Wild Eagle Security

Cyber Training & Forensic Services

One Colonial Drive
Old Fort Niagara
Youngstown, NY 14174

From: Philip Chandler, CEO

Welcome

Thank you for joining Wild Eagle. I'm sure Adam James, CTO has made you aware of the issues with Sam Hammett and the previous team. Our clients expect more than latest cyber-forensics, security training and advice. They expect that we have implemented the best practices we preach. I shouldn't need to remind you what happened to HBGary Federal when it's officers failed to follow best practices.

The recent press has caused client defections and we cannot afford any more losses. Our Senior Investigators are: Chen Xiaolong, Perry Gardner and Auguste Poe. They are the heart of Wild Eagle and require your support. Don't get in their way, give them what they need when they need it.

Until the new team can properly secure our systems; the auditors (John Rankin, Hercule Christie, Dirk Adams, Mike Spillane) have required that confidential information for most but not all clients be moved to a secure offline storage facility. You will need to implement proper data access controls before the data can be put back online.

A few of Adam's directors will be in the room helping you with your "orientation" over the next couple days. Sorry, it will be more a baptism by fire rather than warm and fuzzy HR message about Wild Eagle's mission. The work starts at 10 AM Friday.

--Philip

Wild Eagle Security

From: Adam James, CTO

RE: **Google Accounts**

Like the qualifier; White team injects will be delivered and scored using Google Classroom.

You will be provided a team Google account and login credentials just prior to scoring. Only the black team will know the login credentials. The login information should NOT be shared with anyone.

You can access Classroom with any device in the team room. You will be provided a dedicated device that is independent of your team network infrastructure.

IMPORTANT:

- The account will be monitored by the black team.
- Access to the account must be limited to times when services are actively being scored.
- No attempt should be made to change the login password or add 2FA.
- Only authorized in-room devices are allowed to use the account

Any breach to the above policy will result in disqualification.

Wild Eagle Security

RE: **Machine overviews**

HAMMER.{team}.wildeagle.net: Base image derived from current AWS Linux AMI, one image for all teams. Intent: provide forward proxy for HTTP hosted services.

GENTLY.{team}.wildeagle.net: Palo Alto VM100, one image for all teams. Intent: Control point for network traffic in/out of VPC.

BROWN.{team}.wildeagle.net: Base image derived from EC2Box, customized for each team. Intent: Allow SSH access to systems in the private subnet.

POIROT.{team}.wildeagle.net: Base image derived from current AWS Linux AMI customized with JuiceBox training, one image for all teams. Intent: Support training services Wild Eagle offers to customers.

MASON.{team}.wildeagle.net: Base image derived from Ubuntu AMI with iRedMail, customized for each team. Intent: Provide email support for employees.

SPADE.{team}.wildeagle.net: Base image derived from Ubuntu AMI with GLUU, customized for each team. Intent: Provide identity services.

CAO.{team}.wildeagle.net: Base image derived from Ubuntu AMI with OTRS, customized for each team. Intent: Provide help desk service to employee and customers.

DUPIN.{team}.wildeagle.net: Base image derived from Ubuntu AMI with Splunk, one image for all teams. Intent: Logging cloud events.

TINTIN.{team}.wildeagle.local: Windows Server 2012. Domain controller. Intent: manage local machines and users.

HOLMES.{team}.wildeagle.local: Windows Server 2016. Intent: Web server and common file sharing.

MARPLE.{team}.wildeagle.local: Debian based. Intent file services

TRACY.{team}.wildeagle.local: Debian based. Intent:Web services

User workstations: Not scored. Repurposing as backup services not allowed.

Mulder.{team}.wildeagle.local: Windows 10 workstation

Clouseau.{team}.wildeagle.local: Windows 10 workstation

Gadget.{team}.wildeagle.local: Kali 2018.1. Intent: Pen testing and self analysis tools

Payne.{team}.wildeagle.local: SIFT Workstation. Intent: Forensic and IR tools

Known administrative machine access

Machine access	User	Password
http://cao.{team}.wildeagle.net/otrs/index.pl	sam	Change.me!
http://cao.{team}.wildeagle.net/phpmyadmin	sam	Change.me!
http://cao.{team}.wildeagle.net:8000	sam	Change.me!
https://mail.{team}.wildeagle.net/iredadmin	postmaster@neccdc2018.org	Neccdc-2018
http://splunk.{team}.wildeagle.net:8000	admin	Change.me!
https://brown.{team}.wildeagle.net	admin	Chang3.me!
https://gently.{team}.wildeagle.net	admin	Neccdc-2018
SSH: hammer.{team}.wildeagle.net	ec2-user	team-ssh-key
SSH: poirot.{team}.wildeagle.net	ec2-user	team-ssh-key
SSH: dupin.{team}.wildeagle.net	ubuntu	team-ssh-key
SSH: cao.{team}.wildeagle.net	ubuntu	team-ssh-key
SSH: spade.{team}.wildeagle.net	ubuntu	team-ssh-key
SSH: brown.(team).wildeagle.net	ec2-user	team-ssh-key
SSH: mason.{team}.wildeagle.net	ubuntu	team-ssh-key
tintin.{team}.wildeagle.net	Administrator	Change.me!
holmes.{team}.wildeagle.net	Administrator	Change.me!
marple.{team}.wildeagle.net	admin	Change.me!
tracy.{team}.wildeagle.net	admin	Change.me!
mulder.{team}.wildeagle.net	admin	Change.me!
clouseau.{team}.wildeagle.net	admin	Change.me!
gadget.{team}.wildeagle.net	blue	blue
payne.{team}.wildeagle.net	blue	blue

AWS console access is defined in your team arrival package