

Minecraft Network Defense

Security Education with Competitive Minecraft Scenarios

05 Nov 2016

Will Woodson, @wjwoodson



whoami

“**Will is an InfoSec Person** in San Antonio, TX. He has several years of professional experience in security operations and is currently pursuing a graduate degree in cyber security from UTSA.”

What am I talking about?

- Minecraft level set and adversary analysis
- How the game Minecraft can be used to effectively demonstrate network security and network defense concepts.
- Tools and ideas for you to use Minecraft for security education.
- Live Demo?

Minecraft

Minecraft

Level Set



Minecraft

Level Set



Minecraft

Level Set



Minecraft

Level Set



Network Defense? In Minecraft?

- It's more likely than you think.
- Adversaries
- Sample Mapping

Minecraft

Characteristics

- Common
- Lots of HP
- Slow
- Can't climb walls

Adversaries:
Zombie



Minecraft

Adversaries:
Spider

Characteristics

- Climb walls
- Only attack in low light



Minecraft

Characteristics

- Ranged attack
- High damage
- Flee from attackers

Adversaries:
Skeleton



Minecraft

Adversaries:
Creeper

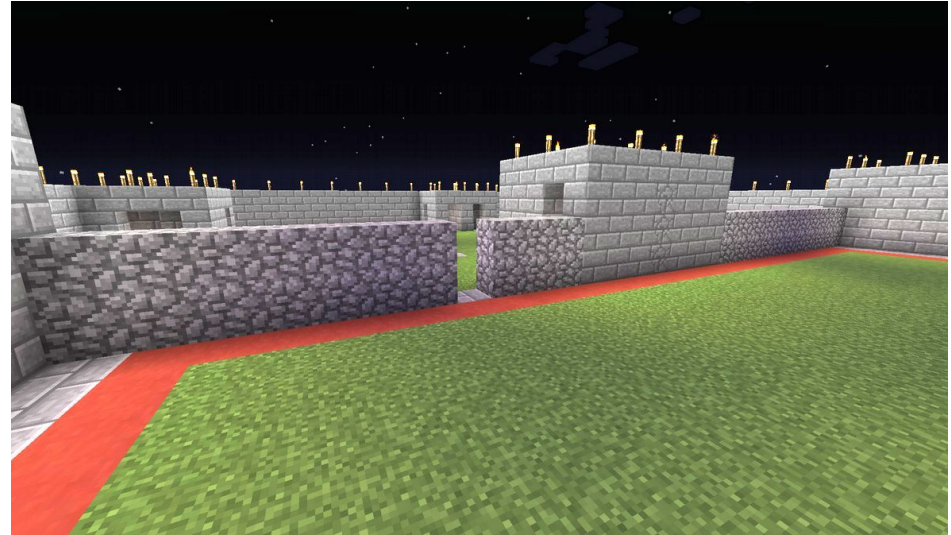
Characteristics

- Explosion destroys blocks
- Does a **ton** of damage
- Only detonates when close to player



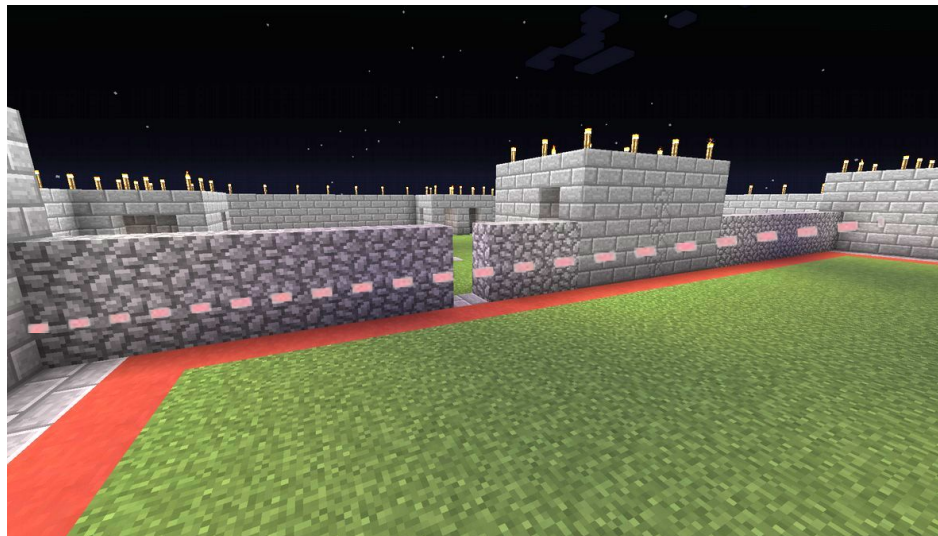
Minecraft

Sample Mapping



Minecraft

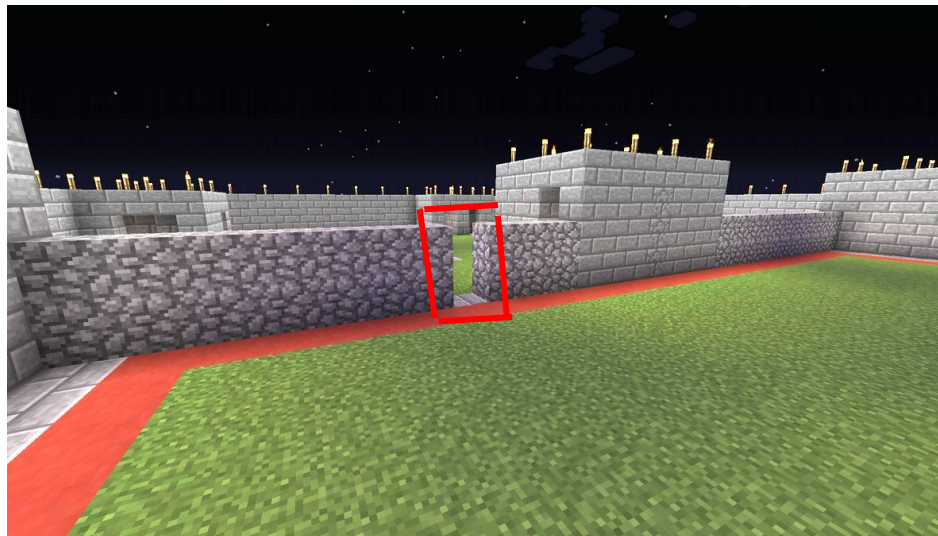
Sample Mapping



Minecraft

Sample Mapping

| Source | | | | Destination | | | |
|---|---------|------|-------------|---|---------|---|---|
| Zone | Address | User | HIP Profile | Zone | Address | Application | Action |
|  Trust | any | any | any |  Untrust | any |  citrix  ssl  web-browsing |  |
|  Trust | any | any | any |  Untrust | any |  gotomeeting  youtube |  |
|  Guest | any | any | any |  Untrust | any |  facebook  gmail-base |  |
|  Guest | any | any | any |  Untrust | any |  web-browsing |  |



Application of Network Defense

Application of Network Defense

The Firewall

- Resource allocation and cost/benefit
 - Defense setup time
 - Limited # of firewall blocks available
 - Defense against external threats vs. internal network segmentation

Application of Network Defense

Threat Types

- External/ commodity
 - Firewall works well
- “Sophisticated attackers”/ insiders
 - Active monitoring, segmentation, response

Application of Network Defense

Threat Intel

- Threat intelligence gathering
 - Time commitment/ resource allocation CBA
- Active defense risk/reward
 - You don't get points for vanquishing adversaries
 - Personal risk

Minecraft Network Defense

→ <https://github.com/wjwoodson/minecraft-vuln-mgt/> ←

Minecraft Network Defense

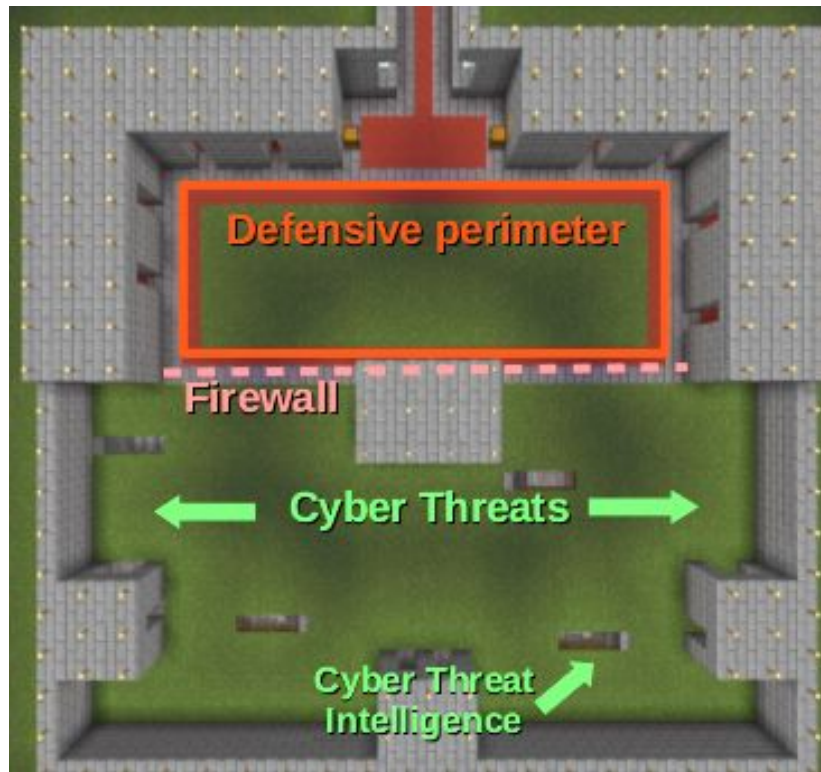
The Scenario

- Defend your **network** against **cyber threats** in this 10 minute 2-4 player Minecraft scenario:
 - build a **firewall** to keep attackers out of a defensive perimeter
 - use **cyber defense tools** to stop the bad guys
 - go **hunting** for **cyber threat intelligence**
 - **sophisticated attackers** might already be inside your network!

Minecraft Network Defense

Your Network

- Build a **firewall** in order to create a **defensive perimeter** within your network.
- The longer you are able to keep attackers from entering the defensive perimeter the more points you will score.



Minecraft Network Defense

Security Tools

- You will be provided with materials for building the **firewall** as well as **cyber defense tools** (sword and armor)
- Make sure to defend yourself too, as **deaths will count against your score**



Minecraft Network Defense

Cyber Threat Intel

- You can earn more points by collecting **cyber threat intelligence** from the network outside your defensive perimeter.
- Threat intelligence blocks can be found in tunnels below the base after attackers begin to spawn.



Minecraft Network Defense

Sophisticated Attackers

- **Sophisticated attackers** will come from **within the perimeter**
- Try to stop them as quickly as possible using your **cyber defense tools**



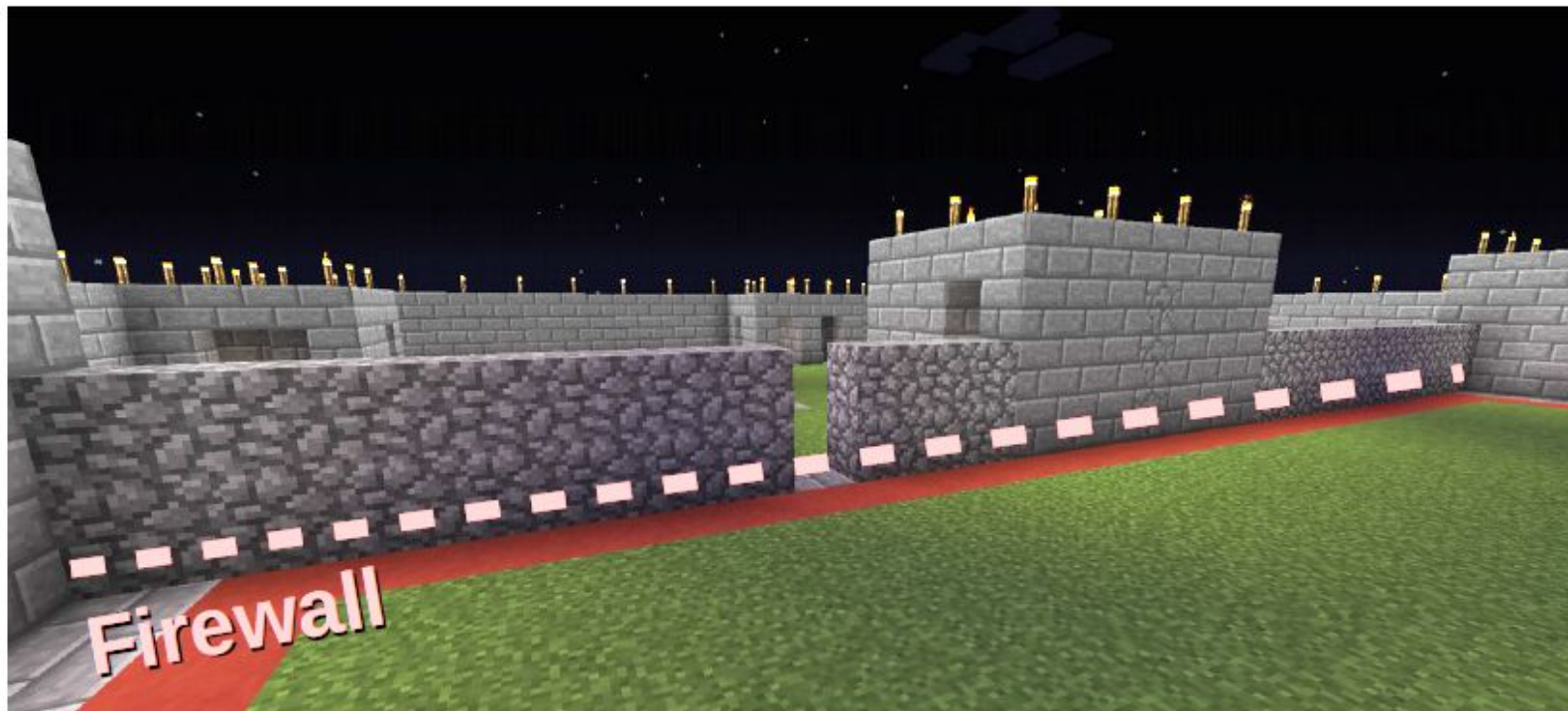
Minecraft Network Defense

Strategies

- Build a **firewall** between **external threats** and internal network
 - Allow egress
- Eliminate **external threats** and go gather **threat intel**
 - This is risky
- Monitor for **potential vulnerabilities** within internal network
 - **Sophisticated attackers / insiders** will show up eventually

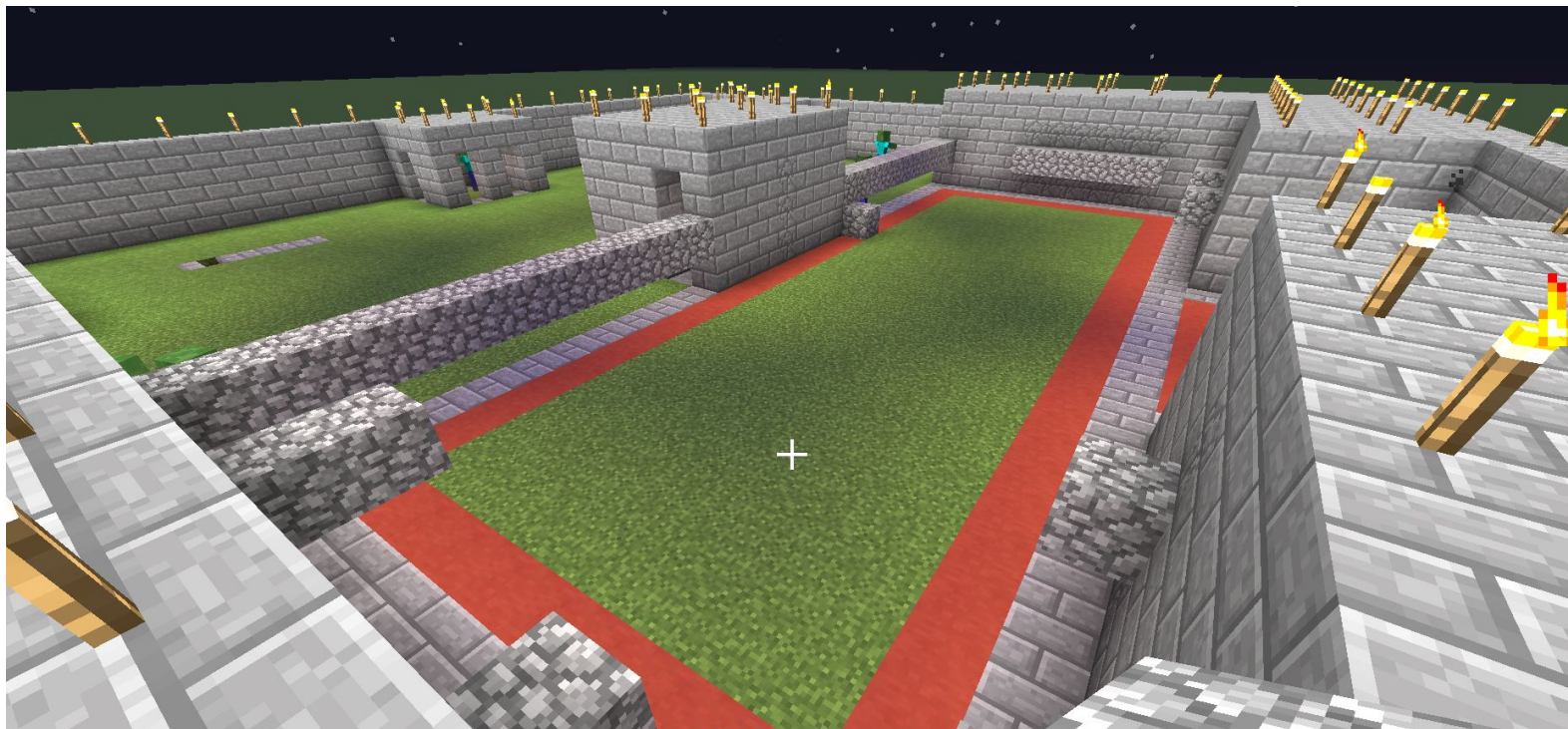
Minecraft Network Defense

Strategies



Minecraft Network Defense

Strategies



Minecraft Network Defense

Strategies



DIY

MINECRAFT
Network Defense

DIY

- I believe that children are, in fact, our future
- **Please run a (this) scenario yourself** in a game of your choosing (Minecraft) **soon**
- Fork repo, add more engaging and intricate blue team scenarios
 - Or pick something in Security, Technology, CS, etc. **and do it.**

“Threat Modeling the Minecraft Way” - Jarred White

(https://www.rsaconference.com/writable/presentations/file_upload/spo2-t10-threat-modeling-the-minecraft-way.pdf)

“Mining Learning and Crafting Scientific Experiments: A Literature Review on the Use of Minecraft in Education and Research” -

Nebel et al. (http://www.ifets.info/journals/19_2/26.pdf)

Minecraft Network Defense

- Applying real world security concepts within games
- Competition between players + measured guidance for how to do well
- Varied ways to score points - perimeter security, IR, etc.

Demo

MINECRAFT
Network Defense

Minecraft Network Defense

Future Plans

- Non-breaking issues requiring manual administrator config/setup time in game.
 - Add whitelist.json configurator
 - Migrate player name whitelists to central file (back with whitelist.json)
 - Add auto-provision & equip firewall materials + sword/armor to beginning of scenario.
- Additional Scenarios
 - More complex adversaries - spiders, skeletons, creepers
 - Patch vulnerabilities in automated system
 - Player collaboration & role division
 - Adversarial scenario - attack & defend

Questions

Minecraft Network Defense

Security Education with Competitive Minecraft Scenarios

→ <https://github.com/wjwoodson/minecraft-vuln-mgt/> ←

05 Nov 2016

Will Woodson, @wjwoodson

