

ATTACKTACTICS

PART 6

RETURN^{OF}_{THE} BLUE TEAM



Webcast

ACTIVE | COUNTERMEASURES



AUGUST 3-6, 2019

MANDALAY BAY / LAS VEGAS

A GUIDE TO ACTIVE DEFENSE, CYBER DECEPTION AND HACKING BACK

instructor: john strand

AI HUNTER™

Network Threat Hunting Solution

ANALYZE

Network Traffic

IDENTIFY

Compromised Systems

HUNT

Menacing Threats



**BEACONS
MODULE**



**LONG CONNECTIONS
MODULE**



**DEEP DIVE
MODULE**



ALERTING

REQUEST A PERSONAL DEMO

Type "Demo" in Questions Window



CALL FOR PAPERS

The CFP is now open for 2019 and
will officially close on May 31st.

Oct 23rd (afternoon) thru Oct 25th | DEADWOOD, SD

11:35 - Start of Attack (Gaining Access), Password Spraying Toolkit

- UBEA on the perimeter
- Remember, no account lockout
- Access accounts via recon
- Possibly setting up honey accounts
- Limit what people put on their LinkedIn and other social media profiles
- CanaryTokens
- Let's have a chat about 2FA



15:24 - Mailsniper, Retrieve Global Access

Windows Defender Advanced Threat Protection
New Alert Detection

Title	Access to Exchange inboxes using MailSniper
-------	---



ACTIVE | COUNTERMEASURES

21:58 - Lateral Movement, OWA, VPN, SSH

- This one is hard
- We were simply “logging in”
- This highlights the need for strong 2FA policies
- Most organizations have 2FA
- It has to be everywhere
- 99% is not enough
- Also, some of the services and pages should have only been accessible **behind** a VPN
- Reduce the external authentication surface
- OVPN Honeypot?

27:05 - Scanning/Enumeration, Nmap SSH Brute Force, "Find Open", Movement, Gaining Access

- Simple internal network IDS should have caught this
- Treat the internal network as hostile, because it is!
- If it is so simple, why do we not see it more often?
- On the topics of luminaries and firewalls
- One security control does not invalidate the need for other controls
- We still have not learned this



34:07 - Gaining Access, Test for LLMNR, What is LLMNR, Responder, NtlmRelayX

- Disable LLMNR.... Now.
- <https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/>
- Why do we see this?
- Admins... It is always the admins... Why?
- CIS templates
- Practice good SMB (Disable SMBv1, Kill LM and NTLM, use host-based firewalls, etc.)
- <https://pen-testing.sans.org/blog/2013/04/25/smb-relay-demystified-and-ntlmv2-pwnage-with-python>
- <https://www.secureauth.com/blog/playing-relayed-credentials>



45:53 - Gaining Access, Lateral Movement - crackmapexec

- Once again, host-based firewalls
- I am also going to go out on a limb and say strong passwords
- I know... I know we can use hashes, but hold up a moment
- Also, Canary accounts are pretty keen for detecting this as well
- Very low impact honeypots can provide high value



50:29 - Gaining Access, GoPhish Campaign, Additional Paths to Access, HTA, Co Strike

- Endpoint is key here
- But set up your endpoint to succeed
- Also, beacon analysis
- RITA is free, we are bringing back Egress NIDS
- The far right of MITRE is often ignored

Command and Control	Exfiltration
Commonly Used Port	Automated Exfiltration
Communication Through Removable Media	Data Compressed
Connection Proxy	Data Encrypted
Custom Command and Control Protocol	Data Transfer Size Limits
Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol
Data Encoding	Exfiltration Over Command and Control Channel

Thanks!

- @strandjs
- john@blackhillsinfosec.com
- @rev10d
- @krelkci



ACTIVE | COUNTERMEASURES