Sun City Computer Club

Cyber Security SIG

May 21, 2020

Questions, Comments, Suggestions welcomed at any time

Even Now

- Audio recording of this session as MP4 file
- Audio recording available at link shown above

Audio Recording In Progress

SIG attendees are required to be members of the chartered club sponsoring that SIG.
Sun City Community Association By-law

PARK PATROL ROBOT TRIAL IN PROGRESS

The robot SPOT (pictured on the right) is being trialled at Bishan-Ang Mo Kio Park from 8 May to 22 May 2020 as part of a collaboration between NParks and GovTech.

SPOT is able to traverse through various terrains autonomously and will aid in ensuring safe distancing in parks and gardens. We seek your cooperation not to disrupt it.

In collaboration with:

NATIONAL PARKS

GOVTECH

Reply-All Storm Protection NDR

Your reply to the email conversation wasn't sent.

The conversation is too busy with too many people.

admin	Office 365	biggroup
Action Required		Recipient

Do not use Reply All

How to Fix It

Consider trying one of the following options:

- **Don't resend the mail** – if the conversation is at risk of becoming a reply-all storm, it might be best to not reply to it at all. Your organization might even have policies that discourage or prohibit replying to everyone.
- **Send to a smaller number of recipients** – If you must reply, try replying or forwarding the message to a smaller number of recipients instead of using Reply All.

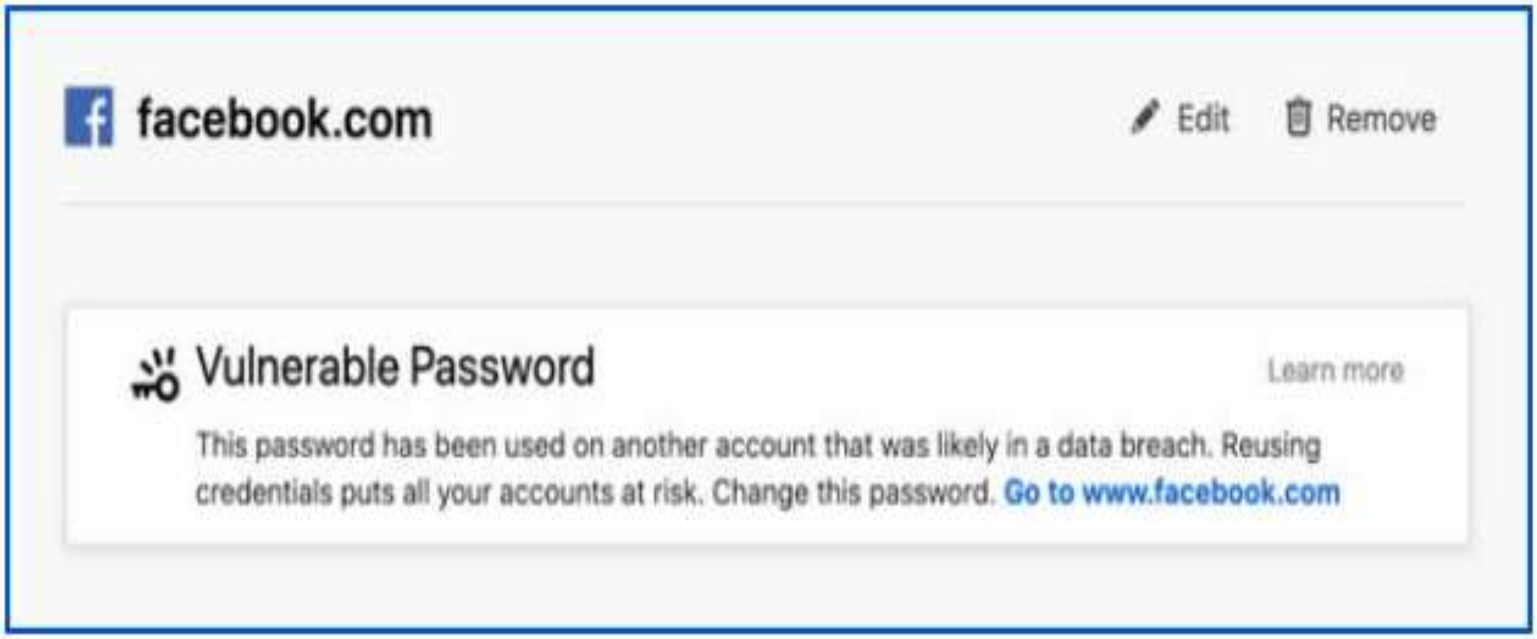
Current Issues

- Apple Mail
- iOS text lockup
- And more ?
- Microsoft May Tuesday Update
  CVE2020-1048 Print Spooler
  Persistent - post patch
  Back Door
- Roku activation fee
- TxDOT ransomware Texas Court System
  20 state & local agencies (Aug 2019)
- Covid-19 related attacks
- Apple Updates 20-May-2020 13.5

Current Issues

- Giphy
  Tracks GIFs
- 1x1 HTLM
- Snore pillow
- Firefox 76
  Lockwise Alert user for SAVED credentials used on REPORTED compromised site


Website Breach
Learn more
This breach occurred on July 10, 2012
Passwords were leaked or stolen from this website since you last updated your login details.
Change your password to protect your account. Go to login.yahoo.com


facebook.com
Edit
Remove
Vulnerable Password
Learn more
This password has been used on another account that was likely in a data breach. Reusing credentials puts all your accounts at risk. Change this password. Go to www.facebook.com

Current Issues

- Stored and Synched credentials
  Any/All browsers Apps
- Firefox video pop-out
- Many security vulnerabilities fixed
- Firefox 76.0.1

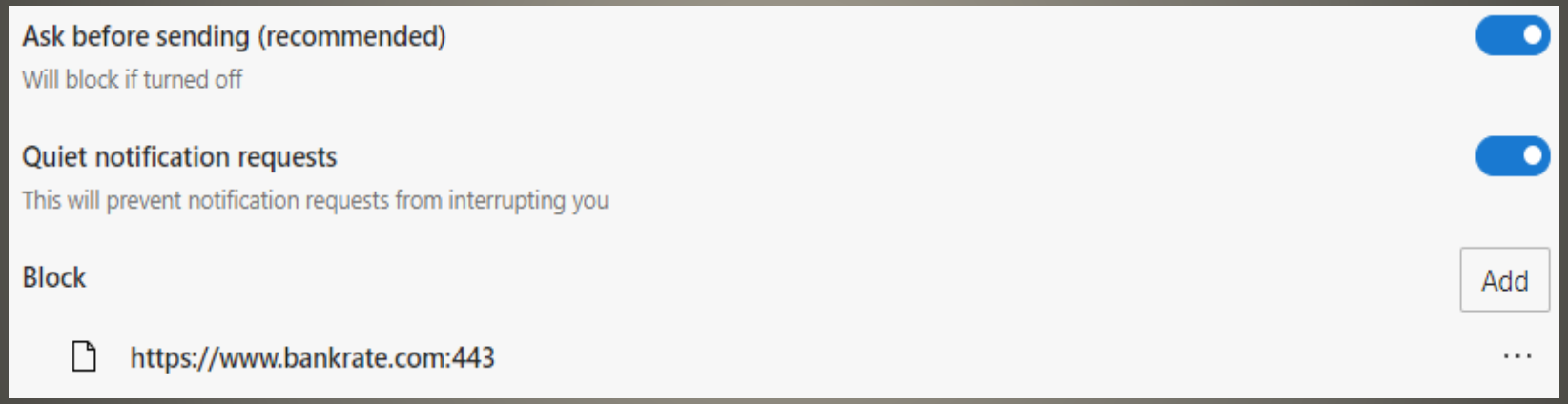
Chrome

- Chrome version 83
- Chromium based browsers
  Edge, Opera, Brave, Vivaldi, etc.
- WFH issues
- Privacy & Security settings
  Cookie if and how
  Cookie block on regular or Incognito
  Block all cookies on some or all sites
- Site settings Permission Permission activity

Chrome

- You and Google Sync controls
- Extension access
- Enhanced Safe Browsing Service
- DNS over HTTPS
- Security vulnerabilities “fixed”

- Notifications OS Notification methods



Edge

WordPress attacks

- 20 million attacks on 500000 sites
- Drive-by Supply chain Updates
  Repositories
- Increasing use of third-party “features”
  Then locked and forgotten
- vBulletin Update Immediately <period>

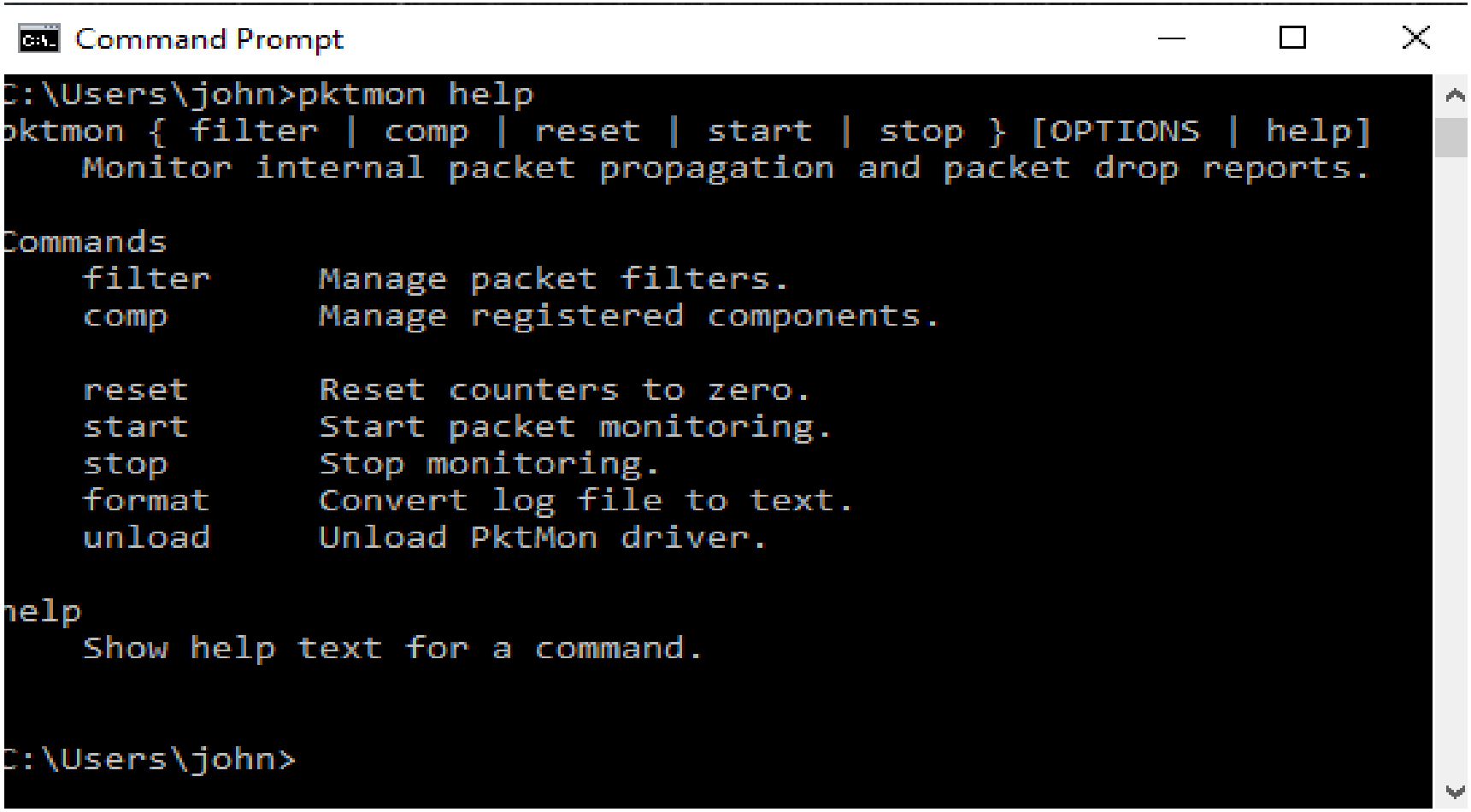
Current Issues

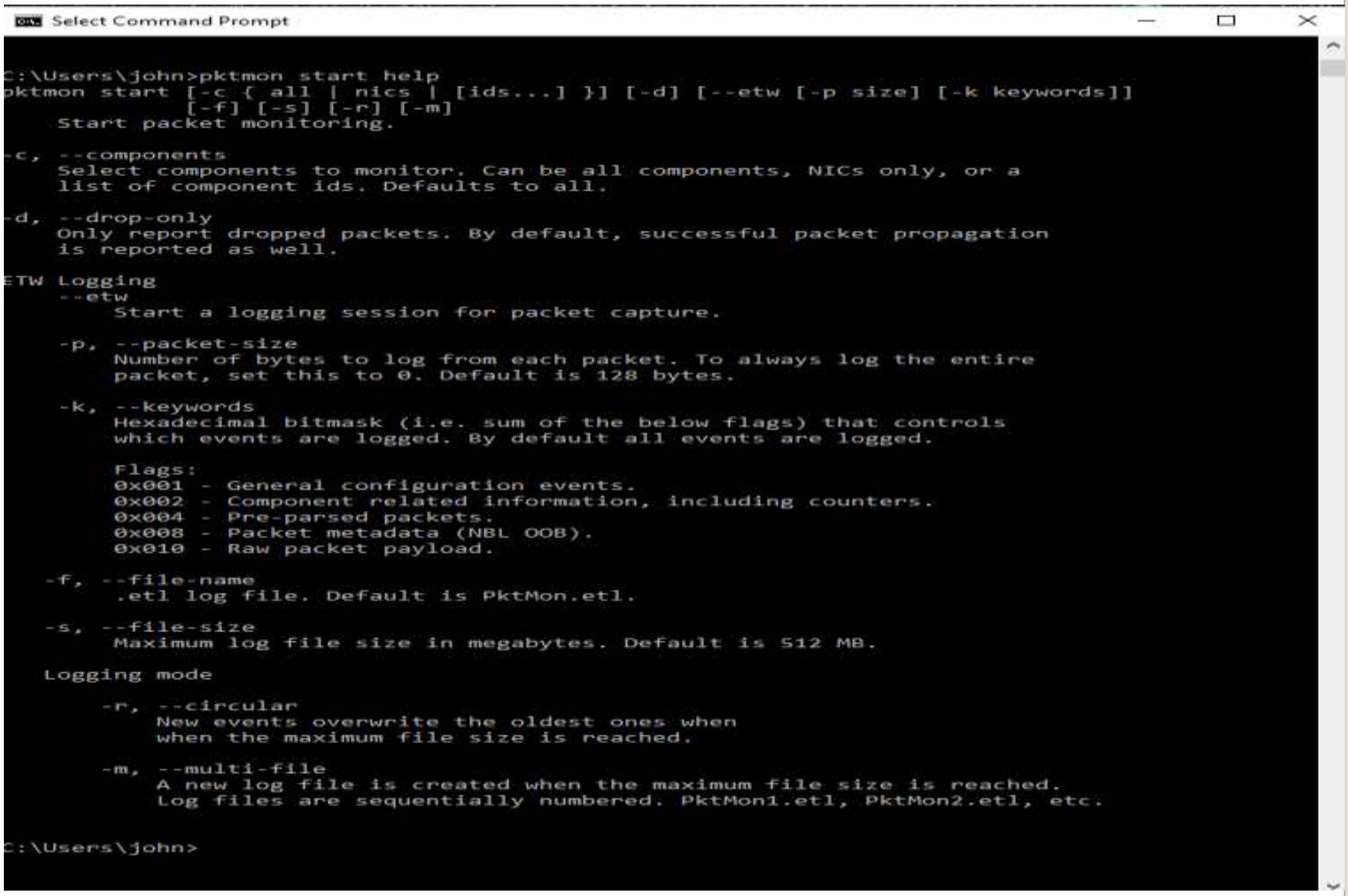
- Virtual security conferences
  Black Hat DefCon
- Samsung flaw for 6 years
  NewsBlog post 8-May
- ThunderSpy Evil Maid

Microsoft Patch Tuesday

- March 115 April 113 May 111
- Vulnerabilities ALL vulnerabilities
  Remote code execution
  Denial of service
  Privilege elevation
  Cross site scripting
  Memory corruption
  Spoofing
  Information disclosure
- .NET, visual studio, Edge NOT Office, Office 365, etc.
- Persistent backdoor not much noise

- DNS over HTTPS for Windows DoH
- Cloudflare 1.1.1.1
- Quad 9 9.9.9.9
- Google ??
- Name lookup – closest resolver
- Smart phone apps
- How now ?
- Packet monitor quick & dirty
  network packet monitor


Command Prompt
C:\Users\john>pktmon help
pktmon { filter | comp | reset | start | stop } [OPTIONS | help]
Monitor internal packet propagation and packet drop reports.
Commands
filter Manage packet filters.
comp Manage registered components.
reset Reset counters to zero.
start Start packet monitoring.
stop Stop monitoring.
format Convert log file to text.
unload Unload PktMon driver.
help
Show help text for a command.
C:\Users\john>


Select Command Prompt
C:\Users\john>pktmon start help
pktmon start [-c { all | nics | [ids...] }] [-d] [--etw [-p size] [-k keywords]]
[-f] [-s] [-r] [-m]
Start packet monitoring.
-c, --components
Select components to monitor. Can be all components, NICs only, or a
list of component ids. Defaults to all.
-d, --drop-only
Only report dropped packets. By default, successful packet propagation
is reported as well.
ETW Logging
--etw
Start a logging session for packet capture.
-p, --packet-size
Number of bytes to log from each packet. To always log the entire
packet, set this to 0. Default is 128 bytes.
-k, --keywords
Hexadecimal bitmask (i.e. sum of the below flags) that controls
which events are logged. By default all events are logged.
Flags:
0x001 - General configuration events.
0x002 - Component related information, including counters.
0x004 - Pre-parsed packets.
0x008 - Packet metadata (NBL OOB).
0x010 - Raw packet payload.
-f, --file-name
.etl log file. Default is PktMon.etl.
-s, --file-size
Maximum log file size in megabytes. Default is 512 MB.
Logging mode
-r, --circular
New events overwrite the oldest ones when
when the maximum file size is reached.
-m, --multi-file
A new log file is created when the maximum file size is reached.
Log files are sequentially numbered. PktMon1.etl, PktMon2.etl, etc.
C:\Users\john>

- pktmon comp list
  lists network interface components
  might be a lot of them
- Silently dropped might be un-dropped
- Other 3rd party network monitoring tools
  Wireshark
- Really eye-opening to “watch” your network
- First release - more to come?

Must run as Administrator

- iPhone encryption
  4 months and lots of costs
- A backdoor
- Subpoena proof
- Court admissible Court evidence
- Facial recognition & masks


255.255.255.0

- Utah system
- The sanctioned one
- The unsanctioned many

Contact Tracking vs Contact Tracing

- Helpful < - > Harmful
- Awareness, Preparedness, Understanding

Computer Club, Help Center, SIGs, Presentations, FirstTime, classes
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com


QUESTIONS?