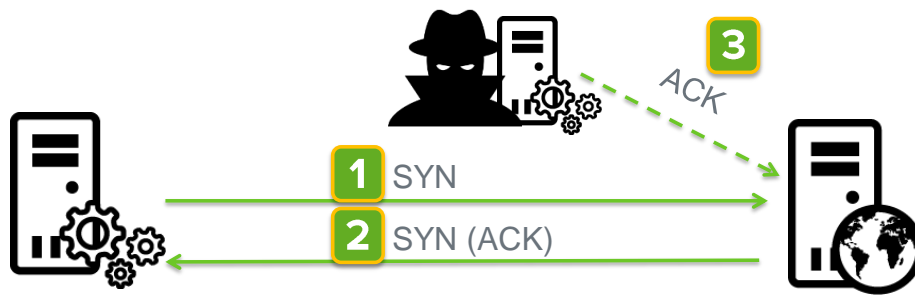
Blind IP Spoofing is very much the same as Non-Blind with one key difference; the attacker is not on the same network segment as the target and the authorized system.

As a result, they will need to modify the network packets they send as well to make the attack successful.

We will now look at how both of these attacks happen in further detail.

## Network Attacks (IP Spoofing — Non-Blind)

| Device      | IP           | MAC               |
|-------------|--------------|-------------------|
| Destination | 192.168.1.10 | 00-50-56-C0-00-10 |
| Source      | 192.168.1.20 | 00-50-56-C0-00-08 |
| Attacker    | 192.168.1.30 | 00-50-56-C0-00-01 |



Copyright© 2017 AlienVault. All rights reserved

32



A Non-Blind IP Spoofing attack happens as follows:

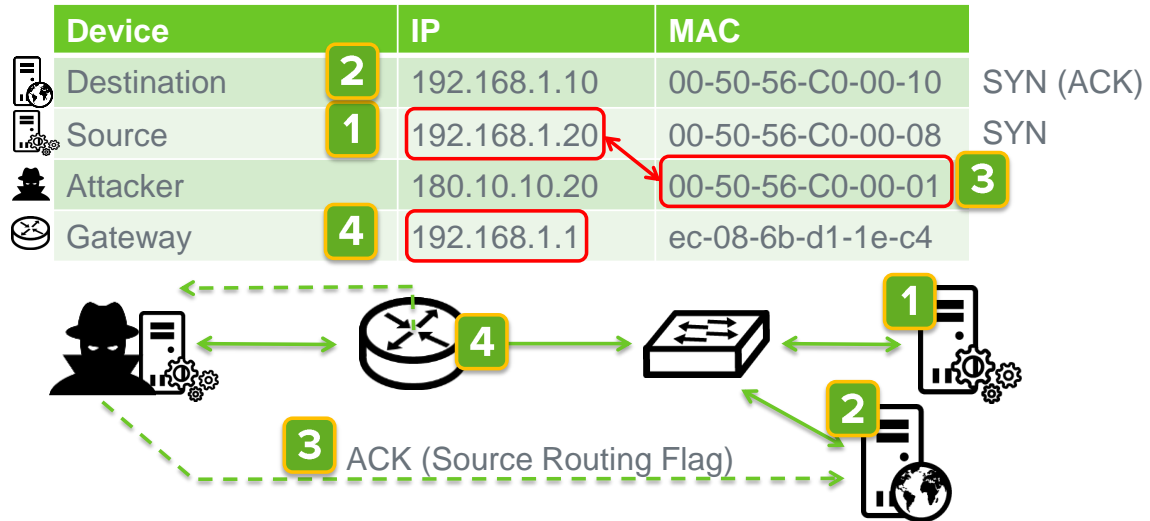
The trusted client sends a SYN packet to the target host asking to connect.

The host responds with a SYN ACK packet confirming the connection and waits for the trusted client, which responds with an ACK to acknowledge and the connection is established.

At this point, the attacker attempts to predict the TCP sequence number and responds with an ACK masquerading as the trusted client before they have a chance to respond.

If successful, the target host will now trust the attacker's MAC address as the correct way to reach the trusted client's IP, believing they are communicating with an authenticated source.

## Network Attacks (IP Spoofing — Blind)



Copyright© 2017 AlienVault. All rights reserved

33



A Blind IP Spoofing attack follows the same idea as a non-blind attack except there is an additional step required since the attacker is not on the same network segment as the trusted client and target server as shown here

The main difficulty for the attacker is there is a Layer 3 device between them and the victims of the attack and needs to find a way to make sure IP packets are routed out of their network so they can get to them.

The process starts the same as usual

The trusted client sends a SYN packet to the target host, asking to connect.

The host responds with a SYN ACK packet confirming the connection and waits for the trusted client to respond with an ACK to acknowledge and the connection is established.

Same as last time, the attacker attempts to predict the TCP sequence number and respond with an ACK masquerading as the trusted client before they have a chance to respond. This time however they modify something called the Source Routing flag in the packet header to ensure that the traffic coming from the target host is not dropped by the router or redirected to the legitimate client.

When this flag is turned on, the router must obey the options set by the attacker and thus the responses from the target host are forwarded to the attacker.



# Cryptographic Attacks

Copyright© 2017 AlienVault. All rights reserved

34



## Cryptographic Attacks



Copyright© 2017 AlienVault. All rights reserved

35



Until now we have discussed many ways that attackers can perpetrate attacks against victims and obtain their information by stealing data or eavesdropping on communications.

In most cases however it is not as straightforward as we have shown, as encryption is employed most of the time to make sure attackers just see a jumbled mess of data.

Communications between a client and a server are typically encrypted.

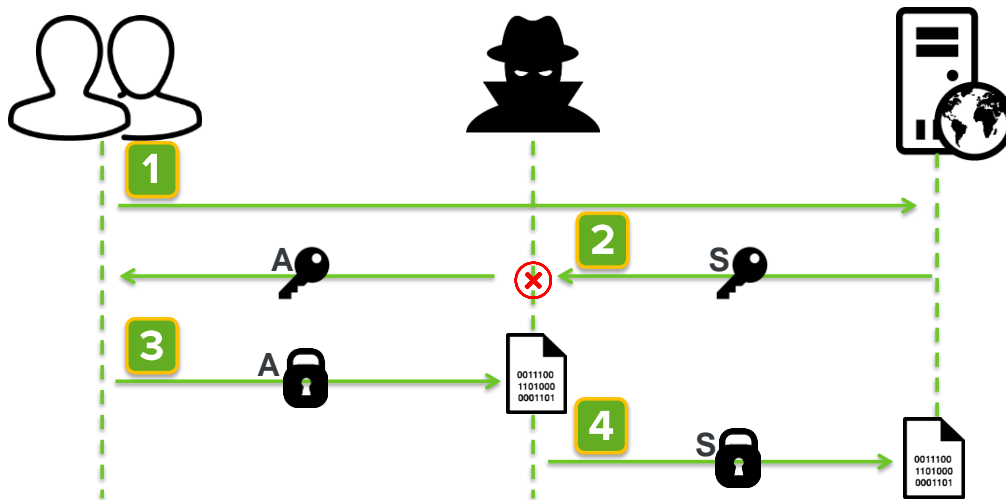
Private wireless networks are protected by a passkey that is required to connect and communicate on the network.

Even the passwords users use to access a system are protected so that they are not readable if the attacker gains access to the system.

Does this mean that attackers are unable to access the data and everything is totally safe? Unfortunately the answer is no.

Attackers have various methods of breaking the cryptography used to secure information and communications. We will review some of the methods they use in the following slides.

## Cryptographic Attacks (Man in the Middle)



Copyright© 2017 AlienVault. All rights reserved

36



The targets of this attack are mostly public key cryptosystems where key exchange is involved before communication takes place.

This type of attack would not be successful against a Private/Public key system such as HTTPS.

A client wants to communicate with the server, and requests the server's public key.

An attacker intercepts the response from the server and sends their public key to the client instead

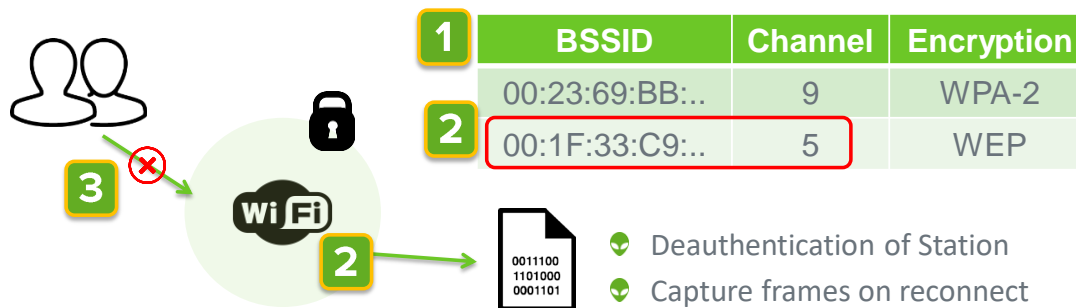
Now the client encrypts all communications to the server using the attacker's key and so the attacker is able to read all the information.

In order to maintain communication, the attacker re-encrypts the data with the server's public key after reading, and sends the data to the server.

Since it is encrypted with the correct key, the server believes it is talking to the client.

## Cryptographic Attacks (WiFi Cracking)

- ✔ Wired Equivalent Privacy
- ✔ WEP is vulnerable to attack due to predictability
- ✔ Use **Wifi Protected Access** instead



Copyright© 2017 AlienVault. All rights reserved

37



This topic could fall under network attacks; however it is included here as there is encryption algorithms employed to maintain the security of wireless networks is vulnerable to cryptographic attacks.

In the past many networks were protected by Wired Equivalent Privacy or WEP for short. Since the data on a wireless network is transmitted over the air, the traffic is very susceptible to sniffing, so WEP was employed to combat this type of attack.

Significant flaws were found in the WEP algorithm which made it predictable and very susceptible to cryptographic attacks that could crack the key quite easily.

Although WEP is still available today, WiFi Protected Access or WPA is a much stronger method of securing a wireless network, although it is not 100%.

Let's look at how an attacker would work to break into a WEP- or WPA-protected wireless network.

First the attacker lists all available wireless networks that are nearby, and gathers their information, such as the BSSID, channel, and encryption method.

The attacker will select the channel and BSSID of the network they want to break into and will start capturing traffic.

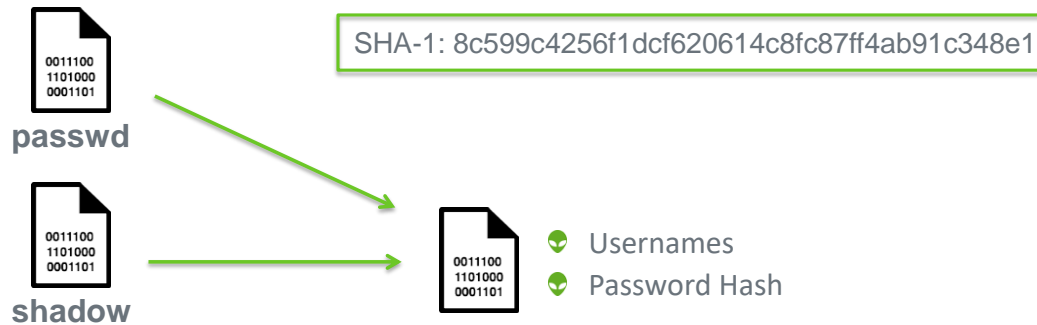
The attacker will then identify a connected device, called a station, and send a deauthentication message to it so it drops off the wireless network, forcing it to reconnect.

This will generate traffic that the attacker will capture and in turn perform a brute force attack on to find the key for the network.



## Cryptographic Attacks (Password Hash)

- 📌 Attacker has obtained password files
- 📌 Used against hashed passwords
- 📌 Same idea as brute force authentication



Copyright© 2017 AlienVault. All rights reserved

38



The final topic we will cover is the decryption of passwords when we already have access to the password files themselves.

We will be looking at how passwords are stored and represented on a Linux system; however the same theory is valid for other operating systems.

For security purposes, user passwords are not stored in plaintext on a system and are kept as a hash.

Hashing is a mathematical method used to produce a fixed length encoded string for any given string. The main strength of the hashing algorithm is the fact that you cannot detect the original string from the encoded string. You will get a unique fixed-length encoded string for any data you give, and that encoded string will be unique to that particular data. The hashing algorithms themselves are publicly available and there are lots of different hashing algorithms available with varying degrees of complexity.

Here is the SHA-1 for the word “unbreakable” >> <http://www.sha1-online.com/>. Note that SHA-256 and SHA-512 would be seen normally as they are far more complex and thus more secure, but the output of SHA-1 is short enough to display on screen.

As complex as these hashes are, they are not exempt from attack, and attackers can attempt to break them using methods similar to those discussed in the brute force authentication section.

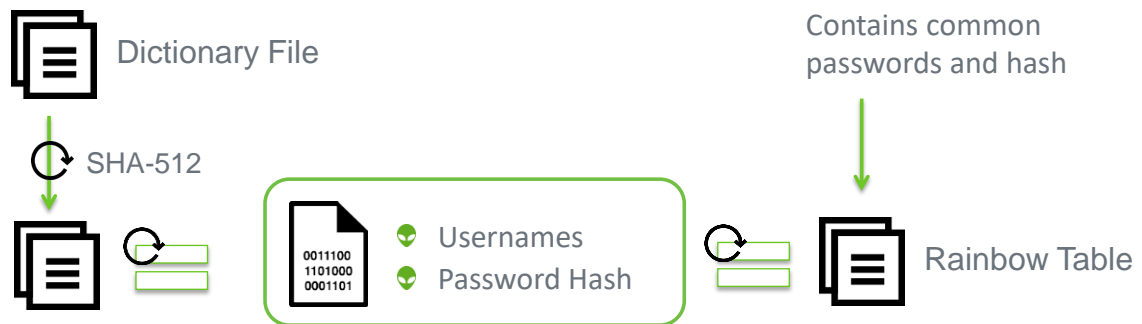
On Linux there are typically 2 files that represent the users and their related passwords.

Passwd contains the user information and a shadow file stores the hashed password as well as other information.

Once the attacker has both of these files, they can run a program that combines them into a single file that lists the user name and its related password hash. Now the attacker can attempt to crack the passwords.

## Cryptographic Attacks (Password Hash)

- 📁 Dictionary Attack
- 📁 Rainbow Tables
- 📁 Salting the Hash



Copyright© 2017 AlienVault. All rights reserved

39



There are a few different methods available to attempt to find a user's password based on the hash. We will discuss 2 here.

The first option is the Dictionary Attack, which is the same methodology as we discussed in the brute force authentication section.

A key component of the Dictionary Attack is the dictionary file, also known as a wordlist file. This file contains commonly used passwords as well as leaked information from sites that have had data breaches in the past.

The attack will systematically go through all the entries, creates a hash based on whichever hashing algorithm is required, and try and discover the correct password by comparing the hash.

The second option is to use a rainbow table to attack a hashed password in reverse.

That means the attacker has a table with hashes pre-calculated for potential passwords that are compared to the password hashes that they have obtained.

With the precomputed table, a simple lookup is now possible given the encrypted/hashed version of the password. If they can find the victim's encrypted/hashed version they can easily return the real plaintext password.

To deter these types of attacks, an operation called salting is employed that makes it more difficult for an attacker to discover a user's password.

A salt is random data that is used as an additional input when hashing a password. The salt and the password are concatenated and processed with the hash function, and the output is stored with the salt in a database.

## Summary

- We identified what motivates attackers.
- We introduced some common system vulnerabilities.
- We learned about attack delivery methods.
- We saw several attack types.



So let's review what was covered in this module:

- We identified the reasons attackers attempt to exploit networks and systems.
- We were introduced to some of the most common system vulnerabilities.
- We learned the methods by which attacks are delivered.
- We saw several attack types and how they are implemented at a high level.

If you have questions or want to learn more...

- Read the Documentation
- Explore Our Training Offerings
- Check Out Our Product Forums



Visit Our Website:  
[HTTPS://WWW.ALIENVAULT.COM](https://www.alienvault.com)



Questions? Feedback?  
[TRAININGHELP@ALIENVAULT.COM](mailto:TRAININGHELP@ALIENVAULT.COM)



Read the Documentation: <https://www.alienvault.com/documentation>

Explore Our Training Offerings: <https://www.alienvault.com/training>

Check Out Our Product Forums: <https://www.alienvault.com/forums>

[HTTPS://WWW.ALIENVAULT.COM](https://www.alienvault.com) | [TRAININGHELP@ALIENVAULT.COM](mailto:TRAININGHELP@ALIENVAULT.COM)

**AlienVault**

1875 S Grant St  
San Mateo, CA  
94402

Alienvault.com

t. (650) 713-3333

