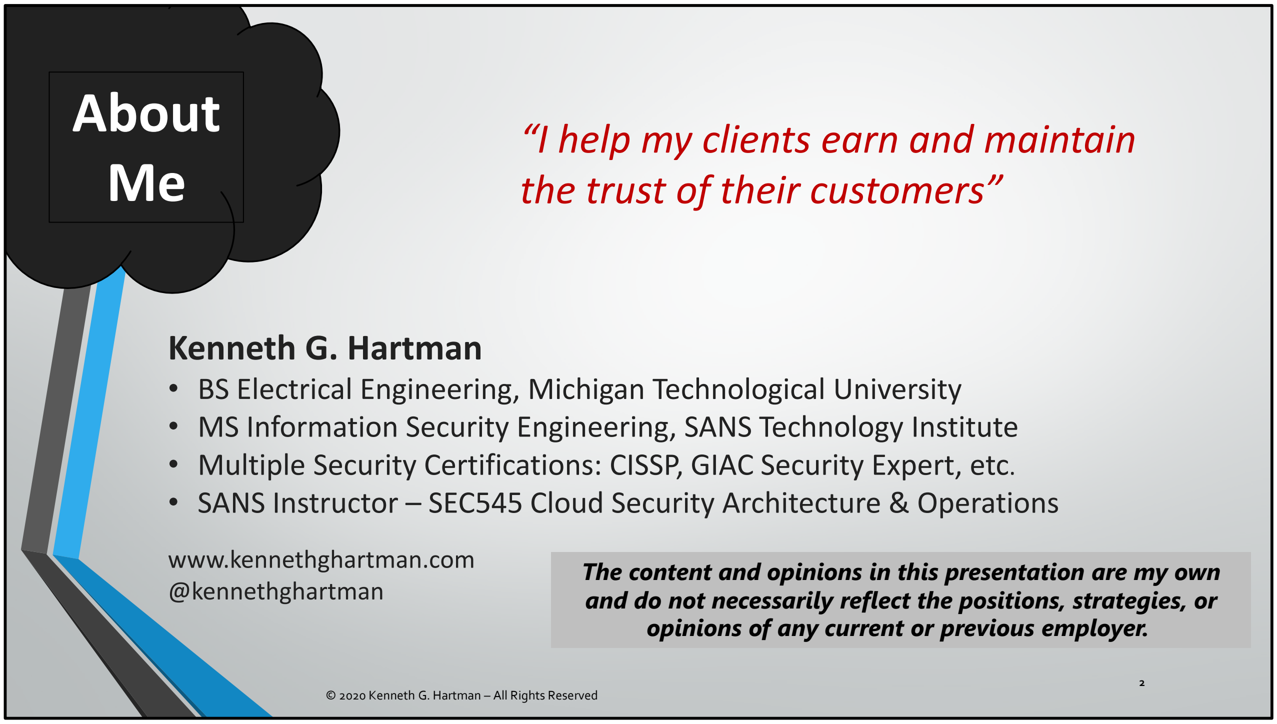
A Purple-Team Approach to Exploring AWS Security Services & Capabilities

Kenneth G. Hartman

Abstract:
Kenneth G. Hartman will demonstrate common attacks on a load-balanced WordPress EC2 Instance with poor security and showcase how that activity can be detected using cloud-native AWS technologies such as GuardDuty, VPC Flow Logs, CloudTrail, Athena, Config, and CloudWatch. At SANS, we believe that nothing beats hands-on experience, and the goal of this talk is to encourage you to use the cloud as your personal lab for sharpening your offensive and defensive skills.



About Me

"I help my clients earn and maintain the trust of their customers"

Kenneth G. Hartman

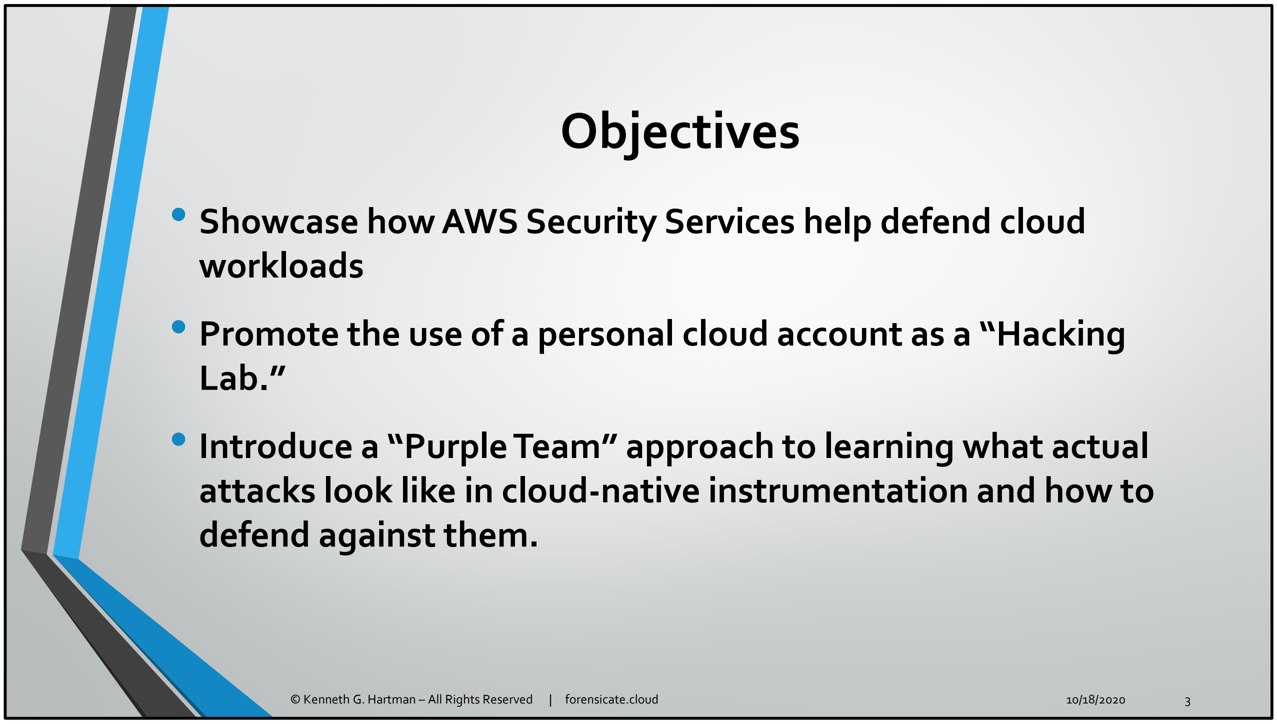
- BS Electrical Engineering, Michigan Technological University
- MS Information Security Engineering, SANS Technology Institute
- Multiple Security Certifications: CISSP, GIAC Security Expert, etc.
- SANS Instructor – SEC545 Cloud Security Architecture & Operations

www.kennethghartman.com
@kennethghartman

The content and opinions in this presentation are my own and do not necessarily reflect the positions, strategies, or opinions of any current or previous employer.

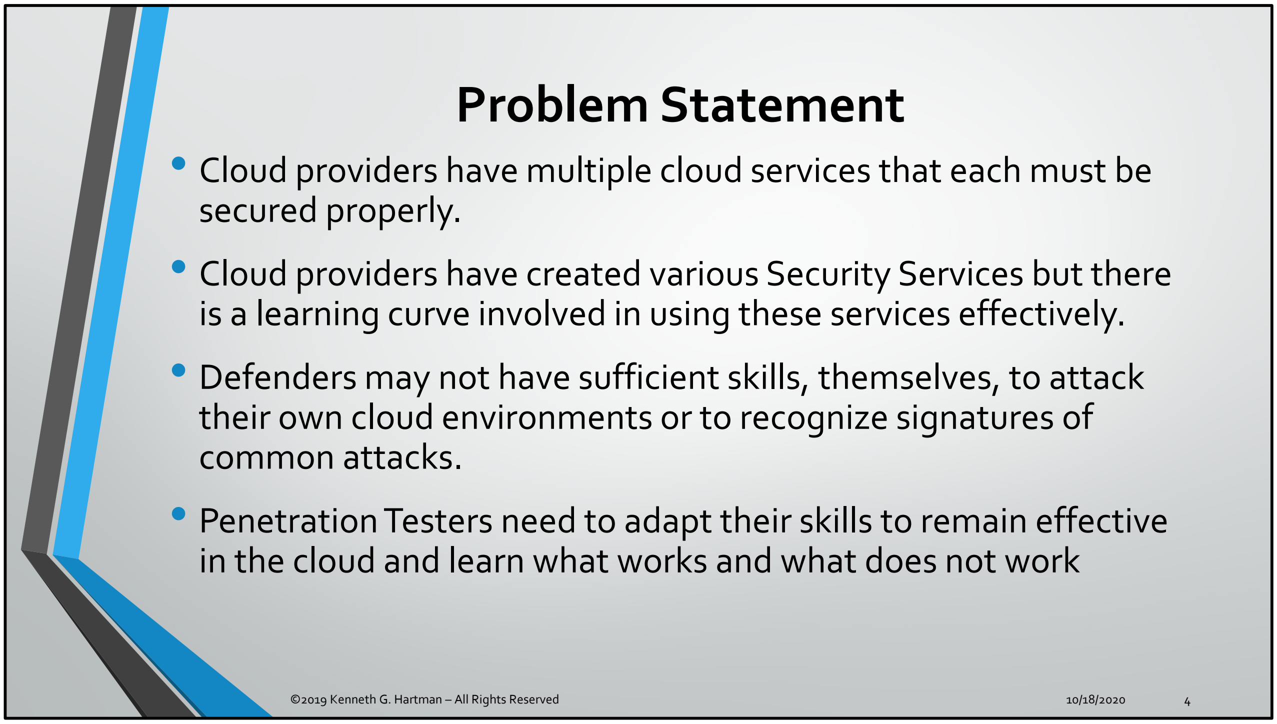
Kenneth G. Hartman - BIO

Kenneth G. Hartman is a security consultant based in Traverse City, Michigan. Ken's motto is "I help my clients earn and maintain the trust of their customers in its products and services." Toward this end, he consults on a comprehensive program portfolio of technical security initiatives focused on securing client data in the public cloud. Ken has worked for a variety of Cloud Service Providers in both the Midwest and Silicon Valley in architecture, engineering, compliance, and security product management roles. An instructor for SEC545: Cloud Security Architecture and Operations and SEC488: Cloud Security Essentials, Ken has also been the co-chair of the 2019 SANS Cloud Security Operations Solutions Forum, the 2019 and 2020 SANS Cloud & DevOps Security Summits.



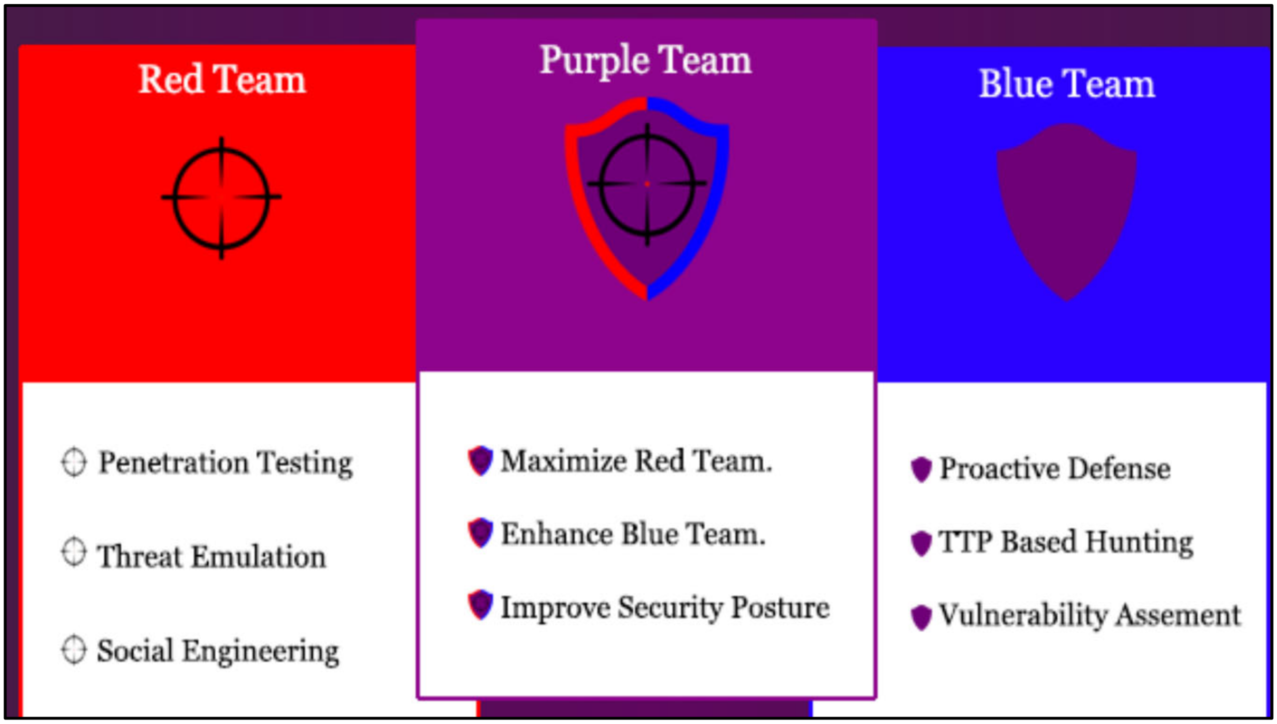
Objectives

- Showcase how AWS Security Services help defend cloud workloads
- Promote the use of a personal cloud account as a “Hacking Lab.”
- Introduce a “Purple Team” approach to learning what actual attacks look like in cloud-native instrumentation and how to defend against them.



Problem Statement

- Cloud providers have multiple cloud services that each must be secured properly.
- Cloud providers have created various Security Services but there is a learning curve involved in using these services effectively.
- Defenders may not have sufficient skills, themselves, to attack their own cloud environments or to recognize signatures of common attacks.
- Penetration Testers need to adapt their skills to remain effective in the cloud and learn what works and what does not work



Red Team

- Penetration Testing
- Threat Emulation
- Social Engineering

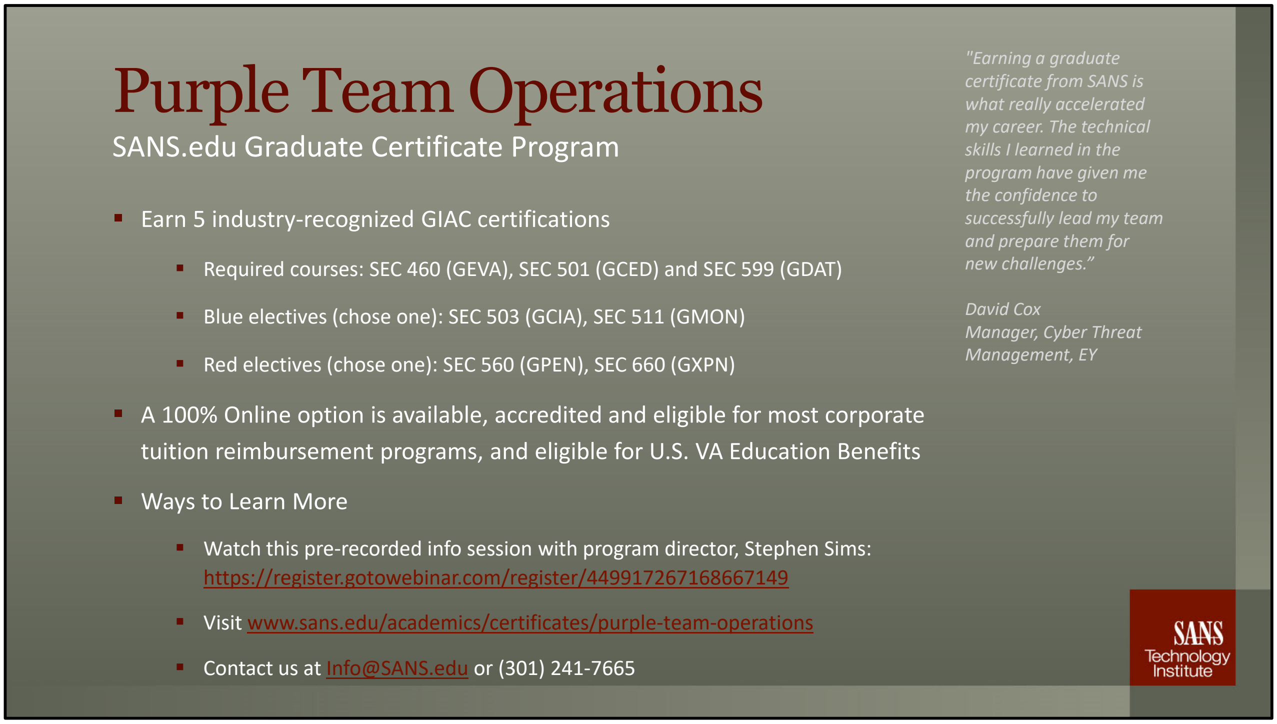
Purple Team

- Maximize Red Team.
- Enhance Blue Team.
- Improve Security Posture

Blue Team

- Proactive Defense
- TTP Based Hunting
- Vulnerability Assement

Image from: https://purpleteamfieldmanual.com/



Purple Team Operations

SANS.edu Graduate Certificate Program

- Earn 5 industry-recognized GIAC certifications
  - Required courses: SEC 460 (GEVA), SEC 501 (GCED) and SEC 599 (GDAT)
  - Blue electives (chose one): SEC 503 (GCIA), SEC 511 (GMON)
  - Red electives (chose one): SEC 560 (GPEN), SEC 660 (GXPN)
- A 100% Online option is available, accredited and eligible for most corporate tuition reimbursement programs, and eligible for U.S. VA Education Benefits
- Ways to Learn More
  - Watch this pre-recorded info session with program director, Stephen Sims: https://register.gotowebinar.com/register/449917267168667149
  - Visit www.sans.edu/academics/certificates/purple-team-operations
  - Contact us at Info@SANS.edu or (301) 241-7665

"Earning a graduate certificate from SANS is what really accelerated my career. The technical skills I learned in the program have given me the confidence to successfully lead my team and prepare them for new challenges."

David Cox
Manager, Cyber Threat Management, EY

SANS Technology Institute

Preventive Controls vs Detective Controls

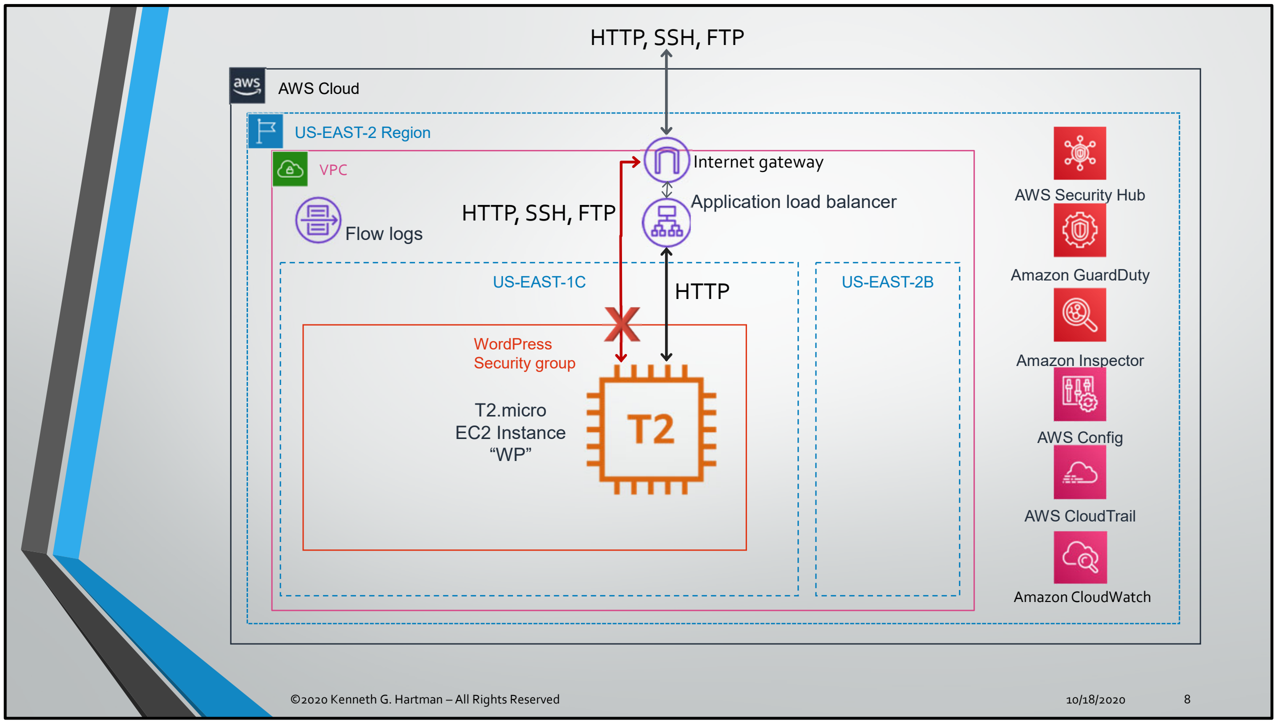
10/18/2020 7

A well-designed cloud environment will have very robust preventive controls. Effective preventive controls keep attackers out while detective controls, properly implemented, will alert us that an attacker has bypassed one or more preventive controls. Detective controls are designed to keep a bad situation from getting worse.

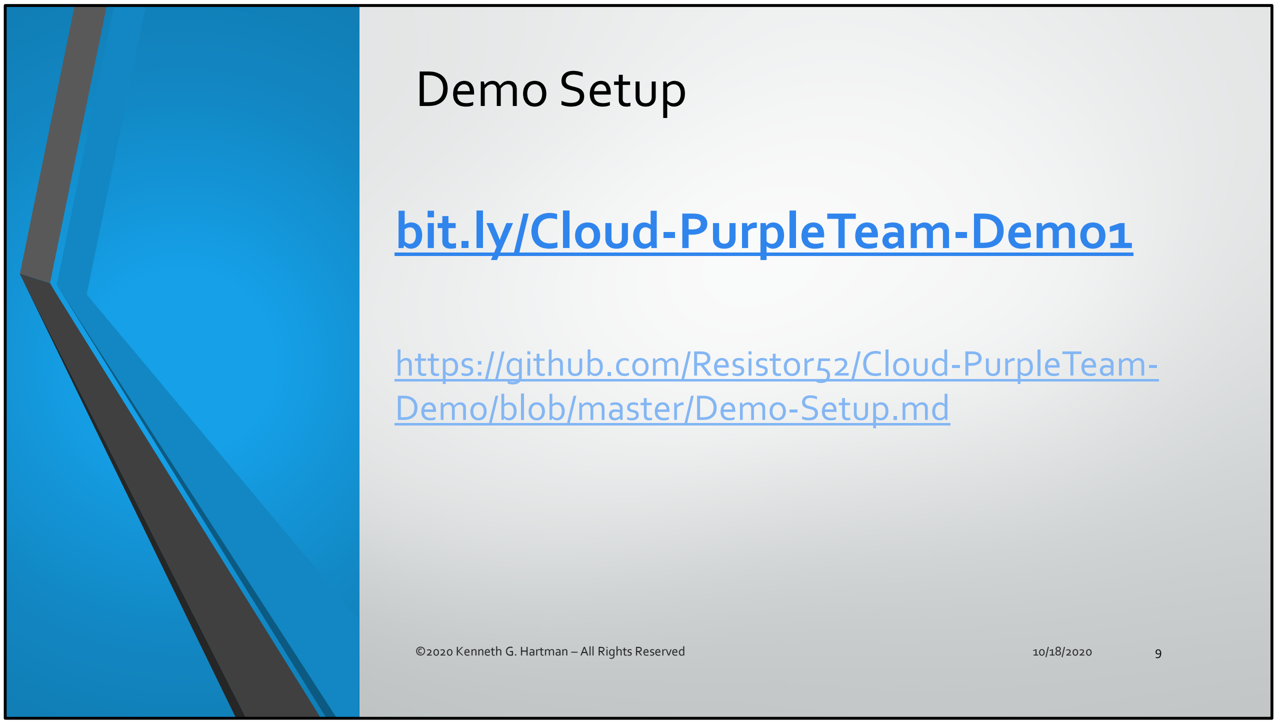
Generally, the earlier you can react to a security incident in progress, the less damage will occur. In the cloud, architects can design cloud environments with extensive network segmentation and strong authentication in keeping with zero-trust principles. In addition, architects can design security automation to programmatically remediate anticipated failures of primary preventive controls and unauthorized changes that weaken the cloud environment's security posture.

We cover these tactics in depth in SEC545 – Cloud Security Operations & Architecture and other classes in the SANS Cloud Curriculum. This truly shifts the advantage back to the defenders.

In this demonstration, we are going to use an intentionally vulnerable virtual machine in a cloud environment with weak preventive controls so that we can have fun attacking it and to see what the detective controls capture.



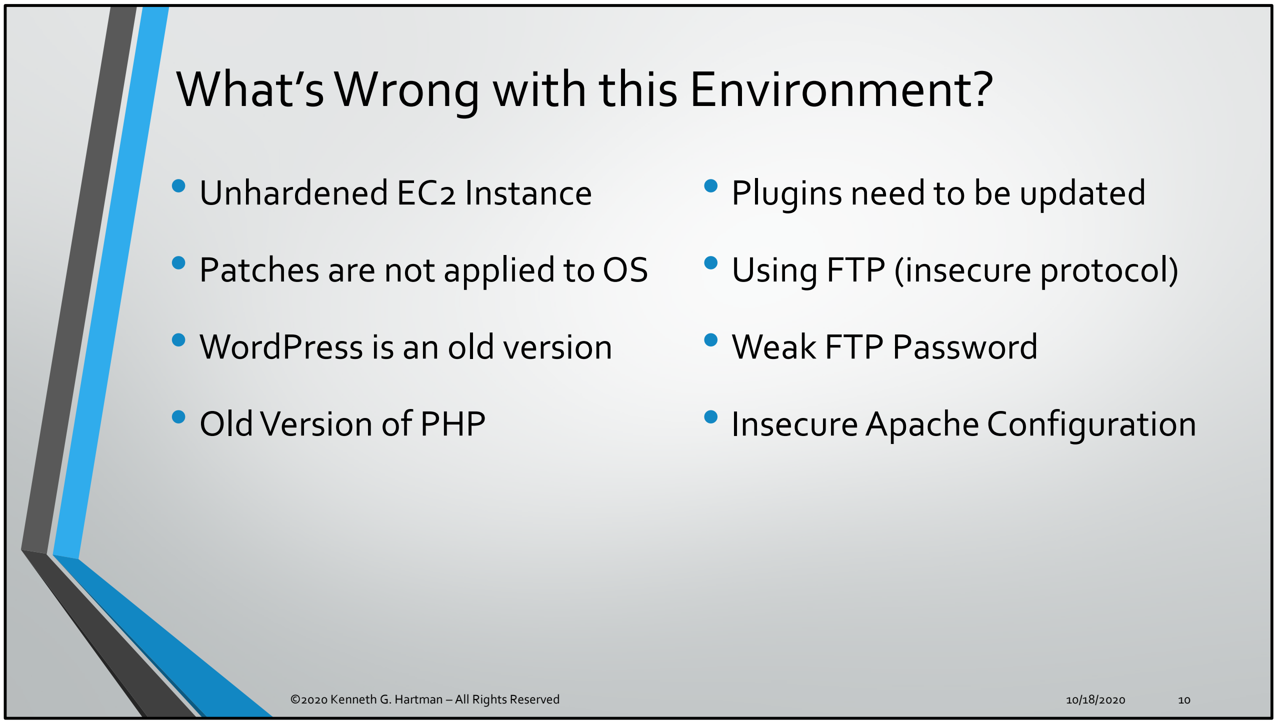
HTTP, SSH, FTP
AWS Cloud
US-EAST-2 Region
VPC
Internet gateway
Application load balancer
Flow logs
HTTP, SSH, FTP
US-EAST-1C
HTTP
US-EAST-2B
WordPress
Security group
T2.micro
EC2 Instance
"WP"
T2
AWS Security Hub
Amazon GuardDuty
Amazon Inspector
AWS Config
AWS CloudTrail
Amazon CloudWatch



Demo Setup

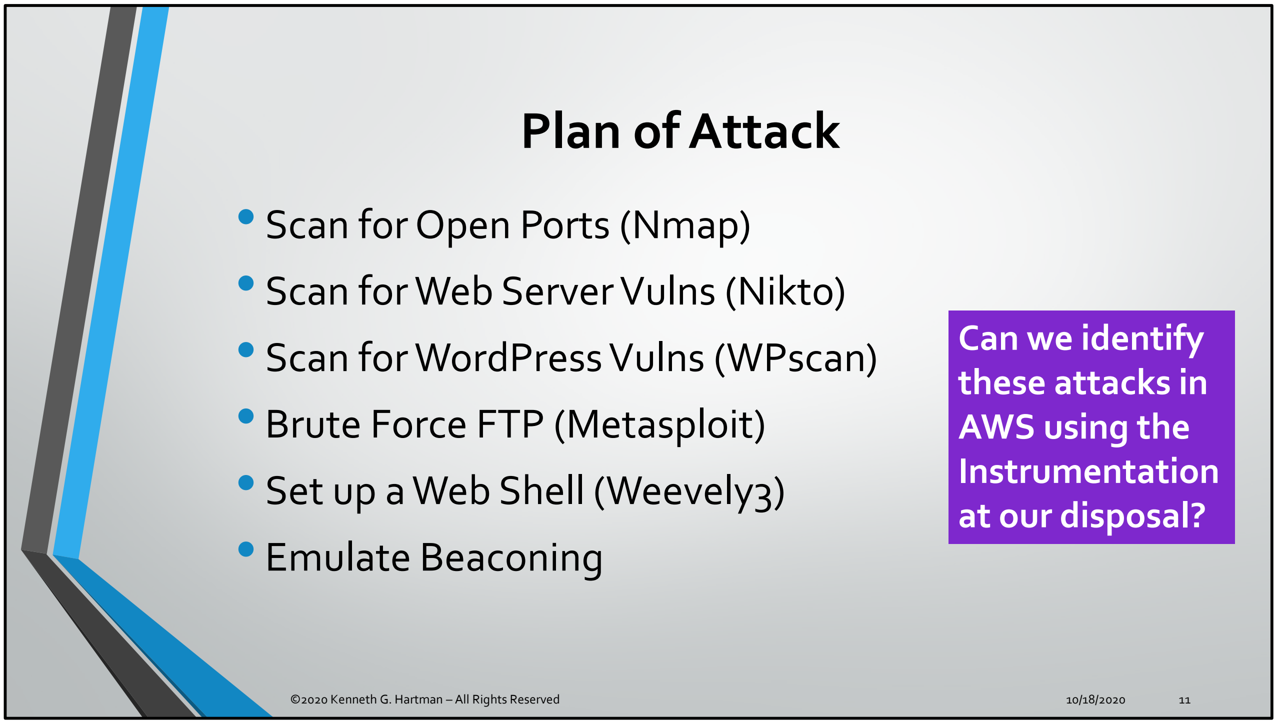
bit.ly/Cloud-PurpleTeam-Demo1

https://github.com/Resistor52/Cloud-PurpleTeam-Demo/blob/master/Demo-Setup.md



What’s Wrong with this Environment?

- Unhardened EC2 Instance
- Patches are not applied to OS
- WordPress is an old version
- Old Version of PHP
- Plugins need to be updated
- Using FTP (insecure protocol)
- Weak FTP Password
- Insecure Apache Configuration



Plan of Attack

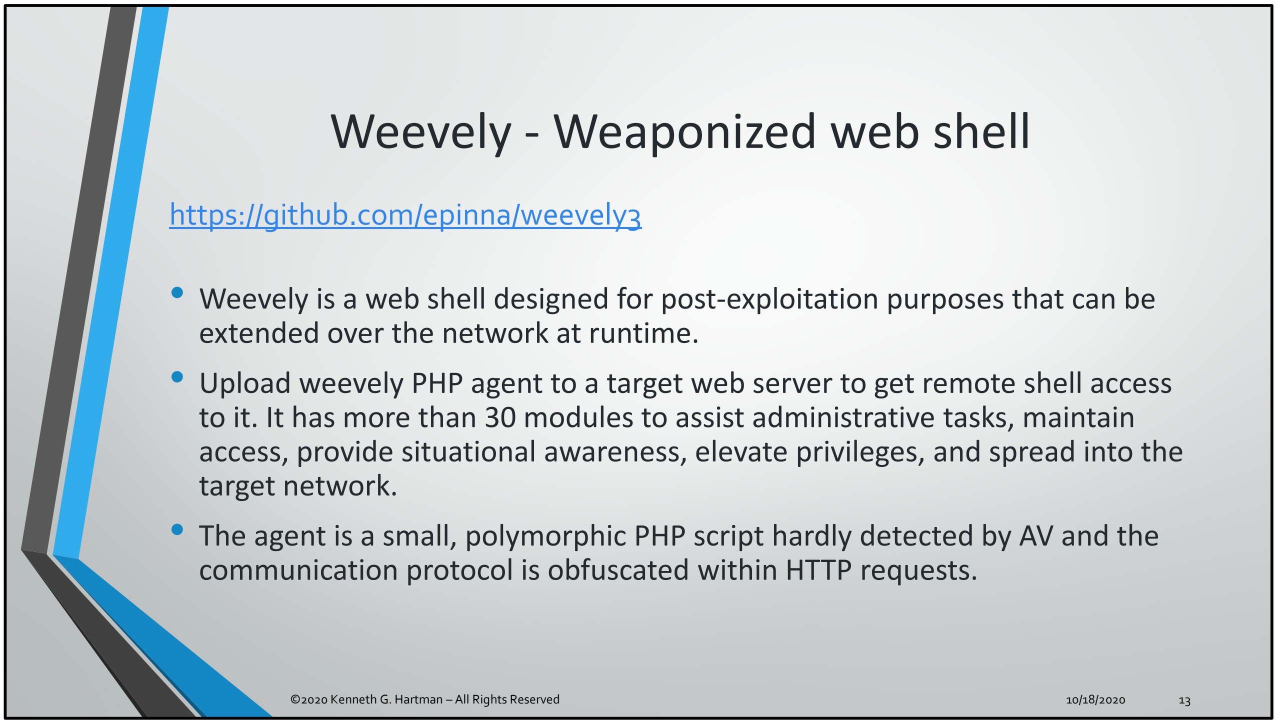
- Scan for Open Ports (Nmap)
- Scan for Web Server Vulns (Nikto)
- Scan for WordPress Vulns (WPscan)
- Brute Force FTP (Metasploit)
- Set up a Web Shell (Weevely3)
- Emulate Beaconing

Can we identify these attacks in AWS using the Instrumentation at our disposal?

Attack Phase

http://bit.ly/Cloud-PurpleTeam-Attack

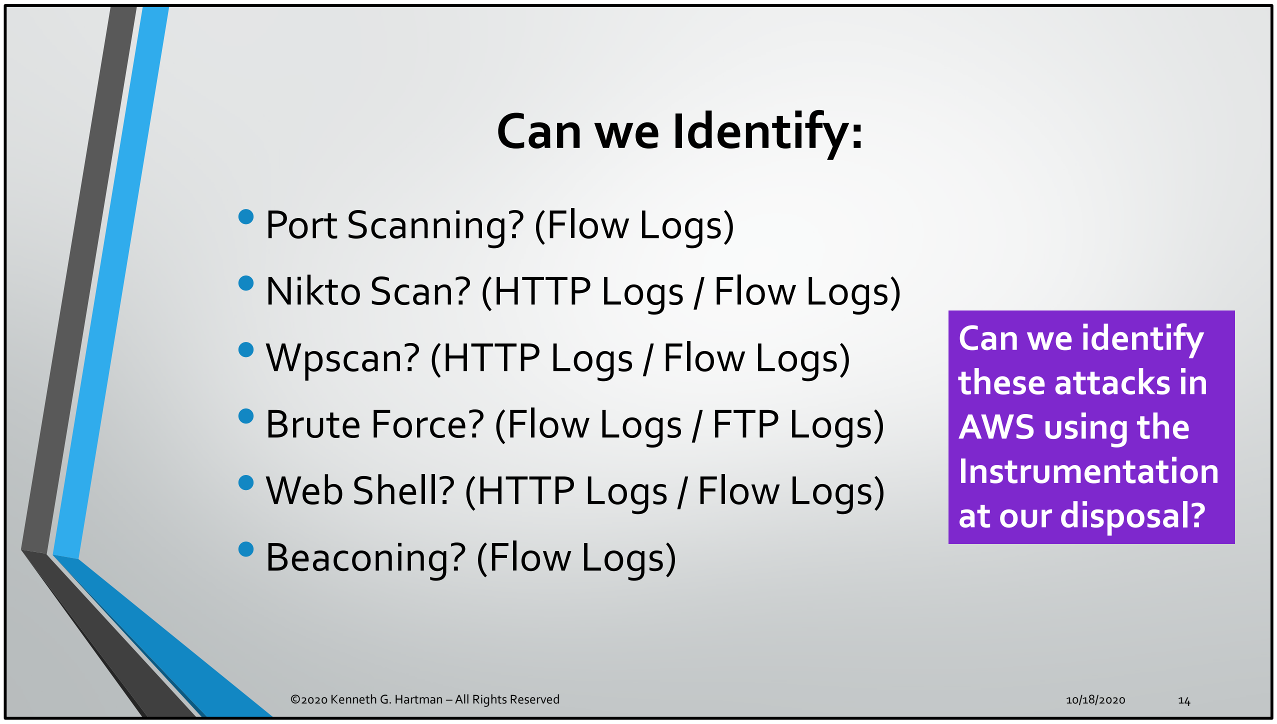
https://github.com/Resistor52/Cloud-PurpleTeam-Demo/blob/master/Attack-WP.md



Weevely - Weaponized web shell

https://github.com/epinna/weevely3

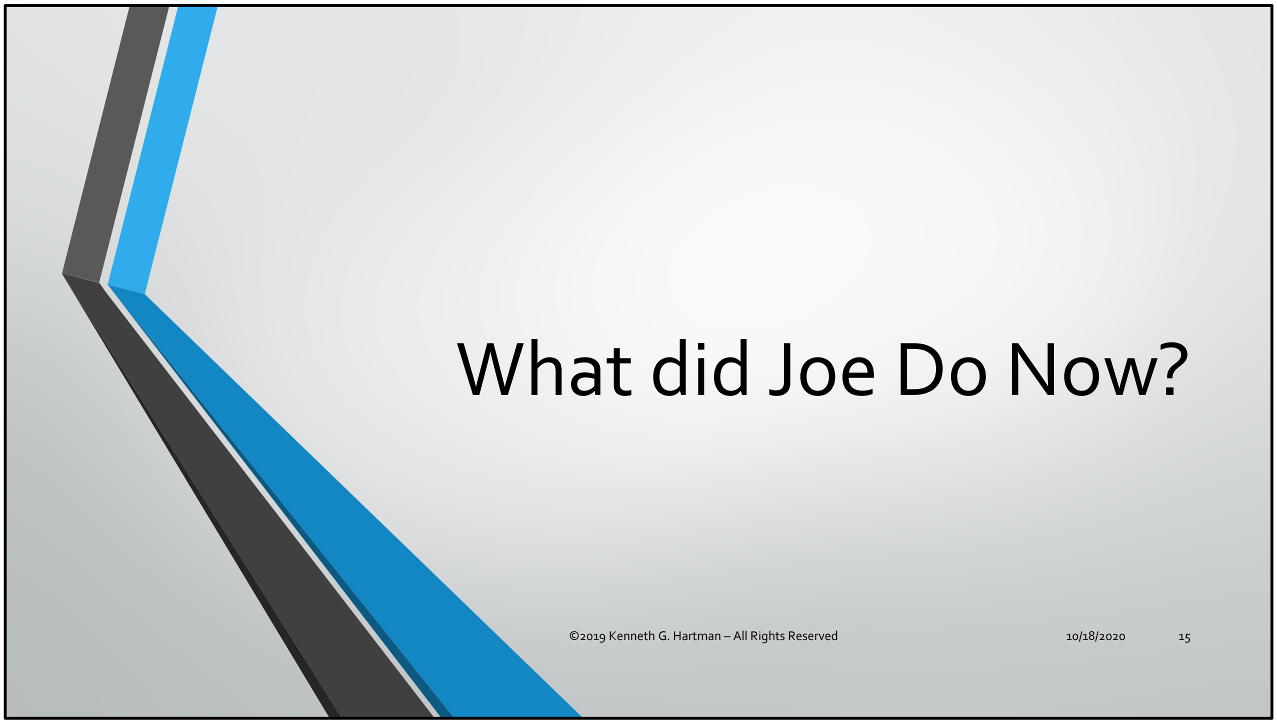
- Weevely is a web shell designed for post-exploitation purposes that can be extended over the network at runtime.
- Upload weevely PHP agent to a target web server to get remote shell access to it. It has more than 30 modules to assist administrative tasks, maintain access, provide situational awareness, elevate privileges, and spread into the target network.
- The agent is a small, polymorphic PHP script hardly detected by AV and the communication protocol is obfuscated within HTTP requests.



Can we Identify:

- Port Scanning? (Flow Logs)
- Nikto Scan? (HTTP Logs / Flow Logs)
- Wpscan? (HTTP Logs / Flow Logs)
- Brute Force? (Flow Logs / FTP Logs)
- Web Shell? (HTTP Logs / Flow Logs)
- Beaconing? (Flow Logs)

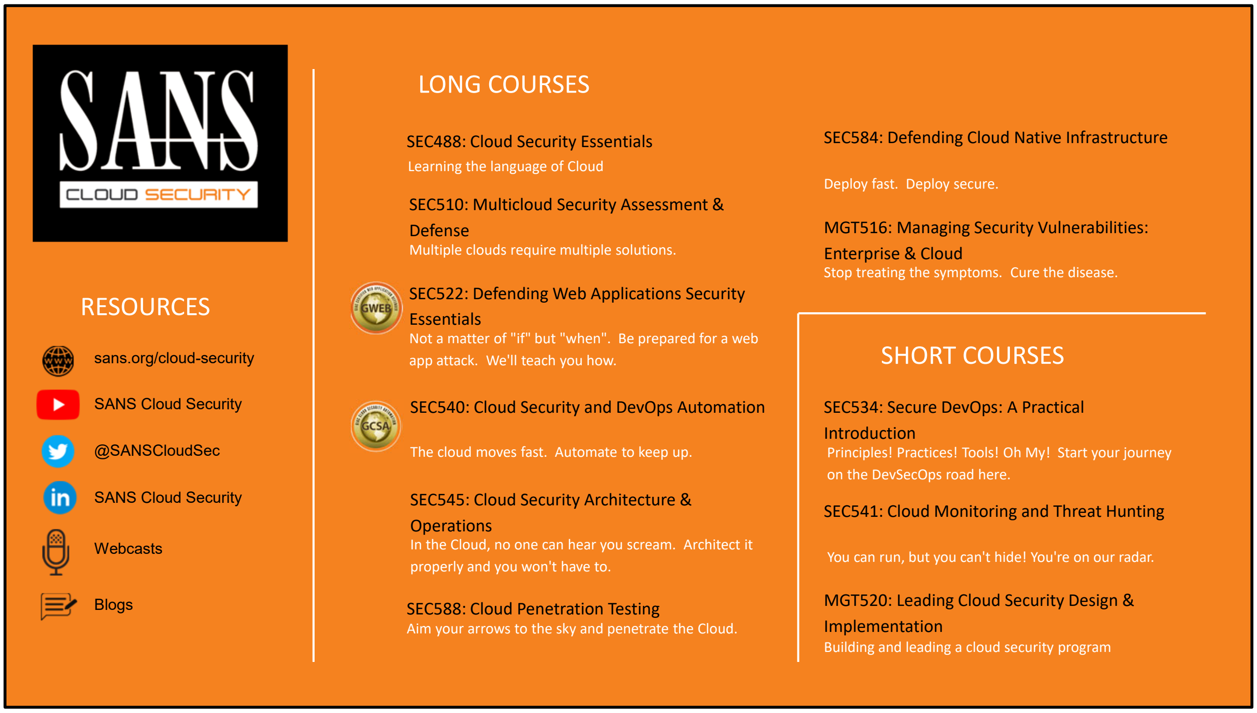
Can we identify these attacks in AWS using the Instrumentation at our disposal?



What did Joe Do Now?

AWS Config

AWS CloudTrail → User: Joe



SANS CLOUD SECURITY

RESOURCES

- sans.org/cloud-security
- SANS Cloud Security
- @SANSCloudSec
- SANS Cloud Security
- Webcasts
- Blogs

LONG COURSES

SEC488: Cloud Security Essentials
Learning the language of Cloud

SEC510: Multicloud Security Assessment & Defense
Multiple clouds require multiple solutions.

GWEB SEC522: Defending Web Applications Security Essentials
Not a matter of "if" but "when". Be prepared for a web app attack. We'll teach you how.

GCSA SEC540: Cloud Security and DevOps Automation
The cloud moves fast. Automate to keep up.

SEC545: Cloud Security Architecture & Operations
In the Cloud, no one can hear you scream. Architect it properly and you won't have to.

SEC588: Cloud Penetration Testing
Aim your arrows to the sky and penetrate the Cloud.

SEC584: Defending Cloud Native Infrastructure
Deploy fast. Deploy secure.

MGT516: Managing Security Vulnerabilities: Enterprise & Cloud
Stop treating the symptoms. Cure the disease.

SHORT COURSES

SEC534: Secure DevOps: A Practical Introduction
Principles! Practices! Tools! Oh My! Start your journey on the DevSecOps road here.

SEC541: Cloud Monitoring and Threat Hunting
You can run, but you can't hide! You're on our radar.

MGT520: Leading Cloud Security Design & Implementation
Building and leading a cloud security program

The SANS Institute, established in 1989 as a cooperative research and education organization, is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost the largest collection of research documents about various aspects of information security, and it operates the internet's early warning system—the Internet Storm Center. Its programs now reach more than 165,000 security professionals around the world.

SANS offers a number of courses that teach developers, architects, testers, security professionals, and managers how to build more secure applications. Anyone involved in developing, securing, and defending applications can benefit from the following courses in the SANS Cloud Security Curriculum:

SEC488: Cloud Security Essentials:

Advise and speak about a wide range of cloud security topics and help your organization successfully navigate both the security challenges as well as the opportunities presented by cloud services.

SEC510: Multi-Cloud Security Assessment & Defense

Perform multi-cloud security assessments across AWS, Azure, and GCP clouds identifying key weaknesses and hardened configurations in core cloud services.

SEC540: Cloud Security & DevOps Automation

Provides development, operations, and security professionals with a methodology to build and deliver secure infrastructure and software using cloud services and DevSecOps workflows.

Questions?