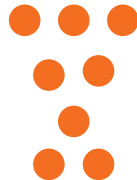


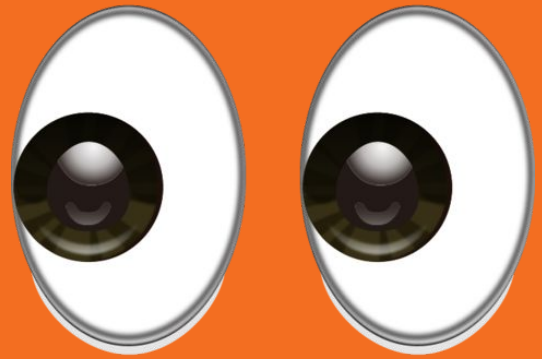
Welcome to RC3



RIT Competitive Cybersecurity Club
“Security Through Community”



**Today's meeting
brought to you
in part by...**



Platinum



Gold

hackerone

Wegmans

Educational Supporter



Gotta come to meeting <3

signin.rc3.club <3

Important dates & times

- The Incident Response Security Competition is **April 21st**
 - **White Team Signups:** <https://tinyurl.com/irsec2018-whiteteam>
 - Come volunteer and help us <3
- BSides Roc is **April 13-14th**
 - Buy tickets here: <https://www.eventbrite.com/e/bsides-rochester-2018-tickets-43047674754>
 - It's a great first conference.
 - 13th is Training day, 14th is the conference
 - If you cannot afford tickets to go, come talk to an RC3 E-board member
 - No one should be excluded from going to security events

HackerOne x RC3 Bug Bounty Competition

- Get money
- Get RC3 points
- Get exclusive HackerOne swag
- When you submit a bug bounty report to HackerOne, once the report has been resolved, you can submit it to @joel for even more points for even more prizes! Woo!

All Member Outing

- Let's try to sport.
- Current ideas are paintball and bowling, but what do you think?
- <https://goo.gl/forms/czAuS4Y41L9EQAr73>

Oh, the places you'll go

- Mailing List: Go to the website, scroll down!
 - Weekly announcements, hints for the Hard challenge, past week's challenge guide
- Facebook: [RITC3](#)
 - Announcements, random postings,
- Twitter: [@RC3 Official](#)
 - Just a lot of memes and retweets
- Youtube: [RC3club RIT](#)
 - SMASH THAT SUBSCRIBE BUTTON
- Instagram: [@rc3.club](#)
 - Please, we have 0 followers
- Slack: <https://ritc3.slack.com>
 - It's where work doesn't happen
- ANSR: [listen.rc3.club](#)

Disclaimer

The information contained in this presentation is for educational purposes ONLY! RC3 nor its members hold any responsibility for any misuse of the information provided in any slides, discussions, activities, or exercises.

...You have been warned.

Without further ado...

8. Intro to Windows Red Teaming



We throwing shade up in here

whoami

- 3rd year Comp Sec
- Windows Clients on CCDC
- Co-Captain of CPTC
- OSCP
- SPARSA
- RC3
- ABC123
- I enjoy music, football, baseball,
and the outdoors



Overview

- Exploitation
 - Popular Exploit Tools
 - Out in the wild exploitation
- Persistence
 - Scheduled Tasks
 - Shares
 - Registry
 - Services



Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.

0% complete



For more information about this issue and possible fixes, visit <http://windows.com/stopcode>

If you call a support person, give them this info:

Stop code: DRIVER_IRQL_NOT_LESS_OR_EQUAL

What failed: mrxsmb20.sys

Metasploit

- Popular pentesting framework
 - Uses meterpreter which is an extremely flexible payload
 - Perform Dll injection, Beacons, pivoting, etc.
 - Has a frontend called armitage but meh
- Has many common exploits that are easy to use
 - MS08-067, MS17-010, MS03-026
- Basic Usage:
 - Setup a listener
 - exploit vulnerability
 - have exploit code call back to listener
 - ???
 - Profit

Metasploit Cont.

- Meterpreter has many modules
 - Mimikatz module to dump credentials
 - Powershell module to run powershell commands on Windows host
 - Wireshark module
- Metasploit has many post-ex modules that can also be used
 - Use this to elevate privs to Local System

Powershell Empire

- Powershell post-exploitation kit
 - With powershell comes a wealth of tools
 - direct access to the win32api
- Comes with a variety of modules and tools
 - Postex
 - Lateral Movement
 - Persistence

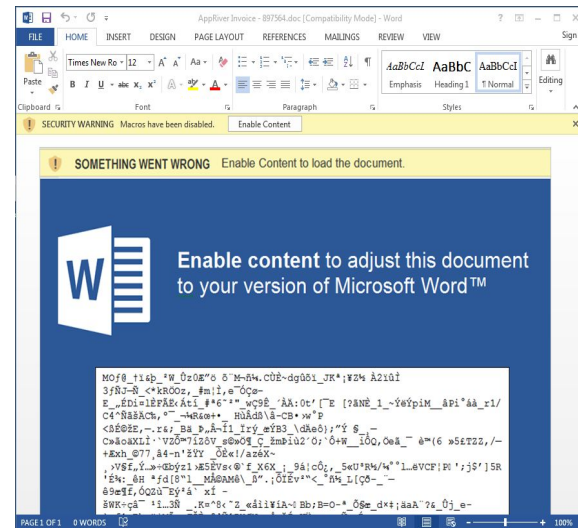


Powershell Empire cont.

- Postex
 - Powerup
 - Great Privesc tool that provides good information on potential ways to Local System!
 - Mimikatz
 - Integration with mimikatz
 - Stores gathered credentials in a db for easy access
 - Access to kerberos for that juicy golden ticket
- Quick [Demo](#)

Out in the Wild Exploitation

- Most “in the wild exploitation” is done by phishing
 - Malicious macros are a big hit
 - Written in vbs and pull down other payloads
- Rarely exploits will actual be used for an attack
 - WannaCry (MS17-010)
 - The Hacking Team Hack (Custom IoT Exploit)
- Postex usually consists of gathering hashes and psexec



Persistence!

- That initial vector may close
- Persistence is an art
- How do you stay hidden while also staying alive?

Scheduled Tasks

- One of the most basic forms of userland persistence
- Similar to a cronjob in Unix
- Will only run if the user that owns the task is logged in
 - Thankfully LocalSystem is always logged in ;)
- Really easy to clear
 - `winkey + r + schtasks /delete /tn * /f`



Shares & SMB

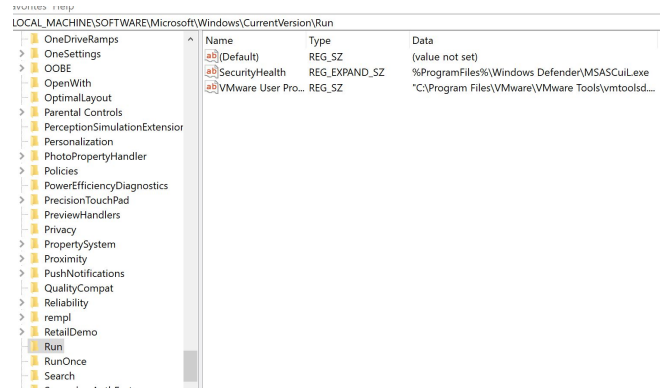
- SMB is vital to normal Windows operation
 - but of course it can be used against you...
- PsExec
 - Really easy but super loud
 - Even creates a service on the target (yikers!)
- net use
 - Administrative shares are shared secretly Ex.) C\$
 - browse targets files on your local machine
- SMBExec
 - a stealthier version of psexec
 - creates a service with a batch file then removes the service

```
root@labs:~/github/smbexec-2# ./smbexec.rb --help
```

```
*****  
* smbexec 2.0 - Machiavellian *  
*****
```

Registry

- Where to even start...
- Autorun keys!
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
 - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
 - run at user level
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
 - run at system level
 - HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
 - There is more but most (if not all) are picked up by autoruns

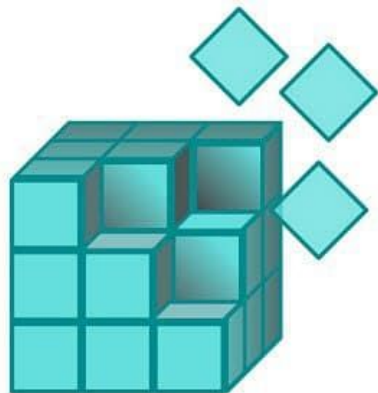


Registry Cont.

- Appinit_DLL
 - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Applnit_Dlls
 - Starting in Windows 7, microsoft requires all Applnit_Dlls to be signed... :(
- Oh wait we can just turn that off!
 - RequireSignedApplnit_DLLs - set to 0
- Houston we have a problem...
 - If Secureboot is enabled, Appinit_Dlls is disabled
 - Autoruns of the sysinternals suite

Registry Cont.

- Default Firewalls rules can be hijacked
 - HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Defaults\FirewallPolicy\FirewallRules
- Capture creds with a password filter
 - HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages
 - Everytime a password request is made, the plaintext creds are sent
 - Downside - Box must be rebooted for filter to be registered

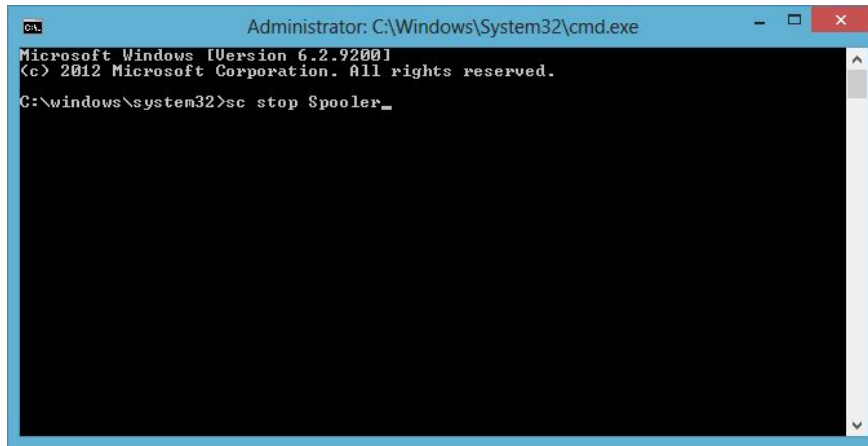


Services

- Crash Course on services
 - All services are managed by the Service Control Manager (SCM)
 - Service accounts run these services
 - **Local System**, Local Service, Network Service
 - **Local System similar to root account on Nix**
 - Perform background task and run important services
 - svchost.exe hosts multiple services to conserve resources
 - requires dll file that is loaded into the registry

Abusing Services

- Loading different binaries for Local System Services
 - `sc config <service> obj= “.\LocalSystem” password=`
 - `sc config <service> binpath= “malicious_binary.exe”`
 - check that space boi
- You can also break services using accounts
 - changing a service account of a service may break it



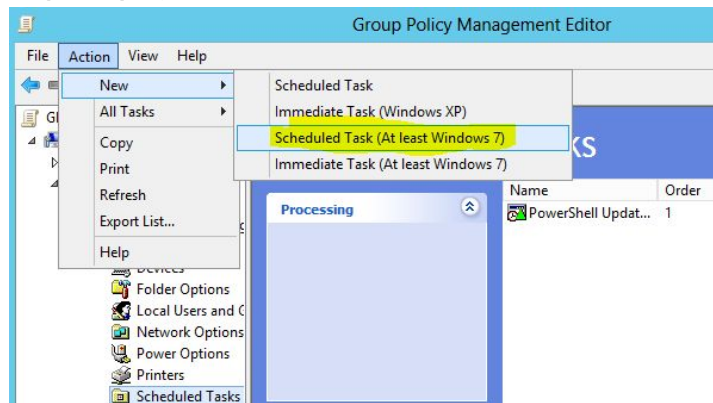
```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.
C:\windows\system32>sc stop Spooler_
```

Abusing Services cont.

- You could also write your own service!
 - With either C# or C++ you have full access to the WinAPI
 - Really isn't much you **CAN'T** do
- Unfortunately, it can be hard to hide from Process Explorer
 - an easy method of detection is verifying signature of signed executable

Group Policy

- If the client is part of a domain and we own the DC, we can spread joy everywhere!
- Some nice techniques:
 - push registry persistence to all clients on the domain
 - enable SMBv1 or downgrade authentication from NetLM to LM
 - enable a scheduled task to forge golden tickets every week
 - Set autorun registry keys to execute a powershell empire payload



Group Policy cont.

- You can also be very mean and disable many things
 - disable access to the registry
 - disallow certain programs
 - prevent the usage of cmd
 - print mean messages to people logging in
- Similar to the registry the group policy settings are very expansive
 - many aren't documented well or are not understood
- If the computer is not on a domain, Local Policy Settings work the same way

Kerberos and the Golden Ticket

- The domain controller is responsible for handling kerberos tickets
 - Used to give access to users and computers
- Important account called KRBTGT
- Three things required to generate a golden ticket
 - Domain Name
 - SID of KRBTGT account
 - KRBTGT password hash
- Using this golden ticket with Domain admin privs = whole network owned

Misc.

- Backdoor Shortcuts
 - surprisingly this still works
- Backdoor Sticky keys or the On Screen Keyboard
 - system shell without authentication
- Gathering registry hives and extracting hashes
 - C:\Windows\System32\config\<SAM or SYSTEM>
 - samdump2 <SAM> <SYSTEM>

Questions?

Demo info:

<info here>

Thank you

Feedback: <https://rc3club.typeform.com/to/JdS2IV>

