PM: How to play the SCI-FI game

Leif Nixon

April 3, 2013

1 Introduction

Welcome to the SCI-FI game, where you as a participant together with your team are responsible for the security of a galactic compute site within the United Federation of Planets. You will face attacks that are very similar to the attacks that we see in reality.

2 Background

You have been tasked with taking over the responsibility of your site after the previous administrator suddenly decided he was fed up with computers, and switched to an alternative career as a blacksmith.

There have been recent rumours about an expected Klingon cyber attack. Whether this influenced your predecessor's decision to resign is not known.

Unfortunately, the previous administrator was chronically overworked, and seldom had time to write documentation, so part of the challenge will be to quickly take stock of your systems.

Your site is being constantly used around the clock by researchers from all over the galaxy, which means you have to avoid downtime as far as possible. Also, since users are constantly travelling, it is very hard to predict from where they will log in.

3 Site architecture

Your site consists of three components; a web server, a cluster frontend, and a set of cluster compute nodes[1].

The **cluster frontend**, host name *team*.`space`, serves as the access point to the cluster for your end users; this is the system they log in to to compile code, submit batch jobs, and so on. This system also runs the SLURM batch server, and serves user home directories.

The **compute node**, host name *team*-`n1.space`, is used for running user compute jobs. This node is not intended for interactive use; all end user access should take place through the batch system.

The **web server**, host name *team*-`www.space`, runs a simple accounting portal which allows users to check on their historical CPU usage, and also provides users with home pages that they can e.g. use to download their output data or run custom web interfaces.

4 Attacks, incidents and flags

The game consists of a number of levels. In each level you will handle a **security incident**, which gets more complicated as the game progresses.

Basically, an incident occurs when an attacker gains access to something he shouldn't have access to. You can expect to see a constant stream of attacks against your site. Unsuccessful attacks do not count as incidents.

[1] Well, actually, there is currently only one compute node, due to the ongoing galactic credit crisis.

Security incidents may be discovered through your own monitoring, by reports from other sites, or through intelligence provided by Starfleet Command.

In each incident, the attacker will leave a number of telltale traces on your system in the form of a small number (2–3) of **flags**. A flag is a 40 character hexadecimal string that will be clearly identified as a flag. It may appear as a file name, as malware payload data, as a source code comment, as instructions on how to generate the flag string[2], or something else.

Note that the flag consists of *only* the 40 character hexstring, not any contextual data – if you find a file called

`the-flag-is-32a0617aab4c9fe725f1b5bc441291180ad25b73.txt`

the actual flag is just "32a0617aab4c9fe725f1b5bc441291180ad25b73".

You gain points by finding and reporting flags left by the attackers – cf. section 6.1.

You also gain points by writing and submitting incident reports documenting the incident. This is also how you progress to the next level – cf. section 6.2.

5 Connecting to the game

To connect to the game, visit `http://game.nixon-security.se` in your browser and log in with the team name and password you should have received on paper. This gives you access to the game management system.

On the Home tab, you can download a private ssh key that can be used to log in to your site machines. For security reasons, the game takes place on an isolated network that can only be reached through a gateway machine, called `stargate.nixon-security.se`. So, to reach your site, first log in to `stargate` with your team name (lower-case only) and the ssh key. From there you can log in as root on your team's machines, using the same key – for your convenience the key has been preinstalled on your account on `stargate`.

Tip: To view your site's web server (*`team`*`-www.space`), you can use OpenSSH's built-in SOCKS proxy support. If you login to `stargate` using the `-D` option, like this:

`ssh -D 9000 `*`team`*`@stargate.nixon-security.se`

you can then configure your browser to use `localhost:9000` as a SOCKS proxy, and all your browser's network accesses will be tunneled through `stargate`.

If you run Firefox, and you get name resolution problems, your browser is probably configured to resolve DNS names by itself, rather than letting the proxy do it. In this case, go to the `about:config` page and search for the setting **network.proxy.socks_remote_dns**. This should be set to **true**. After changing this setting, you will need to restart Firefox.

6 The game management system

The game management system is used to interact with the game and with Starfleet Command.

[2]Tip: If you need to calculate the SHA1 sum of a string, do `echo -n `*`string`*` | sha1sum`

6.1 Reporting captured flags

When you believe you have found a flag, in the form of a hexadecimal string, enter it into the "Capture Flag" box on the Home tab. If the flag is correct, you will be awarded 100 points for it, and it will be listed under "Captured Flags".

There is no punishment for reporting an incorrect flag string[3].

6.2 Submitting incident reports

When you feel that you have investigated an incident fully, you should submit an incident report. Click the corresponding entry under "Levels" (its state will be "Next Level to Report") and submit your report.

The report should describe the incident fully, including a timeline, what vulnerabilities (if any) that were exploited, involved user accounts, actions taken, what you have done to secure your system, and so on.

The report will be sent to Starfleet Command which will judge whether it is good enough. If not, it will be returned to you with feedback, and appear on your home tab with the state "Returned for editing". In this case, you will need to edit it and submit it for a renewed review.

Once your incident report is accepted, you will receive 50–100 points (depending on the quality of the report), proceed to the next level, and be subjected to a new incident to investigate.

Please note that you do not need to find all (or even *any*) flags to proceed to the next level; you only need to submit an acceptable incident report. Also, flags can be reported at any time; if you discover a flag that is left from a previous level, just report it.

6.3 Questions and user communication

If you need to send a question to Starfleet Command, you can do this using the Question box on the Home tab[4]. The answer will also appear on the Home tab.

If you need to communicate with a user – perhaps you need to tell Spock that his password has been reset – you can use the Question box also for this. Starfleet Command will forward your message to the user.

6.4 System monitoring

Your systems and services are continuously monitored for proper function. The current monitoring state of your site can be seen on the Home tab.

If any service or host is shown in red, it is down, and you need to take immediate action to bring it back into service. Extended downtime of a host or service may affect your score.

Services or hosts shown in yellow are in a warning state, which means they are still working, but are outside normal operational parameters. You should investigate this as soon as possible.

[3]But don't try to do a brute-force attack on flag strings. It won't work, and Starfleet Command will get irritated. You wouldn't like that.

[4]Of course, you can also just grab one of the teachers – that's what they are there for.

6.5 Dashboard

The Dashboard tab shows an overview of the complete game state, including scores, system states, and any services in an abnormal state. (Please note that correctly functioning services are not displayed on the Dashboard for reasons of brevity.)

The Dashboard also displays any incoming broadcast messages from Starfleet Command, so you will want to keep a close eye on this page.

7 Dos and Don'ts

Finally, all teams must follow certain ground rules.

7.1 Only play defense

You are strictly forbidden to attack other sites, the game servers or the attacking hosts. Basically, if an action would be unlawful or unethical in the real world, it is forbidden in the game.

7.2 Out of bounds areas

You are generally allowed to do anything you like with your site's systems, as long as services keep running[5]. However, to avoid disruptions to the game machinery, you should avoid or ignore certain things:

- You may assume that no malicious activity has taken place before the start of the game. There is no point in looking at e.g. filesystem timelines earlier than the game start; that data would probably just look weird.
- The root account on all servers comes prepopulated with an ssh key labeled "nixon@game". Do *not* remove this.
- The monitoring is run from the host `game.space` – be careful not to block this host, or your services will turn red.
- All hosts run a service called "nova-agent". Please ignore this; it is part of the hosting infrastructure. The same goes for any files with a ".nova" extension, and the network interface on the 10.0.0.0/8 network.
- The game infrastructure is configuration managed with Ansible – you may see references to Ansible in logs, etc. This is nothing to be concerned about.

[5]Short outages due to reboots or service restarts are OK, of course.