Spawning Your First Shell

Jake Smith
University of Virginia

Cybersecurity News Segment

Disclaimer:

Only perform attacks on networks you own or are specifically authorized to. This information is for educational purposes only. The author is not liable for any misuse or damage.

NICE Challenge Portal

- Visit: https://portal.nice-challenge.com
- Sign-in with your username/password
  - Should have been emailed
  - Usernames look like virginia-jts5np
- Click Workspaces Available
- EternalBlue -> Deploy

Blue Team

- Keep hardware/software up to date
- Security monitoring
- Respond to incidents
- Think about “how to balance security, usability, and risk”

Purple Team

Red Team

- Test security controls
- Emulate threats and adversaries
- Think about “how to break stuff”

Why learn how to attack?

- Raise the overall security posture of the organization
- Assist the blue team to improve defenses and practice

ETERNALBLUE

Server Message Block (SMB)

- Provides access to file shares, printers, etc
- Several versions: SMBv1/CIFS, SMB 2, SMB 3
- Runs on Port 445 over TCP

The case of MS17-010

- On March, 14th, 2017, Microsoft published a critical security bulletin, MS17-010
- “Security Update for Microsoft Windows SMB Server”
- “The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server”

The Leak

- On April 14th, 2017, The Shadow Brokers released a set of exploits purported to belong to the NSA on Twitter
- Contained a number of tools that can be used to target Windows Operating Systems

The Aftermath

But a fix was released first?

The Attack / Metasploit

- We'll exploit a vulnerable Windows Server 2008 computer vulnerable to ETERNALBLUE
- We'll use Metasploit, an all-in-one exploitation and C2 framework

Persistence & Post-Exploitation

- Persistence: maintaining access through several methods
- Post-Exploitation: you've compromised a server, now what?
- After gaining access, we'll create a new user and a share so we can get back in later

The Defense / Patching

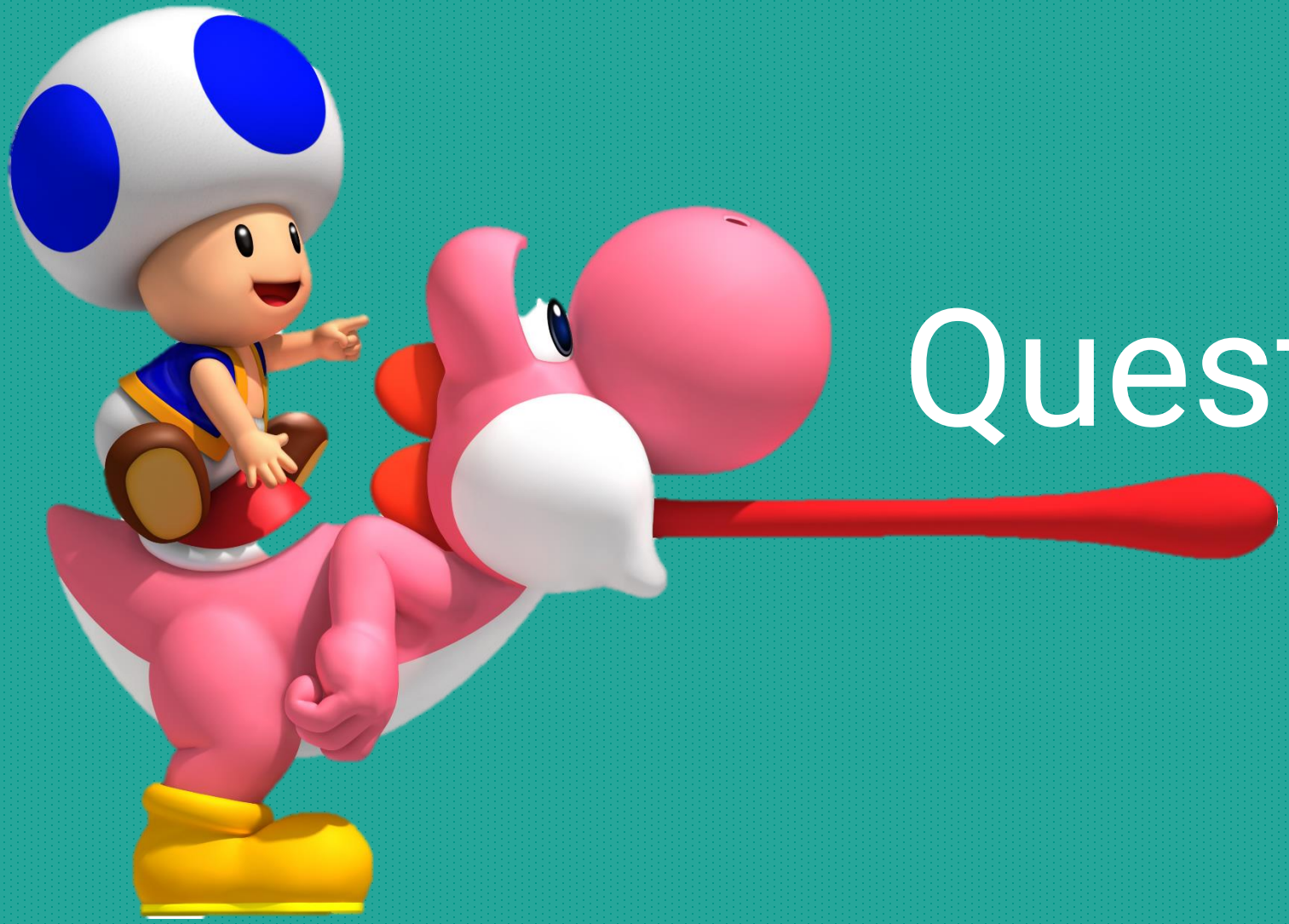
- At the end, we'll apply KB4013389, the patch for MS17-010
- We'll try to rerun the same exploit, but will fail

Hands-on Hackin’ Time

Hands-on Hackin’ Time

Sources

- https://isc.sans.edu/forums/diary/ETERNALBLUE+Windows+SMBv1+Exploit+Patched/22304/
- https://en.wikipedia.org/wiki/The_Shadow_Brokers#ETERNALBLUE
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010#executive-summary
- https://en.wikipedia.org/wiki/Server_Message_Block
- https://pbs.twimg.com/media/DSy0OkmX4AAhb46.jpg



Questions?