

SANS Penetration Testing

10 Nov 2015

Using the SSH "Konami Code" (SSH Control Sequences) (/blog/2015/11/10/protected-using-the-ssh-konami-code-ssh-control-sequences#)

0 comments (/blog/2015/11/10/protected-using-the-ssh-konami-code-ssh-control-sequences#respond) Posted by eskoudis (/blog/author/eskoudis)

Filed under Challenges (/blog/category/challenges), Methodology (/blog/category/methodology)

By Jeff McJunkin

Are you familiar with the Konami code (https://en.wikipedia.org/wiki/Konami_Code)? The one popularized by the Contra video game?



(<https://blogs.sans.org/pen-testing/files/2015/11/contra.jpg>)

Pictured above: Tangentially related to SSH

If not, let me fill you in. This code is a sequence of control actions for some video games that'll let you jump forward in the game (some call it a "cheat," but I'd rather not judge.). The code itself is a series of button presses as follows (from Wikipedia (https://en.wikipedia.org/wiki/Konami_Code)):



For me, learning about SSH control sequences felt like finding SSH's Konami code. First I learned how to kill an SSH client that wasn't responsive, which was convenient. Then, finding out about changing SSH's options *after I had established the connection* felt like cheating. Adding SOCKS proxies or local and remote port forwards after I've already connected to an SSH server is very useful, and far less annoying than typing my SSH key passphrase again.

So, how do you start a control sequence? First, make sure "Enter" was the last key you pressed, as the SSH client won't notice the control sequence otherwise. Next, press the tilde character (shift + backtick) followed by another character.

What are the support escape sequences, you ask? Well, press "?" as your second character, and your SSH client will tell you:

Supported escape sequences:

~. - terminate connection (and any multiplexed sessions)
 ~B - send a *BREAK* to the remote system
 ~C - open a command line
 ~R - request rekey
 ~V/v - decrease/increase verbosity (*LogLevel*)
 ~^Z - suspend ssh
 ~# - list forwarded connections
 ~& - background ssh (when waiting for connections to terminate)
 ~? - this message
 ~~ - send the escape character by typing it twice
 (Note that escapes are only recognized immediately after newline.)

Of these, I use "~." to kill stubborn SSH clients, "~C" to use additional SSH options (like "-D 8080" to start up a new SOCKS proxy), and rarely "~#" to see what forwards I've created.

Here's an example of me connecting to an SSH server (I set up the alias in my ~/.ssh/config file) and using an SSH control sequence to add a SOCKS proxy on port 9001 retroactively:

```

jeff@ccgateway2:~
jeff@jeff-laptop:~$ ssh ccgateway2
jeff@ccgateway2 ~ $
jeff@ccgateway2 ~ $
ssh> -D 9001
Forwarding port.
whoami
jeff
jeff@ccgateway2 ~ $
  
```

(<https://blogs.sans.org/pen-testing/files/2015/11/Jeff-1.png>)

An example of using an SSH escape sequence

Note the line beginning with "whoami". We were interacting with the SSH client itself at the line beginning with "ssh>", but when we finished that by pressing Enter, we didn't get a new prompt from the remote server. The input was still accepted, though, which is why the "whoami" command I typed returned "jeff" in the next line, followed by another newline and the SSH server's prompt.

Gosh, this is useful stuff.

Thanks for reading along! I hope you find as much use for the SSH Konami Code as I have.

- Jeff McJunkin

Follow @jeffmcjunkin { 3,909 followers }

I am teaching SEC560: Network Penetration Testing and Ethical Hacking (<https://www.sans.org/course/network-penetration-testing-ethical-hacking?msc=ptblog>) in San Francisco (<https://www.sans.org/event/san-francisco-fall-2018/course/network-penetration-testing-ethical-hacking?msc=ptblog>) in November 2018.

Upcoming SANS Special Event - Pen Test HackFest 2018

A promotional banner for SANS HackFest 2018. The top section has a red background with the event title 'SANS | HackFest' in white and yellow, followed by 'Information Security Summit & Training'. To the right, it says 'WASHINGTON, DC METRO AREA', 'Bethesda, Maryland', and the website 'www.sans.org/hackfest'. Below this, a photo of attendees at a laptop is shown. Overlaid on the photo are two white boxes: one for 'SUMMIT NOV 12 - 13, 2018' with '20+ Speakers', and another for 'TRAINING NOV 14 - 19, 2018' with 'Top SANS Pen Test Courses'. At the bottom, text describes 'EVENING BONUS SESSIONS' including 'CORE NETWARS EXPERIENCE' (Three Nights of) and 'CYBERCITY' (One Night of), both with a 1:87 scale physical model city. A quote from Jason Nickola, DTS, is on the left.

SANS | HackFest
Information Security Summit & Training

WASHINGTON, DC METRO AREA
Bethesda, Maryland
www.sans.org/hackfest

SUMMIT
NOV 12 - 13, 2018
20+ Speakers

TRAINING
NOV 14 - 19, 2018
Top SANS Pen Test Courses

"If you haven't attended a SANS Summit, it's hard to understand the immense value. This is even more true for Pen Test HackFest."
— Jason Nickola, DTS

EVENING BONUS SESSIONS:
Three Nights of
CORE NETWARS
EXPERIENCE
with Coin-A-Palooza

EVENING BONUS SESSION:
One Night of
CYBERCITY
1:87 SCALE - ICS/SCADA-ENABLED
PHYSICAL MODEL CITY

(<https://www.sans.org/hackfest?msc=ptbloghifimage>)

SANS Pen Test HackFest 2018 - Summit & Training

November 12-19, 2018 | Bethesda, MD (Washington DC Area)

- (2) Day Summit Event with 20+ Amazing Speakers on Pen Test & Red Team Topics
- Evening Networking Sessions
- (3) Nights of SANS Core NetWars, with Coin-A-Palooza
- (1) Night of CyberCity Missions
- Choose from (8) SANS Pen Test Training Courses
- Learn more: www.sans.org/hackfest (<https://www.sans.org/hackfest?msc=ptblog>)

"If you haven't attended a SANS Summit, it's hard to understand the immense value. This is even more true for Pen Test HackFest" - Jason Nickola, DTS

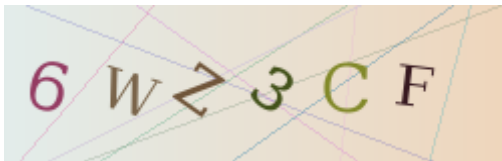
Permalink (/blog/2015/11/10/protected-using-the-ssh-konami-code-ssh-control-sequences) | Comments RSS Feed (/blog/2015/11/10/protected-using-the-ssh-konami-code-ssh-control-sequences/feed) - Post a comment |
Trackback URL (/blog/2015/11/10/protected-using-the-ssh-konami-code-ssh-control-sequences)

Post a Comment


*Name


*Email


Website

Comment*Captcha*****Response**

* Indicates a required field.

 (https://plusone.google.com/_/+1/confirm?hl=en&url=https://pen-testing.sans.org/blog/2015/11/10/protected-using-the-ssh-konami-code-ssh-control-sequences)

 (https://twitter.com/share?url=https://pen-testing.sans.org/blog/2015/11/10/protected-using-the-ssh-konami-code-ssh-control-sequences)

 (http://www.facebook.com/sharer.php?u=https://pen-testing.sans.org/blog/2015/11/10/protected-using-the-ssh-konami-code-ssh-control-sequences)

 Share

Categories

- Advanced Web App Pentesting (/blog/category/advanced-web-app-pentesting) (2)
- Anomaly Analysis (/blog/category/anomaly-analysis) (1)
- Anti-Virus Evasion (/blog/category/anti-virus-evasion) (7)
- Backdoor (/blog/category/backdoor) (2)
- Bash (/blog/category/bash) (11)
- Challenge Coins (/blog/category/challenge-coins) (1)
- Challenges (/blog/category/challenges) (26)
- Cheatsheet (/blog/category/cheatsheet) (8)
- cloud (/blog/category/cloud) (2)
- Command Line Kung Fu (/blog/category/command-line-kung-fu) (17)
- Conferences (/blog/category/conferences) (4)

- [Cryptography \(/blog/category/cryptography\)](/blog/category/cryptography/) (4)
- [CyberCity \(/blog/category/cybercity\)](/blog/category/cybercity/) (1)
- [Databases \(/blog/category/databases\)](/blog/category/databases/) (1)
- [Enumeration \(/blog/category/enumeration-2\)](/blog/category/enumeration-2/) (2)
- [Exploit Development \(/blog/category/exploit-development\)](/blog/category/exploit-development/) (4)
- [File Analysis \(/blog/category/file-analysis-2\)](/blog/category/file-analysis-2/) (2)
- [fuzzing \(/blog/category/fuzzing\)](/blog/category/fuzzing/) (1)
- [Infrastructure \(/blog/category/infrastructure\)](/blog/category/infrastructure/) (4)
- [Introduction \(/blog/category/introduction\)](/blog/category/introduction/) (3)
- [Legal Issues \(/blog/category/legal-issues\)](/blog/category/legal-issues/) (1)
- [Linux \(/blog/category/linux\)](/blog/category/linux/) (2)
- [Metasploit \(/blog/category/metasploit\)](/blog/category/metasploit/) (9)
- [Methodology \(/blog/category/methodology\)](/blog/category/methodology/) (47)
- [Mobile \(/blog/category/mobile\)](/blog/category/mobile/) (21)
- [Network Devices \(/blog/category/network-devices\)](/blog/category/network-devices/) (3)
- [Nmap \(/blog/category/nmap-2\)](/blog/category/nmap-2/) (2)
- [Passwords \(/blog/category/passwords\)](/blog/category/passwords/) (6)
- [Post Exploitation \(/blog/category/post-exploitation-2\)](/blog/category/post-exploitation-2/) (12)
- [Posters \(/blog/category/posters\)](/blog/category/posters/) (22)
- [PowerShell \(/blog/category/powershell\)](/blog/category/powershell/) (8)
- [Presentations \(/blog/category/presentations\)](/blog/category/presentations/) (10)
- [Protocol Analysis \(/blog/category/protocol-analysis\)](/blog/category/protocol-analysis/) (1)
- [Python \(/blog/category/python\)](/blog/category/python/) (20)
- [Quiz \(/blog/category/quiz\)](/blog/category/quiz/) (2)
- [Reporting \(/blog/category/reporting\)](/blog/category/reporting/) (4)
- [Scanning \(/blog/category/scanning\)](/blog/category/scanning/) (7)
- [scapy \(/blog/category/scapy\)](/blog/category/scapy/) (3)
- [Shell Fu \(/blog/category/shell-fu\)](/blog/category/shell-fu/) (5)
- [Summit \(/blog/category/summit\)](/blog/category/summit/) (1)
- [web pen testing \(/blog/category/web-pen-testing\)](/blog/category/web-pen-testing/) (17)
- [Welcome \(/blog/category/welcome\)](/blog/category/welcome/) (2)
- [wireless \(/blog/category/wireless\)](/blog/category/wireless/) (5)

Recent Posts

- [The Secrets in URL Shortening Services \(/blog/2018/08/30/the-secrets-in-url-shortening-services\)](/blog/2018/08/30/the-secrets-in-url-shortening-services/)
- [SANS Pen Test Challenge Coin: SEC460 \(/blog/2018/06/07/sans-pen-test-challenge-coin-sec460\)](/blog/2018/06/07/sans-pen-test-challenge-coin-sec460/)
- [SANS Cheat Sheet: Python 3 \(/blog/2018/05/22/sans-cheat-sheet-python-3\)](/blog/2018/05/22/sans-cheat-sheet-python-3/)
- [SANS Cheat Sheet: Netcat \(/blog/2018/02/28/sans-cheat-sheet-netcat\)](/blog/2018/02/28/sans-cheat-sheet-netcat/)
- [SANS Poster - White Board of Awesome Command Line Kung Fu \(PDF Download\) \(/blog/2018/01/17/sans-poster-white-board-of-awesome-command-line-kung-fu-pdf-download\)](/blog/2018/01/17/sans-poster-white-board-of-awesome-command-line-kung-fu-pdf-download/)

Archives

Select Month 

Links

- [Log in \(https://blogs.sans.org/pen-testing/login.php\)](https://blogs.sans.org/pen-testing/login.php)
- [Entries RSS \(/blog/feed/\)](/blog/feed/)
- [Comments RSS \(/blog/feed/comments/\)](/blog/feed/comments/)

Latest Blog Posts

The Secrets in URL Shortening Services (/blog/2018/08/30/the-secrets-in-url-shortening-services)
August 30, 2018 - 2:49 PM

SANS Pen Test Challenge Coin: SEC460 (/blog/2018/06/07/sans-pen-test-challenge-coin-sec460)
June 07, 2018 - 8:27 PM

SANS Cheat Sheet: Python 3 (/blog/2018/05/22/sans-cheat-sheet-python-3)
May 22, 2018 - 3:22 PM

Latest Tweets @SANSPenTest

SANS | #InfoSec Cheat Sheet Python 3 (Updated) by @MarkBagg [...]
(<https://twitter.com/SANSPenTest/statuses/1038133656961916928>)
September 7, 2018 - 6:35 PM

SANS | Webcast SANS Pen Test Poster: Blueprint - Building A [...]
(<https://twitter.com/SANSPenTest/statuses/1038052876902457344>)
September 7, 2018 - 1:14 PM

Do you know what SANS vLive Training is and how you can trai [...]
(<https://twitter.com/SANSPenTest/statuses/1037792276792131585>)
September 6, 2018 - 7:58 PM

Latest Papers

Times Change and Your Training Data Should Too: The Effect of Training Data Recency on Twitter Classifiers
(/resources/papers/gcih/times-change-training-data-too-effect-training-data-recency-twitter-classifiers-158420)
By Ryan O'Grady

Content Security Policy in Practice (/resources/papers/gcih/content-security-policy-practice-132604)
By Varghese Palathuruthil

Extracting Timely Sign-in Data from Office 365 Logs (/resources/papers/gcih/extracting-timely-sign-in-data-office-365-logs-137566)
By Mark Lucas

"This is the best hands-on course available anywhere."
- Whitney Janes, FedEx

"Ed Skoudis is the best teacher I've ever had. He is 100% competent and professional."
- Petra Klein, FRA

"This was by far the best course I have ever taken."
- Peter Lombars, Intrucom Inc.

 (<http://twitter.com/SANSPenTest>)  (<https://www.facebook.com/pages/SANS-Institute/173623382673767>)  (/blog/feed/)

[Resources \(/resources/\)](/resources/) | [Courses \(/courses/\)](/courses/) | [Events \(/events/\)](/events/) | [Certification \(/certification/\)](/certification/) | [Instructors \(/instructors/\)](/instructors/) | [About \(/about/\)](/about/)

© 2008 - 2018 SANS™ Institute