


Automating Security with PowerShell

Jaap Brasser
@jaap_brasser



jaapbrasser.com/about



 @Jaap_Brasser

Agenda

P O W E R S H E L L



PowerShell

& .\Demo

Defensive
Offensive

& .\Demo

Q & A

State of PowerShell



Demo Mimikatz & PowerShell Logging



Demo Summary

- Setup PowerShell logging
- Dump credentials
- Reconfigure logging
- Follow bread crumbs
- Determined what ran



Offensive PowerShell

Demo Obfuscation & Detection



Demo Summary

- Determined character frequency
- Used Vector Frequency
- Encoded existing scripts
- Looked at different methods of obfuscation



Defensive PowerShell

A close-up of Baby Groot from the movie Guardians of the Galaxy. He is a small, tree-like creature with a large head and small body, looking up with a surprised expression. The background is dark and blurry, suggesting a space environment.

Questions

References

- github.com/jaapbrasser/Events/tree/master/BSidesAms2017
- www.bsidesams.nl
- jaapbrasser.com