

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8A  
n1Nn2Nn3Nn4Nn5Nn6Nn7Nn8Nn9No0No1No2No3No4No5No6No7No8N  
0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9  
Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0  
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8A  
n1Nn2Nn3Nn4Nn5Nn6Nn7Nn8Nn9No0No1No2No3No4No5No6No7No8N  
Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0  
0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9E  
m0Km1Km2K@3Km4KinectaSploitm5Km6Km7Km8Km9Kn0KnKn2Kn3Kn  
3e9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg  
n1Nn2Nn3Nn4Nn5Nn6Nn7Nn8Nn9No0No1No2No3No4No5No6No7No8N  
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8A  
Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9Bh0  
In1Nn2Nn3Nn4Nn5Nn6Nn7Nn8Nn9No0No1No2No3No4No5No6No7No8  
0Bb1Bb2Bb3Bb4Bb5Bb6Bb7Bb8Bb9Bc0Bc1Bc2Bc3Bc4Bc5Bc6Bc7Bc8Bc9  
9Bf0Bf1Bf2Bf3Bf4Bf5Bf6Bf7Bf8Bf9Bg0Bg1Bg2Bg3Bg4Bg5Bg6Bg7Bg8Bg9  
1Nn2Nn3Nn4Nn5Nn6Nn7Nn8Nn9No0No1No2No3No4No5No6No7No8N  
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8

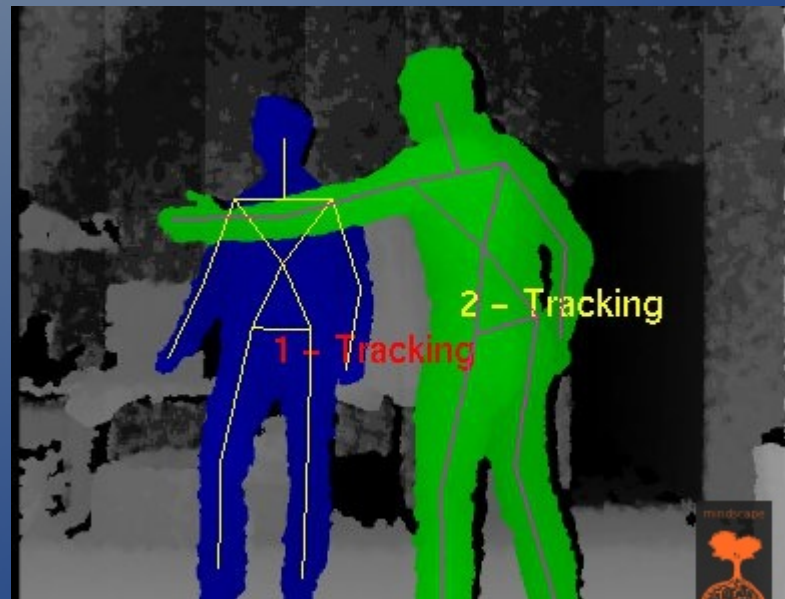
# KinectASploit

What if you took a  
kinect



# KinectASploit

Used it's skeleton tracking feature:



# KinectASploit

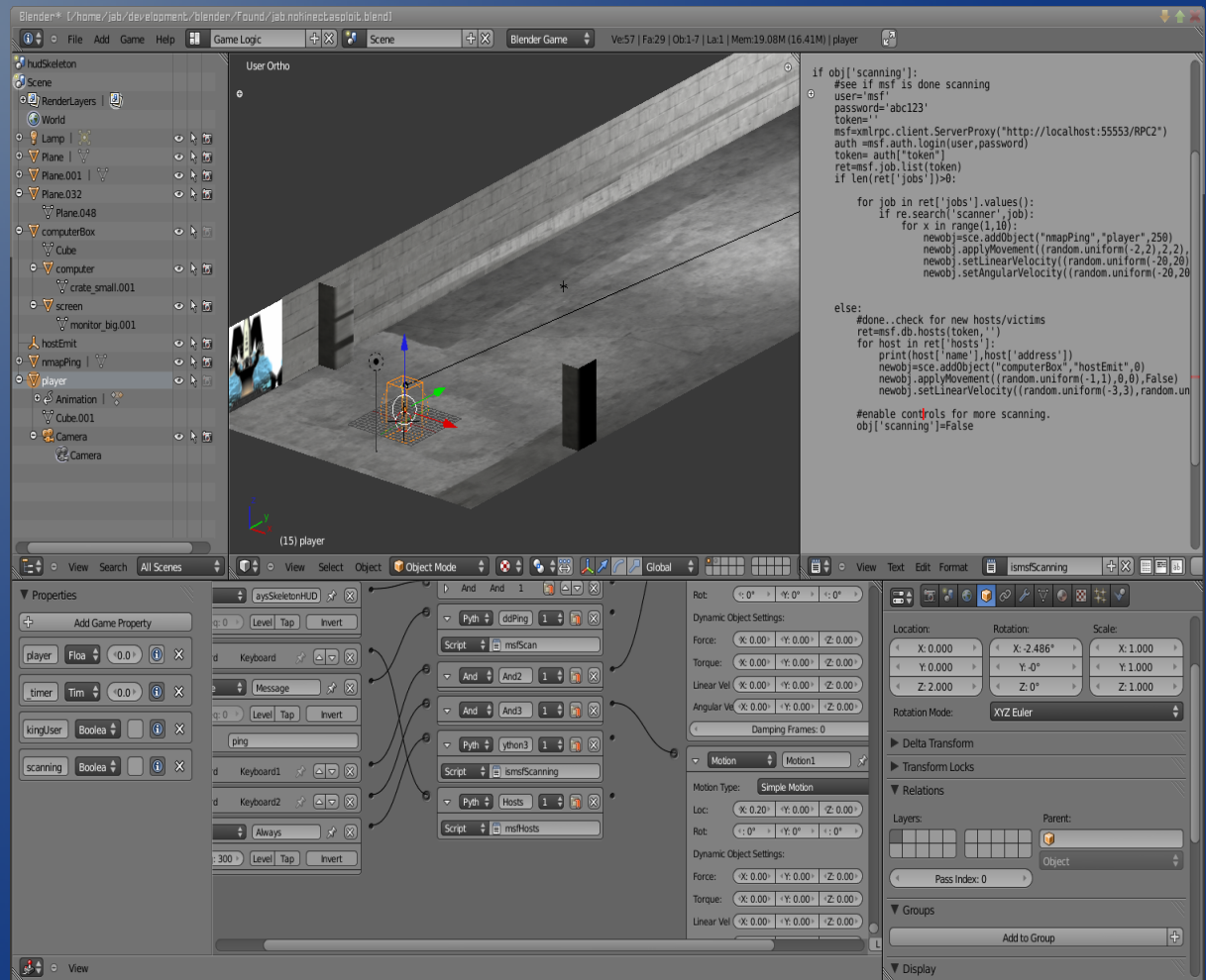
Sprinkled in some  
hacking tools:

```
1 /tcp      open      hosts2-ns
2 [mobile]
3 Starting nmap V. 2.54BETA25
4 Insufficient responses for TCP sequencing (3), OS detection may be less
5 accurate
6 Interesting ports on 10.2.2.2:
7 (The 1539 ports scanned but not shown below are in state: closed)
8 Port      State      Service
9 22/tcp    open      ssh
10
11 No exact OS matches for host
12
13 Nmap run completed -- 1 IP address (1 host up) scanned
14 # sshnuke 10.2.2.2 -rootpw="210N0101"
15 Connecting to 10.2.2.2:ssh ... successful.
16 Attempting to exploit SSHv1 CRC32 ... successful.
17 Resetting root password to "210N0101".
18 System open: Access Level <9>
19 # ssh 10.2.2.2 -l root
20 root@10.2.2.2's password:
21
22 PRE-CONTROL> disable grid nodes 21 - 48
```



# KinectASploit

And combined them  
with a 3D Game Engine:



# Lets find out!

Come see the Demo at  
Defcon19 and look for the tool  
source at:

<http://p0wnlabs.com/defcon19>

Any graphics that look good  
were probably found on  
[wallbase.net/4chan](http://wallbase.net/4chan).

Bad Code by jeff bryner  
[p0wnlabs.com](http://p0wnlabs.com)  
Use @ your own risk