# Global Information Assurance Certification Paper

# Script Kiddies: - What are they and what are they doing?

## Introduction:

Script Kiddies – We are talking about a far more sinister topic than the name suggests.
**Script** – Tells us that the people are using a pre written program or file to do something.
**Kiddies** – Small people, young people or perhaps someone who is 'not entirely sure' what they are doing.
In the following paper I will endeavor to cover this topic and hopefully, by the end of it, you will know what a Script Kiddie is, what they are doing, how you can avoid them and why you should be afraid of them.

## Who are they?

Here are a few points about the Script Kiddie.
They are people who have one thing in mind – To gain access to YOUR system.
The attacks that the Script Kiddies will do are for the most part RANDOM.
They are after easy targets and they don't mind how much noise they make while they are trying to acquire the target. The object is volume. How many systems that you "own" makes you a higher rank in the Script Kiddie world.
They usually have a small arsenal of tools, which are freely available on the Internet.
The tools that they have will allow them to exploit a small number of holes in systems.
They usually don't have much programming knowledge, or experience.
They are limited to the tools that they have already been shown how to use.

## So why are they a big threat then?

The threat comes from these people because they do things on a large scale. They will 'troll' the Internet in search of systems that are vulnerable to their particular hack or hacks that they know how to exploit, open that hole and then implement their script which will then in turn give them total control of the target system. One problem that is often overlooked is the laptop. At work it is protected by your company's security team, who are looking after the interests of the company and protecting the Crown Jewels. Now take this same laptop home and connect it to the Internet. All the Script Kiddie needs to do is put a Trojan on that laptop, wait for it to go back to work and boom, instant access to the crown jewels.

## Why has this happened?

This problem of the Script Kiddies has come about because of the huge expanse and boundless mass of the Internet. It only takes one person to work out how to pick a hole in the fabric of a system, then tell someone else, before long you have a script for the hack.

Then all that it takes is for someone to download it and type ‘go’. It really is that easy.

## Why they do it?

One reason is to help them stay connected on IRC ( Internet Relay Chat ). IRC is the Internet equivalent of the bulletin boards of yester year, and are used by many as a means to exchange ideas and information in. The Script Kiddie will use these IRC channels to gloat about the latest system that they have hacked or the amount of systems that they now own. It is also used to trade systems, passwords and other stolen information like credit card numbers. A reason that the Script Kiddie may want to 'own' your system is to add an IRC robot or bot for short. The IRC bot will be used to keep it’s owner on the IRC channel. People can be removed from an IRC channel for various reasons ( be it a Denial of Service attack or as simple as an Admin. kicking them off ). If the bots owner gets taken off the channel the bot will automatically bring them back on, or try to make them an Operator of the channel amongst other things. Once you get a few of these bots together, you can create a botnet. The botnet is in turn used to strengthen the stead of the Script Kiddie. ie: The more bots on your team, working in harmony, the greater the chance that you won’t get kicked off the IRC channel.

## How do they do it?

The process of taking control of your system is a 3 step process ( more if you count the acquisition of the tools and the learning of the process ). First, scan an address range on the Internet for systems that are alive, and are responding. During this initial scan the results are usually stored in a file or database for use in the 2nd step. Step 2. Use the address’s gained in the 1st step and check each one, for one or more known vulnerabilities. These vulnerable addresses are then stored for the 3rd step. Step 3. This is the manual step. Take each of the target systems and run the hack against it to gain root access. Once they are in the target system, download a ‘root kit’, create a couple of backdoors into the system, ( so that you can get back in later ) and then cover your electronic tracks ( by removing your presence from the system and security logs ) so that you are not caught. Once you ‘own’ the system you can do whatever you like, when ever.

## What can you do to stop them?

Well, stopping is something that you cannot ALWAYS do. There is NO silver bullet, not ‘one single’ thing that stop all attacks, but you can make it harder for them. Remember that the Script Kiddie is after EASY targets. Make your system a HARD target and you just MAY stop a lot of the Script Kiddies from looking at your system with that smile on their face. The best way to do this is to keep your system up to date with any security patches that are released from your OS manufacturer. Close any ports that are not needed to be open. Install and use an easily maintained firewall, and keep an eye on the system logs that are generated.

## What about retaliation?

Retaliation is usually not a good idea. This is because when the Script Kiddie attacks your system, they will normally be doing this from a stolen account, on a stolen system. This means that the source i/p address that you have gleaned and the account name that you have found will most likely NOT be the REAL person who is doing the damage. You can however report the events back to the System Administrator of the source system, so that they may clean their own back yard of the Script Kiddie.

## What is a Honey Pot and should I use one?

A honey pot is a system that is created to try and trap an attacker.
It is a system that has been created and put on the Internet, with no protection.
It is a 'typical install' of an Operating System, with NO patches.
The only extra software put on them is that used to record and trap an attacker.
They should not have any REAL data on them, as they are designed to be attacked.

These systems are an excellent learning tool, if you want to trap the tracks of an attacker and see how, when, where and what tools they use to gain access to your system. They must however be used with extreme care. If an attacker 'thinks' that they have been duped by a honey pot, they will erase the system and leave you with nothing. The Honey Pot will take a lot of work and should be constantly monitored, if you are to learn anything from the attack. It should be well planned and executed or else it could be used as a platform for an attack of others, or all data erased, like so many others before it.

## Summary:

In summary, a Script Kiddie is a form of Hacker that you should be most AWARE of. The tools that they use are considered potent, because of their wide spread availability, ease of use and damage that can be caused. Their affect on your system can however be minimized by simply being aware of and installing the latest system patches, closing the well known holes in your defenses and using a good firewall policy. These steps won't stop the determined ones, but, for the majority of them, they are only after the EASY KILL.

## References:

Spitzner, Lance “Know your Enemy” http://www.enteract.com/~lspitz/enemy.html ( 12 Nov. 2000 ).

Spitzner, Lance “Know your Enemy III” http://www.enteract.com/~lspitz/enemy3.html ( 12 Nov. 2000 ).

Brumley, David “ Tracking Hackers on IRC” http://theorygroup.com/Theory/irc.html ( 12 Nov. 2000 ).

Davis, Noel “The Danger of Script Kiddies” http://rootprompt.org/article.php3?article=756 (12 Nov. 2000 )

The official Site to the world's best underground information and search engines ! http://www.astalavista.com (12 Nov. 2000 )

Last Updated: May 26th, 2017

# Upcoming Training



| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Boston 2017 | Boston, MA | Aug 07, 2017 - Aug 12, 2017 | Live Event |